Integrated Safeguards & Security Management
About
Your Voice Counts
Lessons Learned
Requirements
Mgmt Walkarounds
CY00 Rollout

Protecting Info

Personnel

Cyber Security

Nuclear Materials

Internal Security

Facility

General Resources

NEW! Security LPR/LIR's

ISSM Project Plan (12-13-01)

ISSM Action Plan (9-21-01)

ISSM Gap Analysis (8-17-01)

UC Gap-Analysis Guidance (7-11-01)

ISSM Communications Plan (4-12-01)

 Copyright © 2002 UC | Disclaimer/Privacy

Operated by the University of California for the National Nuclear Security Administration, of the US Department of Energy. Copyright © 2002 UC | Disclaimer/Privacy

Integrated Safeguards & Security Management
About
Your Voice Counts
Lessons Learned
Requirements
Mgmt Walkarounds
CY00 Rollout

Protecting Info

Personnel

Cyber Security

Nuclear Materials

Internal Security

Facility

General Resources

What is ISSM?

Why Should I Care?

ISSM Objective

8 Guiding Principles

5-Step Process

Safety & Security Policy

Draft ISSM Description Document

ISSM LPR

ISSM LIRs

Glossary

Integrated Safeguards & Security Management
About
Your Voice Counts
Lessons Learned
Requirements
Mgmt Walkarounds
CY00 Rollout

Protecting Info

Personnel

Cyber Security

Nuclear Materials

Internal Security

Facility

General Resources

Your Voice Counts

Questions? Concerns?
Call the Security Help Desk
5-2002

Integrated Safeguards & Security Management
About
Your Voice Counts
Lessons Learned
Requirements
Mgmt Walkarounds
CY00 Rollout

Protecting Info

Personnel

Cyber Security

Nuclear Materials

Internal Security

Facility

General Resources

CY00 Rollout

Workshop Guidance | Templates | Presentation Materials | Resources | Logistics

Post-workshop Actions

Workshop Guidance

Templates

Presentation Materials

Resources

Logistics

Integrated Safeguards & Security Management
About
Your Voice Counts
Lessons Learned
Requirements
Mgmt Walkarounds
CY00 Rollout

Protecting Info

Personnel

Cyber Security

Nuclear Materials

Internal Security

Facility

General Resources

Workshop Guidance

Workshop Guidance | Templates | Presentation Materials | Resources | Logistics

Strong Lab-wide management commitment and worker involvement are essential throughout the Laboratory to achieve the buy-in and ownership vital for truly integrating security into all work performed here. To support this end, a series of workshops have been designed to involve all managers and workers in applying the 5-step ISSM process to their work.

The following documents are provided to support you in planning and holding your division workshop planning sesssion and group ISSM workshops. The materials are provided for your convenience, and their use is suggested but optional.

Facilitation Guides provide detailed information on preparing for and implementing the workshops. The guides are available online in a PDF format. There is a table of contents with a listing of pages so that you may select the information you need. A printer-friendly, or condensed version is also available.

Trained facilitators are available to assist group-level managers with workshops. To request facilitation assistance, contact the Ombuds Program Mediation Center, **7-9367**.

Division Level

- Workshop Guidance - Division-Level
- ISSM Rollout Chart

Group Level

CONTACTS

Ombuds Mediation
Mary Beth Stevens
667-9367

RELATED LINKS

Ombuds Program
Mediation Center

- Workshop Guidance - Group-Level
- ISSM Rollout Chart

Operated by the University of California for the National Nuclear Security Administration, of the US Department of Energy. Copyright © 2002 UC | Disclaimer/Privacy

Integrated Safeguards & Security Management
About
Your Voice Counts
Lessons Learned
Requirements
Mgmt Walkarounds
CY00 Rollout

Protecting Info

Personnel

Cyber Security

Nuclear Materials

Internal Security

Facility

General Resources

Templates

Workshop Guidance | Templates | Presentation Materials | Resources | Logistics

These handouts and worksheets are provided to support your implementation of the ISSM model and can be used during the ISSM introductory workshops and beyond. The entire package, including the division and group-level workshop guidance is also available in .pdf.

ISSM 5-Step Process

Sample Applications of the 5-Step Process

Enhancing Your Security Awareness - Behaviors List

Resources Quick Reference List

Report Guidance For Division-level Directors

Report Guidance For Group-level Managers

ISSM Individual Performance Objective Worksheet

CONTACTS

Ombuds Mediation
Mary Beth Stevens
667-9367

RELATED LINKS

Ombuds Program
Mediation Center

Integrated Safeguards & Security Management
About
Your Voice Counts
Lessons Learned
Requirements
Mgmt Walkarounds
CY00 Rollout

Protecting Info

Personnel

Cyber Security

Nuclear Materials

Internal Security

Facility

General Resources

Presentations

Workshop Guidance | Templates | Presentation Materials | Resources | Logistics

Workshop Presentation Materials

- Division-Level Presentation Slides (PowerPoint)
- Group-Level Workshop Presentation Slides (PowerPoint)
- Case Studies
- Resources Quick Reference List
- LabNet 10 Schedule
- All Hands Meeting, July 18, 2000 - Real Video

Presentations Given

- All Hands Meeting, July 18, 2000 - J. Browne
- All Hands Meeting, July 18, 2000 - J. Weisheit
- LIM Meeting, June 27, 2000 - Carl Ostenak

CONTACTS

Ombuds Mediation
Mary Beth Stevens
667-9367

RELATED LINKS

Ombuds Program
Mediation Center

Integrated Safeguards & Security Management
About
Your Voice Counts
Lessons Learned
Requirements
Mgmt Walkarounds
CY00 Rollout

Protecting Info

Personnel

Cyber Security

Nuclear Materials

Internal Security

Facility

General Resources

Resources

Workshop Guidance | Templates | Presentation Materials | Resources | Logistics

Resources listed on this page provide quick links to security-related homepages as well as reference documents, and call lists. Don't forget that help is also just a phone call away. The S-Division Help Desk number is **5-2002** or email to secure@lanl.gov.

ISSM Homepage

Virtual Training Center

S-Division Homepage

ISEC Homepage

CONTACTS

S-Division Help Desk
665-2002

RELATED LINKS

ISSM Homepage

Virtual Training Center

S-Division Homepage

ISEC Homepage

Who To Contact

Annual Safeguards & Security Refresher Briefing

Who To Contact

Annual Safeguards & Security Refresher Briefing

Operated by the University of California for the National Nuclear Security Administration, of the US Department of Energy. Copyright © 2002 UC | Disclaimer/Privacy

LANL External View | security-www@lanl.gov
Security Help Desk: security@lanl.gov
Last Modified: 12/12/01

Integrated Safeguards & Security Management
About
Your Voice Counts
Lessons Learned
Requirements
Mgmt Walkarounds
CY00 Rollout

Protecting Info

Personnel

Cyber Security

Nuclear Materials

Internal Security

Facility

General Resources

Logistics

Attendance in the ISSM Introductory workshops is mandatory for all current LANL workers. Documentation of participation in the ISSM Introductory Workshops is critical in order to ensure those workers identified by line management have been made aware of the ISSM model and have had an opportunity to express concerns or suggestions regarding their individual role in security at the Laboratory.

Target Audience Identification - Who is required to complete the ISSM Workshop and the procedure for assigning your workers the ISSM Training Plan

Attendance Collection - Procedure for entering attendance rosters for EDS credit.

Facilitation Services

Integrated Safeguards & Security Management
About ISSM
Your Voice Counts
Lessons Learned
Requirements
Mgmt Walkarounds
CY00 Rollout

Protecting Info

Personnel

Cyber Security

Nuclear Materials

Internal Security

Facility

General Resources

Post-Workshop Actions

Between July and December 2000, more than 10,000 LANL workers (UC and subcontractors) successfully completed highly interactive ISSM Workshops tailored to their work and aimed at learning about ISSM, identifying S&S concerns, and pursuing actions for improving S&S performance. A post-workshop survey was conducted to assess the overall effectiveness of the program. The 1000 randomly sampled participants reported a better understanding of their security role following the workshops and rated the overall effectiveness of the workshops positively.

NEW! Responses to ISSM Workshop Questions, Concerns, and Suggestions

Survey Results

ISSM Rollout Progress Chart

Newsbulletin Articles

Related

Ombuds Program
Mediation Center, **7-9367**.

Integrated Safeguards & Security Management
About
Your Voice Counts
Lessons Learned
Requirements
Mgmt Walkarounds
CY00 Rollout

Protecting Info

Personnel

Cyber Security

Nuclear Materials

Internal Security

Facility

General Resources

What is ISSM?

The Laboratory's highly successful Integrated Safety Management (ISM) model is being extended to safeguards and security (or "security," more generally). Laboratory Director John Browne launched this new initiative in early 2000 because ISM's basic tenets—management commitment, worker involvement, line "ownership," clearly defined roles, responsibilities, authorities, and accountability, work and worker authorization, self-assessment, continuous improvement, etc.—are vital to the success of both safety and security at Los Alamos. Pursuing this new initiative—called Integrated Safeguards and Security Management, or ISSM—offers not only a stronger Lab-wide security culture and enhanced security performance, but a unified management model for achieving cost-effective operational excellence (safety and security).

ISSM (like ISM) is not a tangible item, not a plan or a checklist. It is a way of doing business, and the focus of the business is work. Integration means that security is an integral part of all work planning, performance, assessment, and improvement. It's achieved using ISSM's (tailored from ISM's) eight guiding principles and 5-step process. Security requirements alone can't accomplish work or make the work or workplace secure. Security and productivity must be vested in the workforce. Total workforce commitment and involvement are essential for achieving the buy-in and ownership necessary to systematically integrate security into all work practices at all levels so that the Laboratory mission is accomplished cost effectively and safely, while protecting security interests and striving for "zero safeguards & security incidents."

Integrated Safeguards & Security Management
About ISSM
Your Voice Counts
Lessons Learned
Requirements
Mgmt Walkarounds
CY00 Rollout
Protecting Info
Personnel
Cyber Security
Nuclear Materials
Internal Security
Facility
General Resources

ISSM 8 Guiding Principles

The ISSM guiding principles shown below guide all LANL actions aimed at effectively and efficiently performing work securely and achieving a secure workplace. These guiding principles are consistent with those in Appendix O of the UC-DOE contract, guidance from the UC and NNSA, DOE ISSM Policy 470.1, and those in LANL's ISM system description. Note that the first guiding principle has been expanded to reinforce the importance of line-management commitment in addition to worker responsibility and participation as the foundation for all other guiding principles. LANL workers implement these guiding principles by performing their work in a secure manner in accordance with ISSM. They use a degree of care commensurate with the security interests and risks associated with their work and are personally responsible and accountable for performing their work securely.

1. Management Commitment and Worker Responsibility and Participation.
ISSM shall be a worker-based security management system. Each worker (manager and nonmanager) shall be directly responsible for performing work securely, including meeting security requirements and contributing to a secure mission and workplace. Managers shall be visibly committed to the effective and efficient implementation and sustained execution of all ISSM system elements, and workers shall directly participate in developing, implementing, and continuously improving these elements, including understanding and using them in their work.

2. Line-Management Security Responsibility.
Line management shall be directly responsible for protecting all security interests. This includes ensuring security risks are analyzed and that required security controls are in place and verified before accepting residual risk and authorizing work. Every member of the workforce belongs to a line-management organization, which extends in an unbroken chain from external sponsors through the LANL Director to workers "on the floor" (see Section 3.3.). Throughout this line-management chain, security shall be integral to all decisions relating to work performance, including resource allocation, planning, scheduling, and

coordination.

3. Clear Roles and Responsibilities.
LANL shall establish and maintain clear and unambiguous lines of authority, responsibility, and accountability at all organizational levels. These shall be effectively communicated so that everyone understands their individual and organizational roles.

4. Competence Commensurate with Responsibilities.
Every member of the workforce shall possess the experience, knowledge, skills, and abilities necessary to fulfill his/her responsibilities, which is consistent with need-to-know requirements. Supervisors shall ensure that workers are competent to perform their work securely, including meeting security requirements, before authorizing them to perform work.

5. Balanced Priorities.
Management shall effectively allocate resources to address security, safety, programmatic, and operational considerations, knowing that achieving programmatic goals is a significant component of achieving national security. Protecting security interests shall be a priority whenever work is planned and performed. Although different considerations often compete, work shall not be performed unless it can be performed securely, including meeting security requirements.

6. Identified Security Standards and Requirements.
Before work is performed, the associated security risks shall be analyzed and an agreed-upon set of security standards and requirements shall be established, which, when properly implemented, shall provide sufficient assurance that the security interests are properly protected.

7. Work-Tailored Security Controls.
Administrative and physical controls to prevent and mitigate security risks shall be tailored to the work being performed, including the work location and configuration. Emphasis shall be on designing the work and/or controls to reduce or eliminate the security interests and risks. Security controls and safety controls shall be carefully selected to promote mutual benefit and prevent mutual conflict.

8. Authorized Operation.
The conditions and requirements to be satisfied for operations to be initiated and conducted shall be clearly established and agreed upon. Certain operations shall be authorized under the UC-DOE prime management and operations contract, while other operations shall be authorized under activity- and/or facility-level security plans jointly approved by LANL and

NNSA. In all cases, managers shall authorize the work and the workers before work is performed.

Operated by the University of California for the National Nuclear Security Administration, of the US Department of Energy. Copyright © 2002 UC | Disclaimer/Privacy

ISSM 5-Step Process

The ISSM eight guiding principles are essential, but give little detail about how to achieve a secure workplace. Therefore, ISSM uses a five-step process (see Fig. 1) to ensure that security expectations are established, implemented, and measured and reinforced in every work activity. As outlined below, the ISSM five-step process defines a systematic approach to actions taken before, during, and after work is performed.

(1) Define the Scope of Work
Translate mission into work, set expectations (e.g., goals and objectives), identify related security interests, identify potential requirements, identify and prioritize tasks, and allocate resources.

(2) Analyze the Security Risk
Identify the security threats and analyze the security risks associated with the defined scope of work.

(3) Develop and Implement Security Controls
Identify security requirements and develop/implement work-tailored security controls to prevent or mitigate security risks. Line management shall accept residual risk before authorizing work.

(4) Perform Work within Security Controls
Confirm that required security controls are in place and then perform work securely within controls.

(5) Provide Feedback and Continuous Improvement (i.e., Ensure Performance)
Collect feedback information on the sufficiency of security controls; identify/implement

opportunities for improving work definition, planning, and execution; conduct line and independent assessments; reinforce expected behaviors; and share best practices and lessons learned. This includes continually evaluating LANL's overall ISSM system and, as needed, refining it to ensure its effectiveness and efficiency for performing work securely.

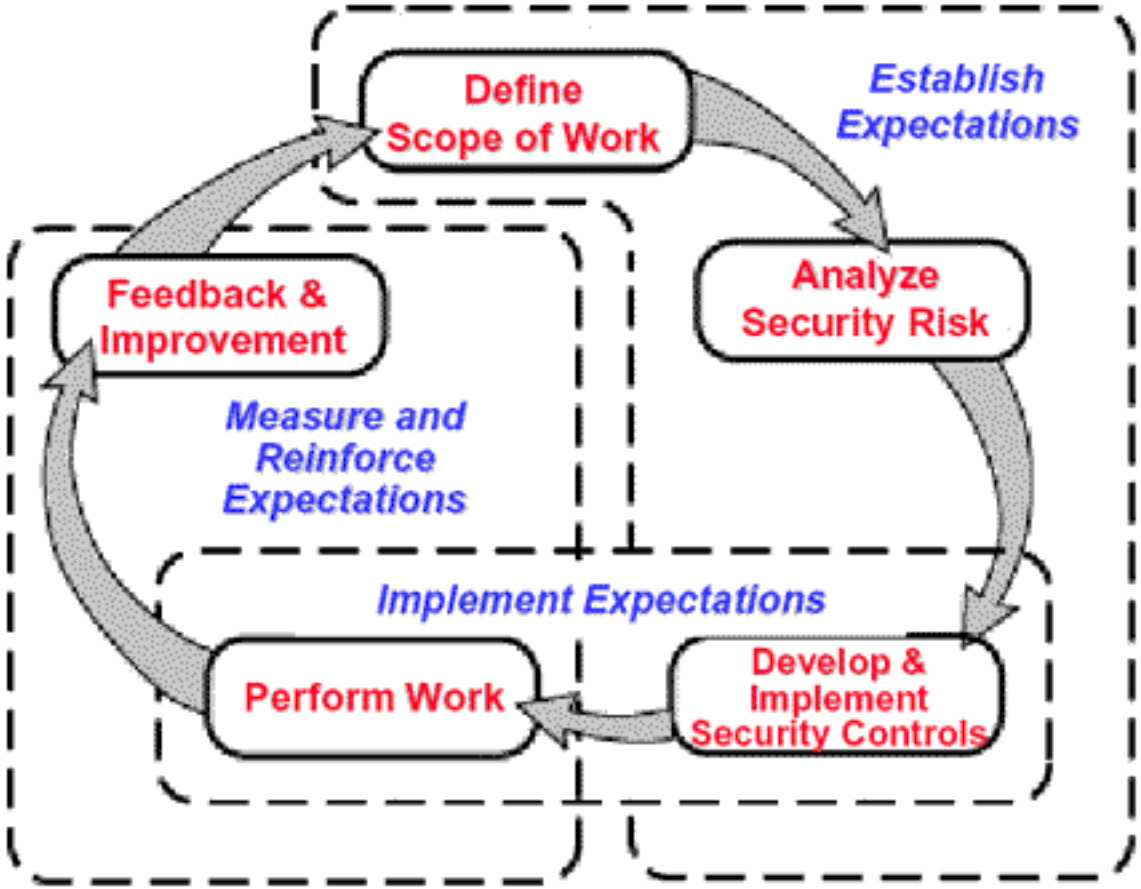


Fig. 1. Relationship between ISSM 5-step process and the three expectations.

Much of what follows is a description of the ISSM system for implementing the eight guiding principles and five-step process.

Meeting Security Expectations

The five-step process applies to all work at LANL, from keyboarding to designing and assembling nuclear criticality-safety experiments. The effort required for applying the five-step process is determined by the nature of the work and the associated security interests and risk.

For work with minimal security risk, the application of the five-step process may be a simple mental exercise at the start of each workday. For example, addressing the risk associated with keyboarding nonsensitive-unclassified information on an unclassified standalone computer may be as simple as ensuring the proper use of passwords for information protection and a

clear understanding of the electronic warning banner.

By contrast, for the design and assembly of nuclear criticality-safety experiments involving large quantities of attractive special nuclear materials such as plutonium or highly enriched uranium, the process may require expert computer-based risk analyses, formal documentation, and third-party review over an extended period.

It is important to note in Fig. 1 that, while the five steps are discrete, their actions overlap. For example, when developing and implementing controls, you may be establishing expectations and implementing physical and/or administrative controls to meet expectations. When you perform work, you may activate the physical controls and see that they are operating properly during the work process.

Application of the Five-Step Process

Figure 2 gives more detail on applying the five-step process. The boxes contain actions typically taken to support each step. The arrows indicate that work begins with some outside direction to take action and that the process is focused on developing a tangible work output. The steps are arranged in a ring to illustrate that this is a process of continuous improvement. It is anticipated that in more complex applications the interrelationships among the different steps may iterate or flow in a different sequence from the directions shown in the figure. The five-step process is the foundation of ISSM and the secure performance of work.

Tailoring Versus Uniformity in Application

LANL is challenged to strike a balance between individual organizations tailoring expectations to their specific facilities and/or activities versus LANL establishing uniform (one-size-fits-all) institutional expectations for all facilities and activities. Tailoring expectations within individual organizations allows flexibility and worker discretion to help ensure: (1) practicable and effective expectations; (2) decision-making at the lowest appropriate level; (3) active worker participation and buy-in; and (4) balanced priorities through integrated risk management. With tailoring, the degree of rigor and formality in documentation, the nature of security controls, and the extent of performance assurance are commensurate with the security interests and risk associated with specific work.

By contrast, uniform institutional expectations offer uniformity in meeting contractual requirements, Labwide application of best business practices, reduced institutional liability and risk, and economy of scale. These benefits are not easily obtained when individual organizations establish tailored expectations that differ between facilities and activities.

To achieve the benefits of tailoring and uniformity, ISSM uses the five-step process to guide individual organizations in creating tailored expectations for specific facilities and activities, while retaining a required level of institutional uniformity - i.e., work-specific tailoring at the activity level and facility-specific tailoring at the facility level, consistent with an overarching set of uniform expectations at the institutional level.

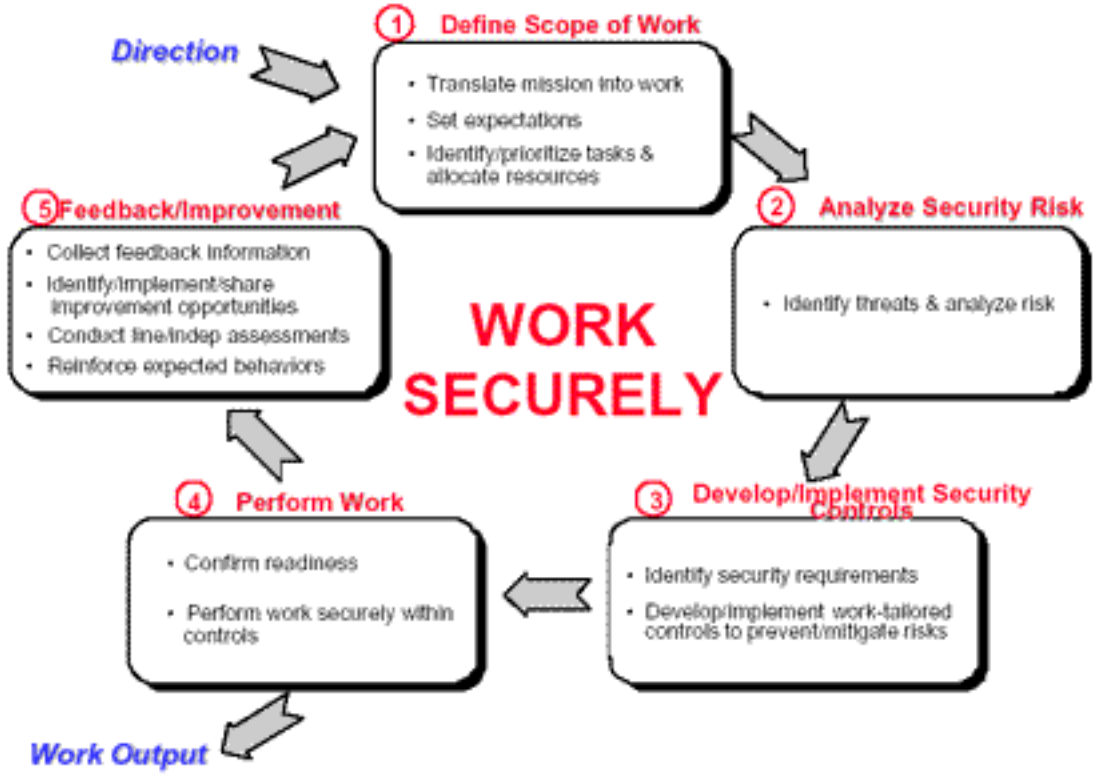


Fig. 2. Laboratory ISSM 5-step process.

Integrated Safeguards & Security Management
About
Your Voice Counts
Lessons Learned
Requirements
Mgmt Walkarounds
CY00 Rollout

Protecting Info

Personnel

Cyber Security

Nuclear Materials

Internal Security

Facility

General Resources

Why Should I Care?

Since April 1999, our Laboratory has gone through a period filled with security briefings, standdowns, and security audits. Changes in policies, procedures, and even the color of badges have helped the Laboratory tighten down the hatches and firm up its security practices.

In January 2000, Energy Secretary Bill Richardson reported that new security policies, a series of tough audits, and major increases in funding brought security at our Laboratory and other DOE facilities to a level that should inspire the confidence of U.S. citizens. Secretary Richardson felt that because of notable improvements, the country's secrets were again safe and secure.

However, in early June 2000, the Laboratory experienced a security incident involving missing hard drives, which brought the Laboratory much negative attention. As a result, Laboratory Director John Browne directed several immediate actions. The success of these actions and those that follow depends vitally on our individual and collective security awareness and unconditional commitment to the goal of "zero safeguards & security incidents."

To this end, ISSM is official Laboratory policy. It will provide a framework that supports and is to be followed by the entire workforce to help fulfill our individual and collective security responsibilities. As with ISM for safety, ISSM will be the single security management system that sets security policy for all people performing work at the Laboratory, irrespective of

CONTACTS

Security Help Desk
665-2002

RELATED LINKS

Laboratory performance requirement (LPR)

employer. ISSM will require that all work and all workers meet the security requirements defined by the Laboratory requirements system, as documented in the ISSM Laboratory performance requirement (LPR), ISSM Laboratory implementation requirements (LIRs), and any supplemental requirements defined for a specific facility and/or activity.

Once ISSM is fully implemented, every worker will be aware of the security risks associated with their work and workplace, and have confidence in their mitigation. This includes being able to respond positively and confidently to the following questions:

1. **Do you perform your work securely?**
2. **How do you know?**
    - Do you know the security requirements governing your work/workplace and how they are being met?
    - Do you know the security risks in your work/workplace and whether controls are sufficient to mitigate them?

If you are currently unable to answer these questions, you should discuss them with your supervisor. Also, the designated security representatives (OSSOs, OCSRs, ADCs, NM Custodians, etc.) in your organization are a valuable resource for you. Additionally, S-Division, ISEC, and CIO-Cyber Security are support organizations at your service, including the new "one-stop shopping" Security Help Desk, which can be reached at **665-2002** or by e-mailing your unclassified (and non-sensitive) security questions, concerns, and suggestions to security@lanl.gov.

 Copyright © 2002 UC | Disclaimer/Privacy

Integrated Safeguards & Security Management
About
Your Voice Counts
Lessons Learned
Requirements
Mgmt Walkarounds
CY00 Rollout

Protecting Info

Personnel

Cyber Security

Nuclear Materials

Internal Security

Facility

General Resources

ISSM Objective

The objective of ISSM at LANL is to systematically integrate security into all management and work practices at all levels so that LANL's mission is accomplished securely by protecting security interests and always striving for "zero safeguards and security incidents" (see LANL Safety and Security Policy). (Note: "zero safeguards and security incidents" means preventing actual and potential compromises to security interests and national security and meeting all applicable security requirements.) This is achieved through effective and efficient integration of security into all facets of work planning, performance, assessment, and improvement. **Security is the responsibility of every member of the workforce.**

Integrated Safeguards & Security Management
About
Your Voice Counts
Lessons Learned
Requirements
Mgmt Walkarounds
CY00 Rollout

Protecting Info

Personnel

Cyber Security

Nuclear Materials

Internal Security

Facility

General Resources

Safety and Security Policy

Safety and Security Policy

"We will never compromise safety or security for programmatic or operational needs."

We are committed to achieving excellence in environmental, safety, health, and security performance.

To meet the **moral imperative** not to injure people, the environment, or compromise the safety of our nation while accomplishing our mission, and the **business imperative** to meet the environmental, safety, health, and security requirements of the contract between the University of California and the Department of Energy, the employees, contractors, and guests of the Los Alamos National Laboratory will always strive to have:

- **ZERO injuries and illnesses on the job**
- **ZERO safeguards and security incidents**
- **ZERO injuries and illnesses off the job**
- **ZERO environmental incidents**
- **ZERO ethics incidents**
- **ZERO people-mistreatment incidents**

Los Alamos
NATIONAL LABORATORY

Integrated Safeguards & Security Management
About
Your Voice Counts
Lessons Learned
Requirements
Mgmt Walkarounds
CY00 Rollout

Protecting Info

Personnel

Cyber Security

Nuclear Materials

Internal Security

Facility

General Resources

Draft ISSM System Description

This latest draft ISSM system description was developed by the Joint LANL-NNSA ISSM Steering Team, which is led by LANL with cross-directorate and NNSA/LAAO membership. It has benefited from extensive Labwide input since the first draft was issued in July 2000 at the start of LANL's ISSM rollout. It incorporates the ISSM expectations in Appendix O of the UC-DOE contract approved January 18, 2001, consistent with recent guidance from the UC and the NNSA, DOE ISSM Policy 470.1 issued May 8, 2001, and LANL's ISM system description. This document will continue to be updated as ISSM matures to reflect lessons learned and process improvements. Always, gains in effectiveness and efficiency must be basic to our thinking as we strive to improve the security of day-to-day operations. Comments on this document can be sent to security@lanl.gov.

Draft ISSM System Description (pdf) (05-31-01)

Integrated Safeguards & Security Management
About
Your Voice Counts
Lessons Learned
Requirements
Mgmt Walkarounds
CY00 Rollout
Protecting Info
Personnel
Cyber Security
Nuclear Materials
Internal Security
Facility
General Resources

Glossary

Security, when used generically, encompasses all aspects of protecting all LANL-controlled safeguards (i.e., nuclear materials-related) and security interests commensurate with defined security threats and associated risk, and consistent with applicable security requirements.

Security interests include LANL-controlled classified and sensitive- unclassified matter, nuclear materials (in particular, special nuclear materials and tritium), and other government resources associated with accomplishing the LANL mission.
Safety, when used generically, encompasses all aspects of environment, safety, and health (ES&H), including regulatory requirements, pollution prevention, and waste minimization.

Work is defined broadly to include all LANL activities undertaken by the workforce, including work-for-others (WFO) activities. Activities undertaken during emergencies should be done as safely and securely as possible, consistent with the nature of the emergency. Emergency actions may be taken outside of the documented requirements of ISM and ISSM.

Worker is any person who performs work at LANL (whether on LANL's DOE-owned, leased, or rental property), including UC employees, subcontractors, vendors, external organization employees, affiliates, and official visitors. See Section 3.0.

Risk refers to the likelihood and potential severity of theft, loss, and/or unauthorized disclosure of security interests by security threats (internal and/or external personnel) committing intentional or unintentional acts; for the purpose of this document, a qualitative judgment based on knowledge and experience, except where quantitative risk analysis is required.

Controls are physical (e.g., security fences) and/or administrative (e.g., access authorization) measures to prevent or mitigate a threat from causing harm to security interests and national security. Security controls and safety controls should be carefully selected to promote synergy (mutual benefit) and to avoid conflict.

Tailoring means the physical and/or administrative controls and other measures to prevent or mitigate security risk are tailored (vs. one size fits all) to the work being performed, including its environment (location and configuration). Emphasis is on designing the work and/or controls to reduce or eliminate the security interests and associated risk to prevent compromises of security interests and national security. With tailoring, the degree of rigor and formality in documentation, the nature of security controls, and the extent of performance assurance are commensurate with the security interests and risk associated with specific work.

Need to know requires a determination by the person(s) having responsibility for specific classified matter, including information, material, and/or equipment, that a prospective recipient's access to such classified matter is necessary in the performance of his/her official or contractual duties of employment.

Operated by the University of California for the National Nuclear Security Administration, of the US Department of Energy. Copyright © 2002 UC | Disclaimer/Privacy

Integrated Safeguards & Security Management
About
Your Voice Counts
Lessons Learned
Requirements
Mgmt Walkarounds
CY00 Rollout
Protecting Info
Personnel
Cyber Security
Nuclear Materials
Internal Security
Facility
General Resources

2000 - 2001 Safeguards & Security Refresher Briefing

The Safeguards & Security Refresher Briefing may be used to meet your annual security training requirements and as an on-line resource document.

To Obtain TRAINING credit

If you are reading the booklet to meet your annual security training requirements, it must be accessed through the Virtual Training Center . Credit for completion of this training will only be recorded through the Virtual Training Center. Go to Virtual Training Center/Safeguards & Security Training/Required Security Courses.

Features of the ON-LINE PDF Version

The information contained in the Safeguards & Security Refresher Briefing can be used as a handy quick reference document. The on-line version of this document is set up in a tabbed format in order for you to tab section by section, or if you prefer, use the sidebar page listing to go directly to a specific page.

The booklet in .PDF version allows you to search the contents for specific topics. Simply use the FIND option (CTRL-F) located in the Tools pull down menu.

Online Reference Document

Operated by the University of California for the National Nuclear Security Administration, of the US Department of Energy. Copyright © 2002 UC | Disclaimer/Privacy

LANL External View | security-www@lanl.gov
Security Help Desk: security@lanl.gov
Last Modified: 12/04/01

Integrated Safeguards & Security Management
About
Your Voice Counts
Lessons Learned
Requirements
Mgmt Walkarounds
CY00 Rollout
Protecting Info
Personnel
Cyber Security
Nuclear Materials
Internal Security
Facility
General Resources

Target Audience Identification

The Laboratory's population of "current workers" varies throughout the year. At any given time, a group leader will have personnel assigned to his/her group who are not physically present at the Laboratory, for example, students, affiliates, etc. The method described below allows the Group level manager, or a designee, to selectively identify members in his/her group for a training requirement or event. In this case, for the Introduction to ISSM: "Enhancing Our Security Awareness Commitment and Performance: ISSM." The process for audience identification will result in the assignment of a training plan used to track completion of the workshops.

Only the Group or Division-level Manager, or designee with the EDGroup authority, are authorized to identify and validate the target audience for their organization using this process.

For assistance with audience identification or the questionnaire, call S-Division Training at **5-4496 or 5-7844,** or contact your Division Training Generalist. For assistance with authorities, contact CIC Customer Service at **5-4444**,

---

Procedure for Audience Identification

1. **Print this page.** The instructions below will not be readily accessible once you have clicked on the link in Step #2.

2. Link to: http://tq.lanl.gov/

3. Select GROUP TRAINING QUESTIONNAIRE and log in using your Smartcard/Cryptocard.

4. Select the names of all group members you wish to identify for the workshops. (See instructions to the left of the scroll box to select more than one name or skip individuals.) The

only exceptions will be staff who are not physically on-site at this time (and will not be through the end of August). This might include:

- Visiting faculty, staff on change of station, staff on leave of absence, students who are away.
- Any questions about who to include should be directed to the Division HR Generalist.

5. Click OK and the questionnaire will open

6. Verify that all the workers you identified are on the list. If you have made an error, click on the TQ HOME button in the upper left hand corner and reselect the Group Training Questionnaire.

7. Click in the Validation box and scroll to the bottom of the page to click APPROVE. **IMPORTANT NOTE:** DO NOT answer any other questions on the questionnaire. Doing so will override any current training plan assignments. Once names are submitted corrections must be made in the Employee Information System. If you need assistance with this, contact your Division Training Generalist.

Operated by the University of California for the National Nuclear Security Administration, of the US Department of Energy. Copyright © 2002 UC | Disclaimer/Privacy

Integrated Safeguards & Security Management
About
Your Voice Counts
Lessons Learned
Requirements
Mgmt Walkarounds
CY00 Rollout
Protecting Info
Personnel
Cyber Security
Nuclear Materials
Internal Security
Facility
General Resources

Attendance Collection

Participation in the ISSM workshops is mandatory for all current workers at Los Alamos National Laboratory. Attendance will be tracked using the Virtual Training Center and the Employee Development System (EDS).

Management may select one of the following options for collecting this data:

- Individual workers may submit for credit on the Virtual Training Center

  NOTE: The user of a SmartCard/CryptoCard will allow an individual to receive immediate credit. A request for credit without the use of a a SmartCard/CryptoCard will take 3-5 days to be credited, or
- Group administrators may submit workers for credit on the Virtual Training Center using the standard, Request for Credit.
- Group offices should circulate hard copy rosters at the group-level workshops. The final roster should be maintained at the group office.

Attendance Reports

In order to track completion of the ISSM workshops, a number of reports may be generated. The following reports are suggested, however, you should consult with your Division Training Generalist for assistance with more detailed reports.

Employee Development System (EDS)—In the IB System

- TPQ report—identifies individual workers who have not met the training requirements
- TPG report—identifies all workers by group and their training status for this requirement. (complete/incomplete)

Employee Development System (EDS)—In Data Warehouse Quick Reports

- Training Plan Overview—run this for Plan # 4519 and your organizational code (6 digit code, e.g., 7E0000)

Attendance Rosters

Online EDS Credit submission

Official Laboratory Training Roster (Form 1651)

Continuation of Training Roster (Form 1651con)

Operated by the University of California for the National Nuclear Security Administration, of the US Department of Energy. Copyright © 2002 UC | Disclaimer/Privacy

LANL External View | security-www@lanl.gov
Security Help Desk: security@lanl.gov
Last Modified: 12/04/01

Integrated Safeguards & Security Management
About
Your Voice Counts
Lessons Learned
Requirements
Mgmt Walkarounds
CY00 Rollout

Protecting Info

Personnel

Cyber Security

Nuclear Materials

Internal Security

Facility

General Resources

Responses to ISSM Workshop Questions, Concerns, and Suggestions

	Date	Volume/Number
	01-18-2001 NEW!	ISSMv1n2
	12-12-2000	ISSMv1n1

Integrated Safeguards & Security Management
About
Your Voice Counts
Lessons Learned
Requirements
Mgmt Walkarounds
CY00 Rollout
Protecting Info
Personnel
Cyber Security
Nuclear Materials
Internal Security
Facility
General Resources

Newsbulletin Articles

Date	Title
10/26/2000	Promoting positive security behaviors
10/19/2000	A great start for Integrated Safeguards and Security Management
07/17/2000	Tuesday's all-hands meeting to feature five-step process for enhancing security performance at the Laboratory

S-DO: Security & Safeguards Division Office
S-1: Security Plans and Programs
S-2: Security Integration
S-3: Security Systems
S-4: Material Control & Accountability
S-5: Security Support
S-6: Personnel Security
S-7: Classification
S-8: Emergency Management & Response
S-OSI: Office of Security Inquiries

Questions? Concerns? Call the Security Help Desk 5-2002

A lessons learned is an experience from the past you can use to improve the future.You can learn about lessons learned tools and resources in a short informational video or by visiting the Lessons Learned Resources site.

These tools and resources will help you find and share operating experience information that can lead to faster, safer, more secure ways to do your work.

Our site is in the process of being updated.

For the latest security related information, please go to http://int.lanl.gov/security/. This new site combines S Division's content with information from Internal Security (ISEC) and Cyber Security (CIO-CS).

This site is limited to S Division

If you're having difficulty finding the information you need, please contact the Security Help Desk at **665-2002**. If you have web site-related comments, please contact the security web team.

CONTACTS

Emergency - 911 or 667-6211

Emergency Management & Response: 667-6211

Security Help Desk: 665-2002

Cyber Security (CIO-CS): 665-1795

Internal Security (ISEC): 665-6090

Protection Technology Los Alamos: 667-4437

Security & Safeguards Division: 667-5911

Badge Office: 667-6901

Clearances: 667-7253

Lab Security Organizations

PROTECTION TECHNOLOGY Los Alamos

Pro-Force Staffing Request
Suggestions@lanl.gov

S-DO: Security & Safeguards Division Office
S-1: Security Plans and Programs
S-2: Security Integration
S-3: Security Systems
S-4: Material Control & Accountability
S-5: Security Support
S-6: Personnel Security
S-7: Classification
S-8: Emergency Management & Response
S-OSI: Office of Security Inquiries

Questions? Concerns?
Call the Security Help Desk 5-2002

S-DO Security & Safeguards Division Office

Mission

S Division supports the Laboratory organizations' efforts to comply with and implement Department of Energy Safeguards and Security orders and regulations by developing integrated S&S plans, training, security assistance visits, self-assessments, and corrective action planning and closure. Using the data obtained through daily customer interactions S Division seeks to continually improve its program plans and the effectiveness of S&S at the Laboratory.

- Management Philosophies
- Value-Based Leadership Principle
- Organization Chart
- Strategic Plan
- Integrated Safety Management Plan

Division Office Services & Teams:

Business

Computer Services

CONTACTS

Division Leader:
Stanley Busboom

Deputy Division Leader:
John E.(Gene) Tucker

Program Manager:
Kevin Leifheit

Chief of Staff:
Carol Estes

Nuclear Safeguards Assurance:
Carl Ostenak

Division Office Info
Phone: 7-5911
Fax: 5-3810
Mailstop: G729
Location: TA-3, SM-468, rm.117

Division Office Admin:
Janelle Armendariz

Group Roster

Operated by the University of California for the National Nuclear Security Administration, of the US Department of Energy. Copyright © 2002 UC | Disclaimer/Privacy

S-DO: Security & Safeguards Division Office
S-1: Security Plans and Programs
S-2: Security Integration
S-3: Security Systems
S-4: Material Control & Accountability
S-5: Security Support
S-6: Personnel Security
S-7: Classification
S-8: Emergency Management & Response
S-OSI: Office of Security Inquiries

S-1 Security Plans & Programs

Mission

Our mission is to:

- provide a consistent and effective voice for safeguards and security programmatic planning in support of LANL technical, scientific and operational directorates for Strategic Research (SSR), Threat Reduction (TR), Weapons Engineering & Manufacturing , Weapons Physics as well as Operations (ADO).
- assess and analyze security threats / risks and vulnerabilities for selected LANL operations in accordance with DOE design basis threat guidance.
- compile and publish LANL's Site Safeguards and Security Plan
- coordinate safeguards and security strategic, business, functional planning.
- provide S Division line groups with planning support, including integration of safeguards and security support for mission change and construction projects.

Strategic Planning Team
Cam Campbell, Team Leader

- Provide a single voice to the programmatic stakeholders for safeguards and security support to mission change and construction projects.

CONTACTS

Group Leader:
Bill Gillison

Group Office Info
Phone: 7-0558
Fax: 5-5143
Mailstop:G728
Location: TA-3, SM- 496, rm.101B

Office Admin:
Lynn Wysocki-Smith

Group Roster

Questions? Concerns?
Call the Security Help Desk 5-2002

- Write, coordinate, and publish S Division strategic plan and safeguards and security elements of other Laboratory plans.
- Ensure linkage and interface of the Site Safeguards and Security Plan and the S Division strategic plan, S Division group functional and business plans, the S Division budget process and other Laboratory safeguards and security planning.
- Compile and publish the Site Safeguards and Security Plan.

Site Safeguards and Security Plan (SSSP) Vulnerability Analysis Team
Ralph Garcia, Team Leader

- Integrate analysis and threat and risk assessments into a jointly prioritized SSSP process involving LANL, OLASO, AL and HQ DOE utilizing the LANL SSSP Change Control Board Process.
- Conduct, analyze, and publish Vulnerability Analyses (VAs) for selected programmatic work using "ASSESS", the Joint Conflict and Tactical Simulation Laboratory " JCATs" and Joint Tactical Simulation "JTS" and other NNSA approved analytical modeling tools.
- Compile force on force exercise validation data for VA modeling results and analysis.
- Provide required analysis, format, content and guidance for the LANL Site Safeguards and Security Plan.
- Conduct, analyze and publish special facility security plans (SFSP)

Nuclear Materials Safeguards and Security Upgrades Project (NMSSUP)
Kirk O. Ellard, Project Manager

- Manage the NMSSUP project.

Operated by the University of California for the National Nuclear Security Administration, of the US Department of Energy. Copyright © 2002 UC | Disclaimer/Privacy

security-www@lanl.gov | Last Modified: 01/25/02

S-DO: Security & Safeguards Division Office
S-1: Security Plans and Programs
S-2: Security Integration
S-3: Security Systems
S-4: Material Control & Accountability
S-5: Security Support
S-6: Personnel Security
S-7: Classification
S-8: Emergency Management & Response
S-OSI: Office of Security Inquiries

S-2 Security Integration

Our mission is to provide a consistent and effective voice for interface with LANL line divisions (NMT, DX, ESA, etc.). Consolidate and coordinate the efforts of the S Division line groups to deploy their security products and requirements into the laboratory line management. Set standards for program management and assess against them, managing any identified deficiencies in coordination with the line group.

- **Organizational Support Team**
  Staff the Security Helpdesk. Provide guidance and oversight for LANLs DSO program.
- **Standards Team**
  Write and/or review all security related documentation. Coordinate all assessment and performance testing activity. Provide Protective Force (PTLA) oversight. Manage the UC Performance Measures.
- **Training & Comunications Team**
  Develop all security related training and communication products.

CONTACTS

Acting Group Leader:
Darryl Overbay

Group Office Info
Phone: 7-7565
Fax: 7-3388
Mailstop: K560
Location: TA-52, SM- 1, rm. 219

Office Admin:
Johanna Lopez

Group Roster

Questions? Concerns?
Call the Security Help Desk 5-2002

S-DO: Security & Safeguards Division Office
S-1: Security Plans and Programs
S-2: Security Integration
S-3: Security Systems
S-4: Material Control & Accountability
S-5: Security Support
S-6: Personnel Security
S-7: Classification
S-8: Emergency Management & Response
S-OSI: Office of Security Inquiries

S-3 Security Systems

Mission

Design, install, and maintain cost-effective physical security systems that provide detection and deterrence of malevolent actions. Develop, implement, and maintain the software systems that protects Nuclear Material and control intrusion detection.

Security System Topics

- Access Control Systems
- Access Area Vault and VTR Training
- Fire Protection Integration
- Interior Intrusion Detection Systems
- Perimeter Intrusion Detection Systems
- FAQ & Trouble Shooting

CONTACTS

Group Leader:
Bill Sole

Group Office Info
Phone: 7-7873
Fax: 5-8477
Mailstop: G725
Location: TA-3, SM-440, rm.103

Office Admin:
Vacant

Group Roster

Questions? Concerns?
Call the Security Help Desk 5-2002

S-DO: Security & Safeguards Division Office
S-1: Security Plans and Programs
S-2: Security Integration
S-3: Security Systems
S-4: Material Control & Accountability
S-5: Security Support
S-6: Personnel Security
S-7: Classification
S-8: Emergency Management & Response
S-OSI: Office of Security Inquiries

S-4 Material Control & Accountability

Mission

The mission of the Materials Control and Accountability (MC&A) Group is to provide Safeguards and Security program support, and to ensure effective accountability and control of nuclear materials at the Laboratory. It ensures Laboratory compliance to DOE orders and requirements and the UC contract in a cost-effective manner supplying guidance, support and oversight using an integrated team approach and technically driven solutions. It also promotes professional growth and recognition among the staff.

Also See:

- Nuclear Materials
  - Nuclear Materials Accountability
  - Nuclear Materials Control
  - Nuclear Materials Measurement

CONTACTS

Group Leader:
Steven Croney

Group Office Info
Phone: 7-5886
Fax: 5-5566
Mailstop: G735
Location: TA-3, SM- 513, rm.124

Office Admin:
Frances Montoya

Group Roster

Questions? Concerns?
Call the Security Help Desk 5-2002

S-DO: Security & Safeguards Division Office
S-1: Security Plans and Programs
S-2: Security Integration
S-3: Security Systems
S-4: Material Control & Accountability
S-5: Security Support
S-6: Personnel Security
S-7: Classification
S-8: Emergency Management & Response
S-OSI: Office of Security Inquiries

Questions? Concerns?
Call the Security Help Desk 5-2002

S-5 Security Services

Mission

Our mission is to establish Laboratory standards for the protection of classified interests; to provide operational oversight of physical protection at the Laboratory that includes protection of special nuclear material and facilities, classified matter and government property; and to ensure strong and responsive security support to Laboratory organizations in their implementation of orders and regulations.

Information Security Team

- Classified Matter Protection Control

Physical Security

- Cellular Phones
- Video Teleconference Systems
- Crypto (KG, STU, NES)
- Tempest
- TSCM (Technical Security Countermeasures)
- Vault & VTR Information (Manual and all associated forms, lists, logs, etc.)
- Escorting

CONTACTS

Group Leader:
Leigh Barnes

Group Office Info
Phone: 5-8756
Fax: 5-0432
Mailstop: G733
Location: TA-3, SM-512, rm.138

Office Admin:
Louise Rodriguez

Group Roster

S-DO: Security & Safeguards Division Office
S-1: Security Plans and Programs
S-2: Security Integration
S-3: Security Systems
S-4: Material Control & Accountability
S-5: Security Support
S-6: Personnel Security
S-7: Classification
S-8: Emergency Management & Response
S-OSI: Office of Security Inquiries

S-6 Personnel Security

Our mission is to be proactive and innovative in maintaining cost-effective performance-based systems for the protection, accountability, and control of national security assets / interests and government property while supporting the Laboratory's scientific and technology programs. S-6 serves our customers in the areas of Access Control, Personnel Security, Foreign Visits and Assignments, Security Education, Information Security and Counterintelligence.

- Badge Office
- Clearance Processing
- Personnel Security Assurance Program (PSAP)

CONTACTS

Group Leader:
Larry Freestone

Group Office Info
Phone: 5-6565
Fax: 5-4999
Mailstop:G733
Location: TA-3, SM- 512, rm.132

Office Admin:
Denise M Tiede

Group Roster

Questions? Concerns?
Call the Security Help Desk 5-2002

S-DO: Security & Safeguards Division Office
S-1: Security Plans and Programs
S-2: Security Integration
S-3: Security Systems
S-4: Material Control & Accountability
S-5: Security Support
S-6: Personnel Security
S-7: Classification
S-8: Emergency Management & Response
S-OSI: Office of Security Inquiries

S-7 Classification

Mission

The Group's main mission is to correctly identify information that requires protection in the interest of national security, balanced with the requirement to properly disseminate the Laboratory's scientific and technical information to the maximum extent possible, consistent with the common defense and security. Specifically, classification is the process of determining and identifying the information to be protected, and is distinct from security...the mechanism for protecting classified or other sensitive information identified.

The Group's mission to process and account for the Laboratory's publications is integrally linked with its mission to balance the need for the protection of certain information with the need for maximum dissemination of information -- both of which are in the national interest. Accomplishment of these missions, simultaneously and efficiently satisfies a number of diverse DOE requirements.

The Group's final mission is to satisfy DOE requirements for accountability for the benefits of foreign travel by the Laboratory's staff.

Also see:

- the Classification web site

CONTACTS

Group Leader:
Jay Brown

Deputy Group Leader:
Mark Jones

Group Office Info
Phone: 7-5011
Fax: 5-4251
Mailstop: F674
Location: TA-3, SM- 43, rm.A116 (SW wing of Ad Bldg., ground floor)

Office Admin:
Mable Salazar

Group Roster

Questions? Concerns?
Call the Security Help Desk 5-2002

S-DO: Security & Safeguards Division Office
S-1: Security Plans and Programs
S-2: Security Integration
S-3: Security Systems
S-4: Material Control & Accountability
S-5: Security Support
S-6: Personnel Security
S-7: Classification
S-8: Emergency Management & Response
S-OSI: Office of Security Inquiries

S-8 Emergency Management & Response

S-8 is the Laboratory's core organization which provides Laboratory-wide emergency plans, preparedness programs, and oversight capability to respond to and mitigate ALL LANL emergencies with the objective of minimizing harm to employees, contractor personnel, and the general public and to limit negative impacts or damage to the environment and property. In accordance with DOE, UC, and LANL guidance and directives, we establish and maintain requirements necessary for an effective and efficient emergency management program to minimize adverse affects of any type of emergency which may occur at LANL. As such, our mission is:

"Emergency Management & Response supports the Laboratory mission as its center of excellence for Emergency Management, Emergency Planning, Emergency Preparedness, and Emergency Response."

Also See:

- EM&R website

CONTACTS

Group Leader:
George Van Tiem

Group Office Info
Phone: 7-6214
Fax: 7-7770
Mailstop: K493
Location: TA-59, SM-97, rm. 303B

Office Admin:
Mary Darling

Group Roster

Questions? Concerns?
Call the Security Help Desk 5-2002

S-DO: Security & Safeguards Division Office
S-1: Security Plans and Programs
S-2: Security Integration
S-3: Security Systems
S-4: Material Control & Accountability
S-5: Security Support
S-6: Personnel Security
S-7: Classification
S-8: Emergency Management & Response
S-OSI: Office of Security Inquiries

Questions? Concerns?
Call the Security Help Desk 5-2002

S-OSI Office of Security Inquiries

The mission of the Office of Security Inquiries is to provide expertise for a broad range of Security & Safeguards projects, inquiries, and reports of interest to the Laboratory. These include, but are not limited to: property loss, vandalism/unauthorized tampering, illegal/controlled substance, threats and/or harassment, law enforcement liaison, security for public meetings, security coordination for protests/demonstrations, violence in the work place, pornography issues, the Drug Detection/Deterrence program, incidents of security concern, security badge retrieval, Very Important Person (VIP) visitor protection, Pride Line, and oversight of the National Parks Service contract. This office is at the immediate service of the Security & Safeguards Division Leader, and Laboratory senior management to conduct confidential inquiries as requested.

The Office of Security Inquiries also provides oversight and direction for the Laboratory's Property Protection Program, the Parking Program, as well as the Security & Safeguards On-Call Program.

VIP Visitor Protection:
This office provides coordination/protection to very important persons who visit the Laboratory at the request of senior management or visiting dignitary.

Security Coordination for Protests and or Demonstrations:

CONTACTS

Office Leader:
Glenn A. Walp

Group Office Info
Phone: 5-3505
Fax: 7-7579
Mailstop: G723
Location: TA-3, SM-470, rm.121

Office Admin:
Becky Rodriguez

Group Roster

000695

This office is responsible for coordination and implementation of expanded security procedures for protests/demonstrations on Laboratory property.

Law Enforcement Liaison:
This office provides liaison for all law enforcement agencies (federal, state, county, local, and tribal) that have a need to conduct business on Laboratory property i.e., conduct interviews, make arrests, serve legal documents etc.

Security for Public Meetings:
This office provides or arranges for security for public meetings on or off site as required.

Pride Line (7-7433) Inquiries:
This office conducts appropriate inquiries into reports of criminal activity via the Pride Line contact.

Oversight of Random Property/Prohibited Article Searches:
This office provides oversight and assistance for the random property/prohibited article searches conducted by PTLA.

Security Badge Retrieval:
This office provides assistance to Laboratory supervisors in retrieving security badges when employees ex-employees and/or contractors refuse to turn in their security badges.

Parking Enforcement Program:
This office provides oversight and direction for the LaboratoryÃs Parking Program, including the hearing officer.

Security & Safeguards On-Call Program: This office provides oversight and direction for the Safeguards and Security On-Call Program, to include scheduling.

This office conducts inquiries into:

- Theft

- Harassing/Threatening Letters and Phone Calls:
- Vandalism/Unauthorized Tampering
- Illegal/Controlled Substance
  - conducts inquiries into incidents of use possession or trafficking on Laboratory property
- Property Protection Program
  - provides guidance and assistance for protection of government property at the Laboratory
- Drug Detection/Deterrence Program
  - manages and schedules the random drug dog searches throughout the Laboratory
- Incidents of Security Concern
  - conducts inquiries into any unusual incidents that may be deemed a security concern

---

Operated by the University of California for the National Nuclear Security Administration, of the US Department of Energy. Copyright © 2002 UC | Disclaimer/Privacy

security-www@lanl.gov | Last Modified: 12/18/01

Los Alamos National Laboratory

ISSM Project Plan

(December 13, 2001)

Donald D. Cobb
LANL ISSM Champion and
Associate Director for Threat Reduction

Los Alamos National Laboratory
ISSM Project Plan

I. INTRODUCTION

Los Alamos National Laboratory (LANL) is totally committed to accomplishing its crucial national security mission in a safe, secure, reliable, and cost-effective manner. To this end, LANL Director John Browne launched Integrated Safeguards and Security Management (ISSM) in January 2000, modeling it after Integrated Safety Management (ISM) -- i.e., line ownership, active worker involvement, clearly defined roles/responsibilities, continuous improvement, etc.

Following this lead, in August 2000 the University of California (UC) proposed to the U.S. Department of Energy (DOE) an initiative to strengthen management and performance of safeguards and security (S&S) at LANL and LLNL to ensure that S&S is an integral and visible part of work planning and execution. To this end, both Labs have committed to putting ISSM "in place" by December 31, 2002, consistent with contractual expectations (Appendix O) established January 18, 2001, between the UC and DOE. A critical success factor is that every worker must assume personal responsibility for performing their work securely and contributing to a secure workplace to help ensure national security.

This *LANL ISSM Project Plan* resulted from a series of activities that began when the UC, LANL, and LLNL adopted the ISSM Guiding Principles contained in the DOE Policy statement on ISSM. Criteria were then developed by UC, Aegis, and the two Labs to assist in determining how the Guiding Principles would apply in the work environment. Applying the criteria to the current S&S program processes and soliciting input from the entire LANL workforce yielded a clear picture (see *LANL* ISSM *Gap Analysis* submitted to UC on August 17, 2001) of where the Lab stood relative to achieving the ISSM objectives. Several opportunities for S&S improvement were identified.

The *Gap Analysis* served as the basis for the *LANL ISSM Action Plan*, which identified seven major tasks for addressing the S&S improvement opportunities. The *Action Plan* also described the completion criteria for each of these tasks. It was submitted to UC on September 23, 2001, and recently approved by NNSA. While the *Action Plan* served as the top-level document describing what is required to put ISSM in place, a subordinate plan was needed to identify in more detail how the tasks would be done and the schedule and resources required to do them. This *Project Plan* is intended to accomplish that purpose and is fully responsive to the guidance provided by UC.

It should be emphasized that while Appendix O requires UC to verify that ISSM is "in place" at both Labs as of December 31, 2002, and while this *Project Plan* deals with those tasks required to achieve that objective, LANL will continually seek ways to enhance its S&S performance well

beyond 2002. Always, gains in effectiveness and efficiency will remain basic to our thinking as we strive to improve the security of day-to-day operations. Moreover, we will sustain "top-down" leadership and active "bottom-up" participation to achieve the buy-in and ownership necessary for success. Extensive workforce involvement, including active solicitation of worker and manager input and feedback, will continue to be the foundation of LANL's ISSM journey.

II. ASSUMPTION

This plan and program schedule are based on the Lab having fixed target funding and workload for fiscal year 2002. Any major changes or disruptions in either funding or workload could result in reprioritization and schedule changes.

III. INDIVIDUAL "WORD" TASK SUMMARIES & "PROJECT" DATA SHEETS

The following "Microsoft Word" pages describe the seven major tasks (one page each), including key milestones, for achieving the NNSA-approved LANL ISSM Action Plan and building on ISSM accomplishments to date for putting ISSM in place. The more detailed "Microsoft Project" data sheet(s) corresponding to each of the seven tasks are shown after each one-page task summary.

Task A1: S&S Training and Awareness

Task Leaders: Bob Lopez/S-2 & Kim Thomas/C-DO
(Plus input/feedback from cross-directorate ISSM Steering Team & LLNL collaboration.)

Description: To enhance worker and management S&S training; to enhance awareness mechanisms other than training.

Objective: To increase awareness of ISSM responsibilities and resources.

Deliverables: Documentation of individual S&S training modules and awareness mechanisms, and of an integrated S&S training and awareness plan.

Completion Criterion: Production of deliverables.

Major Activities to be Accomplished:

Prior to 12/31/02:

- Develop/deploy an integrated S&S Training & Awareness Plan based on focus team input (users and SMEs);
- Enhance current web-based and "live" worker and manager S&S training modules (e.g., GET, ASR, RMT, CMPC, NM Handler, Access Custodian/User, Escorting);
- Develop/deploy new web-based and "live" worker and manager S&S training modules (e.g., SUI, ADC, CREM, SPL/DSO, S&S threats/risk management);
- Enhance and develop/deploy new S&S awareness mechanisms (e.g., newsletter, resources/tips brochure, posters, kiosks, speakers, promo items, Superstar Awards).

Beyond 12/31/02:

- Implementing and continuously improving the effectiveness of S&S training modules and awareness mechanisms through ongoing Labwide input/feedback.

Key Milestones: (specific progress indicators for UC quarterly review)

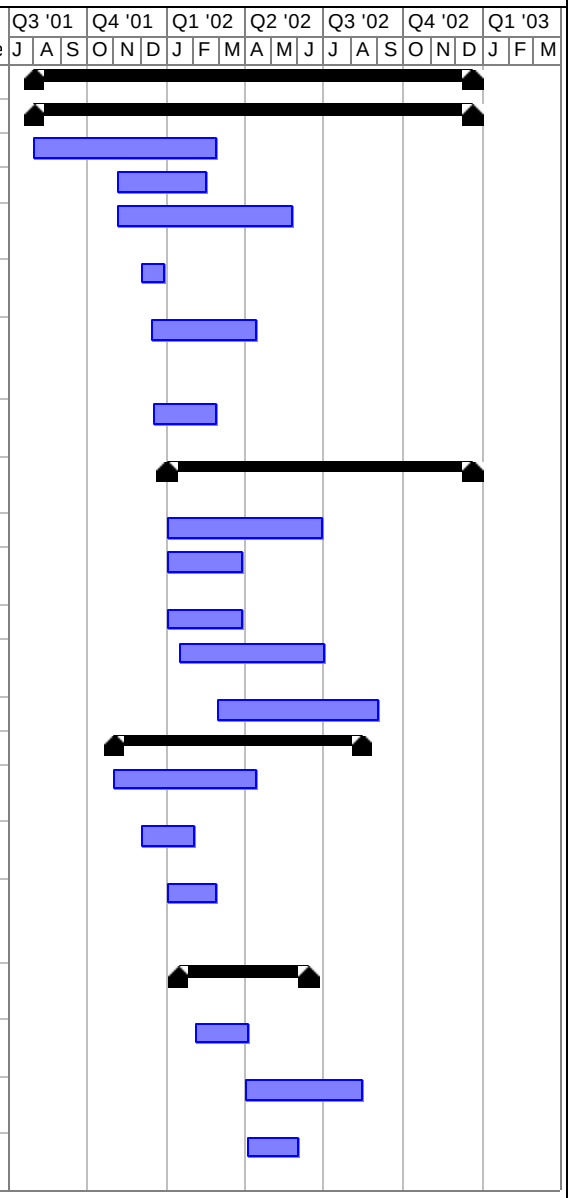
- Enhance Required Management Training content & delivery frequency (2/28/02);
- Develop/deploy an integrated S&S Training & Awareness Plan (4/30/02);
- Update GET and Annual Security Refresher consistent with S&S LIRs (6/3/02);
- Develop/deploy annual community "Safety & Security Days" (7/1/02);
- Develop/deploy web-based Sensitive Unclassified Information Training (8/1/02);
- Develop/deploy Senior Manager S&S Briefing/Desktop Reference (10/1/02).

Critical Dependencies: Refine/publish remaining S&S LIR attachments.

Resource Requirements: ~5 FTEs and Aegis support

LANL Appendix O/ISSM Project Plan
(12-12-01)

ID	Outlin	Task Name	Start	Finish	Resource Name
1	**1**	**S&S Training & Awareness (w/LLNL collaboration & Aegis support)**	**Wed 8/1/01**	**Fri 12/20/02**	**Lopez/Thomas**
2	**1.1**	**Enhance S&S Awareness Mechanisms**	**Wed 8/1/01**	**Fri 12/20/02**	**Lopez**
3	1.1.1	Select/design/deploy S&S promotional items (e.g., pins/lanyards)	Wed 8/1/01	Thu 2/28/02	Brown
4	1.1.2	Develop/deploy “Security Smart” communications for SPLs/DSOs	Mon 11/5/01	Fri 2/15/02	Brown
5	1.1.3	Develop/pilot “Nested Safety & Security Committee” (vs. safety only) in ADSR	Tue 11/6/01	Tue 5/28/02	Webster
6	1.1.4	Develop/deploy enhanced S&S Superstar Awards process (focus on recognizing "line" orgs/personnel)	Mon 12/3/01	Fri 12/28/01	Maes
7	1.1.5	Establish coordination mechanism with S, ISEC, CIO for Director’s Colloquia S&S speakers (e.g., create speakers' calendar, identify S&S themes and speakers)	Fri 12/14/01	Mon 4/15/02	Brown
8	1.1.6	Develop/deploy web-based S&S "slide show" awareness presentations	Mon 12/17/01	Thu 2/28/02	Stewart
9	**1.1.7**	**Develop/deploy S&S awareness posters (coordinate with S, ISEC, CIO)**	**Mon 12/31/01**	**Fri 12/20/02**	**Brown**
14	1.1.8	Develop/deploy quarterly security newsletter	Wed 1/2/02	Fri 6/28/02	Brown
15	1.1.9	Establish bimonthly S&S article topic and submission schedule for LANL Newsbulletin	Wed 1/2/02	Fri 3/29/02	Brown
16	1.1.10	Develop/publish annual security resources and tips brochure	Wed 1/2/02	Fri 3/29/02	Brown
17	1.1.11	Coordinate with ISM Office to expand annual "Safety Days" to “Safety & Security Days”	Tue 1/15/02	Mon 7/1/02	Brown
18	1.1.12	Select/design/deploy Labwide S&S information kiosks	Fri 3/1/02	Mon 9/2/02	Brown
19	**1.2**	**Enhance Current S&S Training Modules**	**Thu 11/1/01**	**Thu 8/15/02**	**Lopez**
20	1.2.1	Update live Classified Matter Handling Training (including parts) to ensure consistency with S&S LIRs	Thu 11/1/01	Mon 4/15/02	Valdez
21	1.2.2	Update web-based NM Handler Awareness Training to ensure consistency with S&S LIRs	Mon 12/3/01	Fri 2/1/02	Huff
22	1.2.3	Update Required Management Training (RMT) module to ensure consistency with S&S LIRs (emphasize S&S threats and risk management) and increase delivery frequency	Wed 1/2/02	Thu 2/28/02	Lopez
23	**1.2.4**	**Update web-based Security Escort Training to ensure consistency with S&S LIRs**	**Tue 1/15/02**	**Fri 6/14/02**	**Huff**
25	1.2.5	Update web-based Annual Security Refresher to ensure consistency with S&S LIRs	Mon 2/4/02	Thu 4/4/02	Valdez
26	1.2.6	Update web-based Area Access Custodian/User Training to ensure consistency with S&S LIRs	Mon 4/1/02	Thu 8/15/02	Cornely
27	1.2.7	Update General Employee Training (GET) to ensure consistency with S&S LIRs	Thu 4/4/02	Mon 6/3/02	Valdez

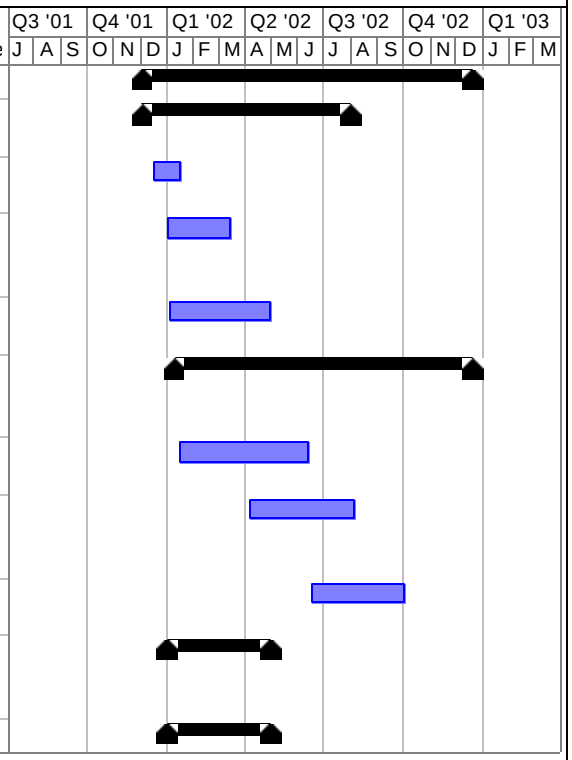


Project: LANL ISSM (12-12-01)
Date: Thu 12/13/01

Task | Milestone | External Tasks
Split | Summary | External Milestone
Progress | Project Summary | Deadline

LANL Appendix O/ISSM Project Plan
(12-12-01)

ID	Outlin	Task Name	Start	Finish	Resource Name
28	**1.3**	**Develop/Deploy New S&S Training Modules**	**Mon 12/3/01**	**Thu 12/19/02**	**Lopez**
29	**1.3.1**	**Develop/deploy web-based Sensitive Unclassified Information Training (coordinate to ensure consistency with S&S LIRs)**	**Mon 12/3/01**	**Thu 8/1/02**	**Stewart**
32	1.3.2	Develop/deploy new web-based ADC Training (coordinate to ensure consistency with S&S LIRs)	Mon 12/17/01	Thu 1/17/02	Lopez
33	1.3.3	Develop/deploy new live Annual Security Refresher briefing to augment web-based delivery (coordinate to ensure consistency with S&S LIRs)	Wed 1/2/02	Fri 3/15/02	Huff
34	1.3.4	Develop/deploy CD-based Suspicious Packages Training and incorporate into GET (coordinate to ensure consistency with S&S	Fri 1/4/02	Tue 4/30/02	Stewart
35	**1.3.5**	**Develop/deploy interim and full-scope/performance-based SPL and DSO Training (coordinate to ensure consistency with S&S LIRs)**	**Thu 1/10/02**	**Thu 12/19/02**	**Huff**
42	1.3.6	Develop/deploy live Security Escort Training (coordinate to ensure consistency with S&S LIRs)	Tue 1/15/02	Fri 6/14/02	Huff
43	1.3.7	Develop/deploy web-based Classified Removable Electronic Media Accountability Training (coordinate to ensure consistency with S&S LIRs)	Fri 4/5/02	Mon 8/5/02	Valdez
44	1.3.8	Develop/deploy Senior Manager Briefing/Desktop Reference covering S&S threats, risk management, and ISSM expected behaviors	Mon 6/17/02	Tue 10/1/02	Lopez
45	**1.4**	**Integrate S&S Training & Awareness Strategy (determine what, how, and when to provide information through training & other mechanisms)**	**Wed 1/2/02**	**Tue 4/30/02**	**Lopez**
46	**1.4.1**	**Develop/deploy an integrated S&S Training & Awareness Plan**	**Wed 1/2/02**	**Tue 4/30/02**	**Lopez**



Project: LANL ISSM (12-12-01)
Date: Thu 12/13/01

Task		Milestone		External Tasks	
Split		Summary		External Milestone	
Progress		Project Summary		Deadline	

Task A2: S&S Guidance Tools

Task Leaders: Marcene Roybal/S-2 & Susan Seestrom/P-DO
(Plus input/feedback from cross-directorate ISSM Steering Team & LLNL collaboration.)

Description: To enhance S&S training, awareness, implementation & assessment tools.

Objective: To support ISSM awareness as well as feedback and improvement processes.

Deliverables: Documentation of enhanced S&S guidance tools.

Completion Criterion: Production of deliverables.

Major Activities to be Accomplished:

Prior to 12/31/02:

- Refine/publish remaining S&S LIR attachments and develop/deploy activity- and facility-based security plan templates to support LIR implementation;
- Enhance S&S website value and user friendliness consistent with new S&S LIRs;
- Develop/deploy S&S operational guidance cards for self-assessments and MWAs;
- Develop/deploy mechanism for trend analysis of Help Desk data to support security program improvements and establish STU III secure communications link;
- Develop/deploy formal S&S suggestion process (e.g., electronic "suggestion box") for collecting, evaluating, and responding to Labwide worker input/feedback;
- Develop/deploy annual S&S Program Improvement Plan process based on workforce and external stakeholder input;
- Establish with LLNL a mechanism for routinely sharing ideas and, as practicable, effort aimed at addressing S&S policy issues of common interest.

Beyond 12/31/02:

- Implementing and continuously improving the effectiveness of Labwide S&S guidance tools through ongoing Labwide input/feedback.

Key Milestones: (specific progress indicators for UC quarterly review)

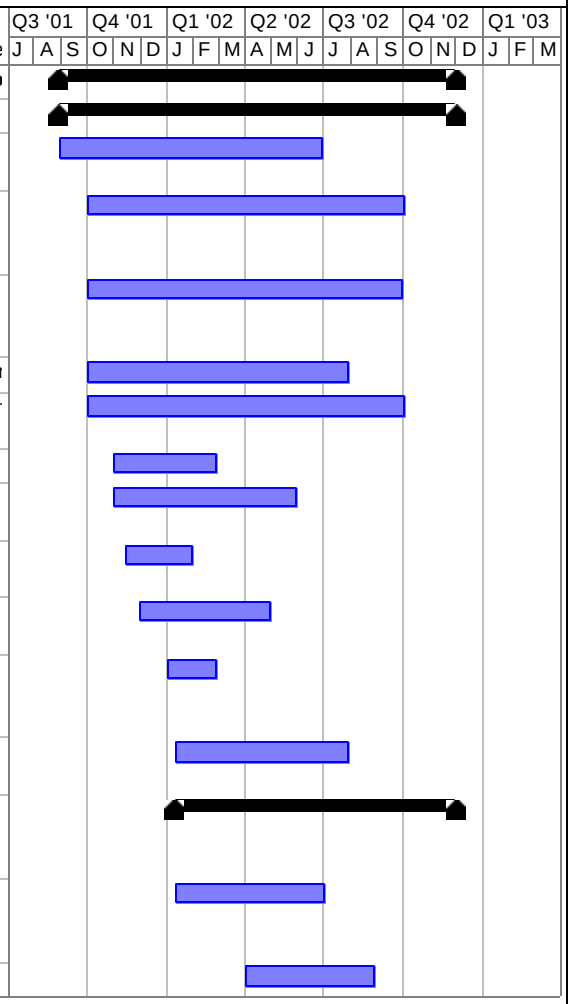
- Refine/publish remaining S&S LIR attachments (2/28/02)
- Develop/deploy operational guidance cards for self-assessments & MWAs (5/31/02);
- Develop/deploy activity- and facility-based security plan templates to support S&S LIR implementation (7/30/02)
- Develop/deploy a formal S&S suggestion process (9/30/02);
- Develop/deploy annual S&S Program Improvement Plan process (11/29/02).

Critical Dependencies: Refine/publish remaining S&S LIR attachments.

Resource Requirements: ~5 FTEs and Aegis support

LANL Appendix O/ISSM Project Plan
(12-12-01)

ID	Outlin	Task Name	Start	Finish	Resource Name
48	**2**	**S&S Guidance Tools (w/LLNL collaboration & Aegis support)**	**Wed 8/29/01**	**Fri 11/29/02**	**Roybal/Seestro**
49	**2.1**	**Enhance S&S Guidance Tools**	**Wed 8/29/01**	**Fri 11/29/02**	**Roybal**
50	2.1.1	Enhance S&S website value and user-friendliness, consistent with new S&S LIRs	Wed 8/29/01	Fri 6/28/02	Stewart
51	2.1.2	Develop/deploy mechanism for trend analysis of Help Desk data to support security program improvements (e.g., training, communications, policy)	Mon 10/1/01	Tue 10/1/02	Maes
52	2.1.3	Develop/deploy formal S&S suggestion process (e.g., electronic "suggestion box") for collecting, evaluating, and responding to Labwide worker input/feedback	Mon 10/1/01	Mon 9/30/02	Brown
53	2.1.4	Develop/deploy Voice of the Customer (VOC) process	Mon 10/1/01	Tue 7/30/02	Salazar-Kierster
54	2.1.5	Develop/deploy mechanism to solicit customer feedback on Help Desk service	Mon 10/1/01	Tue 10/1/02	Salazar-Kierster
55	2.1.6	Refine/publish remaining S&S LIR attachments	Thu 11/1/01	Thu 2/28/02	Irving
56	2.1.7	Develop/deploy S&S operational guidance cards for self assessments and MWAs	Thu 11/1/01	Fri 5/31/02	Maes
57	2.1.8	Develop/deploy OPSEC checklist to assist OPSEC WG in providing risk management guidance (e.g., publishing on LANL "green" web	Wed 11/14/01	Wed 1/30/02	Crook
58	2.1.9	Establish STU III secure communications link to Help Desk (with need-to-know caution)	Fri 11/30/01	Wed 5/1/02	Roybal
59	2.1.10	Establish with LLNL a mechanism for routinely sharing ideas and, as practicable, effort aimed at addressing S&S policy issues of common interest	Wed 1/2/02	Thu 2/28/02	Leifheit
60	2.1.11	Develop/deploy activity- and facility-based security plan templates to support S&S LIR implementation	Thu 1/10/02	Tue 7/30/02	Torres
61	**2.1.12**	**Develop/deploy process for maintaining an annual S&S Program Improvement Plan based on workforce and external stakeholder input**	**Thu 1/10/02**	**Fri 11/29/02**	**Leifheit**
64	2.1.13	Assist in the institutional development of a web-based tool for managers to monitor worker authorization (based on EDS training plans)	Thu 1/10/02	Mon 7/1/02	Lopez
65	2.1.14	Review/refine CY01 Checkpoint Survey S&S questions	Mon 4/1/02	Fri 8/30/02	Lopez



Project: LANL ISSM (12-12-01)
Date: Thu 12/13/01

Task		Milestone		External Tasks	
Split		Summary		External Milestone	
Progress		Project Summary		Deadline	

Task A3: S&S Experts

Task Leaders: Stan Busboom/S-DO & Don Cobb/ADTR
(Plus input/feedback from cross-directorate ISSM Steering Team & LLNL collaboration.)

Description: To permanently fill key S&S positions needed to support ISSM; to enhance real-time access to S&S experts in the workplace.

Objective: To support ISSM and enhance real-time physical access to S&S experts.

Deliverables: Documentation of key S&S positions having been filled with highly qualified personnel, and of a strategy for enhancing real-time access to S&S experts in the workplace.

Completion Criterion: Production of deliverables.

Major Activities to be Accomplished:

Prior to 12/31/02:

- Identify and fill key S&S positions and develop a long-term S&S staff recruiting/retention strategy;
- Develop/implement S&S deployment strategy.

Beyond 12/31/02:

- Implementing and continuously improving the S&S deployment and staff recruiting/retention strategies through ongoing Labwide input/feedback.

Key Milestones: (specific progress indicators for UC quarterly review)

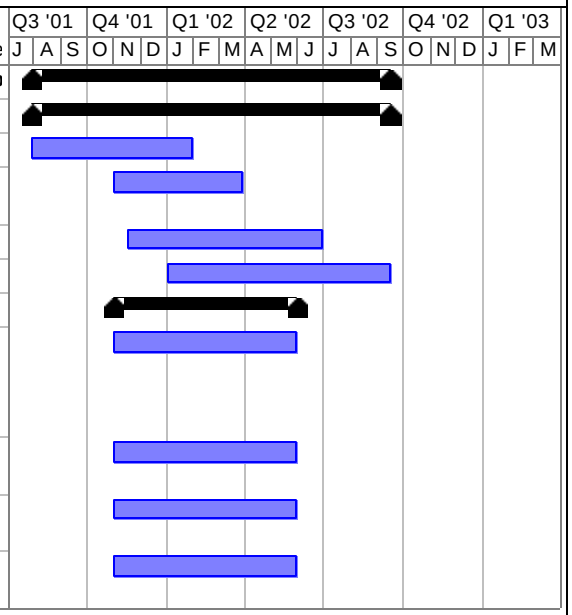
- Identify/advertise/fill S-1, S-3, S-5, OSI, and S&S PM leadership positions (1/31/02);
- Identify/advertise/fill new Security Program Leader (SPL) positions, one assigned to each directorate (3/29/02);
- Develop/communicate roles, responsibilities and authorities between SPLs, Division Security Officers, and line and S&S staffs (5/31/02);
- Develop long-term S&S staff recruiting/retention strategy (9/16/02).

Critical Dependencies: None.

Resource Requirements: ~1 FTE and Aegis support

LANL Appendix O/ISSM Project Plan
(12-12-01)

ID	Outlin	Task Name	Start	Finish	Resource Name
66	**3**	**S&S Experts (w/LLNL collaboration & Aegis support)**	**Mon 7/30/01**	**Mon 9/16/02**	**Busboom/Cobb**
67	**3.1**	**Identify/Fill Key S&S Positions**	**Mon 7/30/01**	**Mon 9/16/02**	**Busboom**
68	3.1.1	Identify/advertise/fill S-1/S-3/S-5/OSI/S&S PM mgmt positions	Mon 7/30/01	Thu 1/31/02	Busboom
69	3.1.2	Identify/advertise/fill new Security Program Leader (SPL) positions (one per directorate)	Thu 11/1/01	Fri 3/29/02	Busboom
70	3.1.3	Identify/advertise other S&S vacancies (S, ISEC, CIO)	Thu 11/15/01	Fri 6/28/02	Busboom/Kend
71	3.1.4	Develop long-term S&S staff recruiting/retention strategy	Wed 1/2/02	Mon 9/16/02	Estes/Epperson
72	**3.2**	**Develop/Implement S&S Deployment Strategy**	**Thu 11/1/01**	**Fri 5/31/02**	**Leifheit**
73	3.2.1	Develop/communicate roles, responsibilities, authorities (RRAs) for SPLs & DSOs (e.g., planning, budgeting, policy review/development, operational plans/procedures, self-assessments, training, problem solving)	Thu 11/1/01	Fri 5/31/02	Leifheit
74	3.2.2	Develop/communicate with line orgs the goals/objectives of deployed S&S support & their RRAs	Thu 11/1/01	Fri 5/31/02	Leifheit
75	3.2.3	Develop/communicate respective RRAs between SPLs, DSOs, and S&S staffs (S, ISEC, CIO)	Thu 11/1/01	Fri 5/31/02	Leifheit
76	3.2.4	Develop/communicate respective RRAs between SPLs/DSOs and other line org S&S reps (ADCs, CDCs, etc.)	Thu 11/1/01	Fri 5/31/02	Leifheit



Project: LANL ISSM (12-12-01)
Date: Thu 12/13/01

Task | Milestone | External Tasks
Split | Summary | External Milestone
Progress | Project Summary | Deadline

Task B1: S&S Management Walk-Arounds

Task Leaders: Mike Irving/S-2 & Christopher Webster/ADSR
(Plus input/feedback from cross-directorate ISSM Steering Team & LLNL collaboration.)

Description: To enhance S&S MWA content and worker involvement and to establish frequency expectations.

Objective: To promote and reinforce positive S&S behaviors in the workplace.

Deliverables: Documentation of S&S MWA expectations for content, worker involvement and frequency.

Completion Criterion: Production of deliverables.

Major Activities to be Accomplished:

Prior to 12/31/02:

- Enhance MWA content and establish frequency;
- Enhance worker involvement.

Beyond 12/31/02:

- Implementing and continuously improving the effectiveness of MWAs through ongoing Labwide input/feedback.

Key Milestones: (specific progress indicators for UC quarterly review)

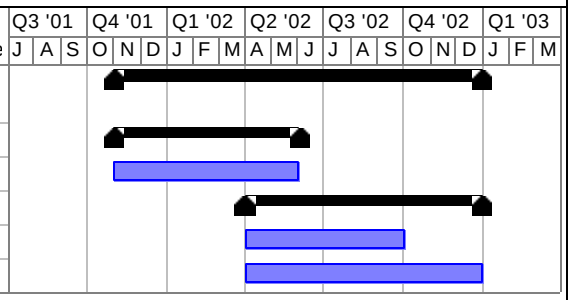
- Develop/deploy S&S guidance cards to be used for S&S MWAs (5/31/02);
- Update MWA LIR to emphasize worker involvement (10/1/02);
- Complete analysis of S&S MWA activity and worker involvement (12/31/02).

Critical Dependencies: Refine/publish remaining S&S LIR attachments.

Resource Requirements: ~0.5 FTE and Aegis support

LANL Appendix O/ISSM Project Plan
(12-12-01)

ID	Outlin	Task Name	Start	Finish	Resource Name
77	**4**	**S&S Management Walk-Arounds (w/LLNL collaboration & Aegis support)**	**Thu 11/1/01**	**Tue 12/31/02**	**Irving/Webster**
78	**4.1**	**Enhance Content and Establish Frequency for S&S MWAs**	**Thu 11/1/01**	**Mon 6/3/02**	**Irving**
79	4.1.1	Develop/deploy S&S guidance cards to be used for MWAs	Thu 11/1/01	Mon 6/3/02	Maes
80	**4.2**	**Enhance Worker Involvement**	**Mon 4/1/02**	**Tue 12/31/02**	**Irving**
81	4.2.1	Update MWA LIR to emphasize worker involvement	Mon 4/1/02	Tue 10/1/02	Irving
82	4.2.2	Complete analysis of MWA activity and worker involvement	Mon 4/1/02	Tue 12/31/02	Irving



Project: LANL ISSM (12-12-01)
Date: Thu 12/13/01

Task		Milestone		External Tasks	
Split		Summary		External Milestone	
Progress		Project Summary		Deadline	

Task B2: S&S Self-Assessments

Task Leaders: Mike Irving/S-2 & Christopher Webster/ADSR
(Plus input/feedback from cross-directorate ISSM Steering Team & LLNL collaboration.)

Description: To shift primary responsibility for assessing S&S performance to the line organizations responsible for performing the work; to assess facility- and activity-specific practices/procedures against new S&S LIRs; to engage managers in considering how well they are managing S&S risks; to enhance worker involvement in self-assessments.

Objective: To promote and reinforce active worker involvement in and line (vs. support) responsibility for S&S.

Deliverables: Documentation of ISSM-based S&S self-assessment process.

Completion Criterion: Production of deliverables.

Major Activities to be Accomplished:

Prior to 12/31/02:

- Develop/deploy ISSM-based self-assessment process;
- Update Self-Assessment LIR to reflect new process, including worker involvement.

Beyond 12/31/02:

- Implementing and continuously improving the effectiveness of the new S&S self-assessment process through ongoing Labwide input/feedback.

Key Milestones: (specific progress indicators for UC quarterly review)

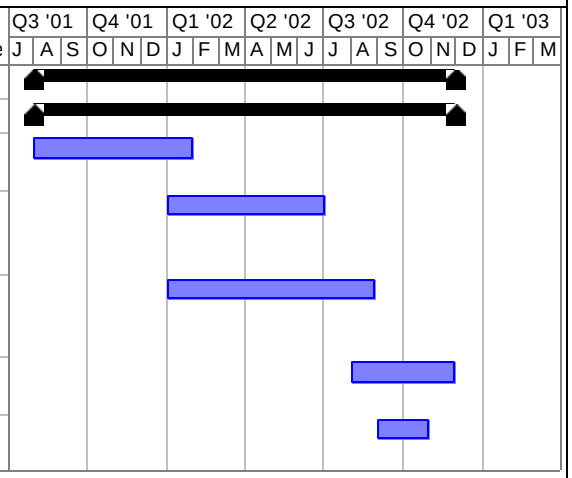
- Coordinate/develop/publish initial "line" self-assessment process focused on implementation of the emerging S&S LIRs (1/31/02);
- Coordinate/develop/publish refined "line" self-assessment process focused on implementation of the approved S&S LIRs and S&S performance (7/1/02);
- Coordinate/develop/publish overall "S&S Program" self-assessment process, including consolidated reporting, consistent with internal and external expectations, e.g., SFM, UC, NNSA, DOE/OA (8/30/02);
- Coordinate/develop/publish criteria-based "line" & "S&S Program" FY03 self-assessment plans (10/30/02).

Critical Dependencies: Refine/publish remaining S&S LIR attachments.

Resource Requirements: ~3 FTEs and Aegis support

LANL Appendix O/ISSM Project Plan
(12-12-01)

ID	Outlin	Task Name	Start	Finish	Resource Name
83	**5**	**S&S Self-Assessments (w/LLNL collaboration & Aegis support)**	**Wed 8/1/01**	**Fri 11/29/02**	**Irving/Webster**
84	**5.1**	**Develop/Deploy ISSM-based Self-Assessment Process**	**Wed 8/1/01**	**Fri 11/29/02**	**Irving**
85	5.1.1	Coordinate/develop/publish initial “line” self-assessment process focused on implementation of the emerging S&S LIRs	Wed 8/1/01	Thu 1/31/02	Irving
86	5.1.2	Coordinate/develop/publish refined “line” self-assessment process focused on implementation of the approved S&S LIRs and S&S performance	Wed 1/2/02	Mon 7/1/02	Irving
87	5.1.3	Coordinate/develop/publish overall “S&S Program” self-assessment process, including consolidated reporting, consistent with internal and external expectations (e.g., SFM, UC, NNSA, DOE/OA)	Wed 1/2/02	Fri 8/30/02	Irving
88	5.1.4	Update Self-Assessment LIR to reflect the new Labwide ISSM-based S&S self-assessment process, emphasizing active worker involvement	Thu 8/1/02	Fri 11/29/02	Irving
89	5.1.5	Coordinate/develop/publish criteria-based “line” & “S&S Program” FY03 self-assessment plans	Mon 9/2/02	Wed 10/30/02	Irving



Project: LANL ISSM (12-12-01)
Date: Thu 12/13/01

Task		Milestone		External Tasks	
Split		Summary		External Milestone	
Progress		Project Summary		Deadline	

Task B3: S&S Incidents and Lessons Learned

Task Leaders: Gene Tucker/S-DO & Gerald Reisz/IM-5
(Plus input/feedback from cross-directorate ISSM Steering Team & LLNL collaboration.)

Description: To enhance incident tracking and root-cause analysis (especially human-error analysis); to enhance Labwide communication of concerns, lessons learned and best practices.

Objective: To ensure that managers and workers are informed in a timely, efficient, and integrated manner through routine summary information and appropriate "alerts."

Deliverables: Documentation of enhanced mechanisms for tracking and analyzing S&S incidents and root causes and for communicating S&S concerns, lessons learned and best practices.

Completion Criterion: Production of deliverables**.**

Major Activities to be Accomplished:

Prior to 12/31/02:

- Adapt safety methods and apply/refine them to assess/reduce security human errors;
- Develop/deploy S&S lessons learned process and co-sponsor a Lessons Learned Network with ISM;
- Communicate S&S incidents (type/frequency) through web-based tools (analogous to ES&H TRI/LWC).

Beyond 12/31/02:

- Implementing and continuously improving the effectiveness of incident tracking and root-cause analysis as well as Labwide communication of concerns, lessons learned and best practices through ongoing Labwide input/feedback.

Key Milestones: (specific progress indicators for UC quarterly review)

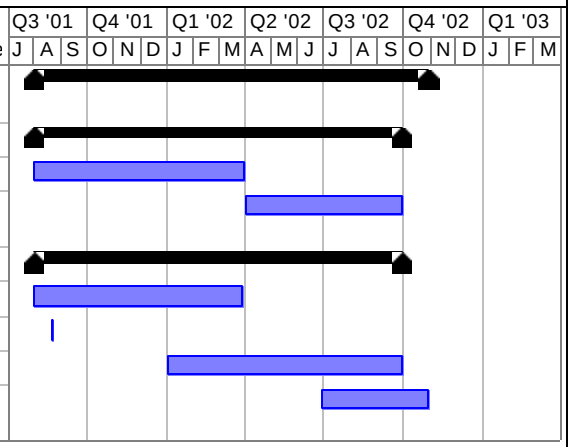
- Produce/distribute "lessons learned" awareness video to Lab workforce (3/29/02);
- Complete review of current safety methods for assessing/reducing human errors and adapt/apply/refine them to assess/reduce security human errors (9/30/02);
- Benchmark/publish S&S best practices (9/30/02);
- Communicate S&S incidents through web-based tools (10/30/02).

Critical Dependencies: None.

Resource requirements: ~2 FTEs and Aegis support

LANL Appendix O/ISSM Project Plan
(12-12-01)

ID	Outlin	Task Name	Start	Finish	Resource Name
90	**6**	**S&S Incidents and Lessons Learned (w/LLNL collaboration & Aegis support)**	**Wed 8/1/01**	**Wed 10/30/02**	**Tucker/Reisz**
91	**6.1**	**Enhance Security through Human-Error Reduction**	**Wed 8/1/01**	**Mon 9/30/02**	**Tucker**
92	6.1.1	Review current safety methods for assessing/reducing human errors	Wed 8/1/01	Mon 4/1/02	Pond
93	6.1.2	Adapt safety methods & begin applying/refining them to assess/reduce security human errors	Mon 4/1/02	Mon 9/30/02	Pond
94	**6.2**	**Develop/Deploy S&S Lessons Learned Process**	**Wed 8/1/01**	**Mon 9/30/02**	**Brown**
95	6.2.1	Produce/distribute lessons learned awareness video to Lab workforce	Wed 8/1/01	Fri 3/29/02	Brown
96	6.2.2	Initiate co-sponsorship of LANL Lessons Learned Network with ISM	Mon 8/20/01	Mon 8/20/01	Brown
97	6.2.3	Benchmark & publish S&S best practices	Wed 1/2/02	Mon 9/30/02	Brown
98	6.3	Communicate S&S Incidents (type/ freq) through Web-based Tools (analogous to ES&H TRI/LWC)	Fri 6/28/02	Wed 10/30/02	Brown



Project: LANL ISSM (12-12-01)
Date: Thu 12/13/01

Task		Milestone		External Tasks	
Split		Summary		External Milestone	
Progress		Project Summary		Deadline	

Task B4: S&S Institutional Committees

Task Leaders: Kevin Leifheit/S-2 & Scott Gibbs/ADO
(Plus input/feedback from cross-directorate ISSM Steering Team & LLNL collaboration.)

Description: To review and clarify the respective roles, responsibilities and authorities (RRAs) of LANL's S&S institutional committees (policy boards, steering groups, etc.).

Objective: To clarify the relationships and ensure consistency with Labwide ISSM expectations.

Deliverables: Documentation of the clarified RRAs and relationships of the S&S institutional committees.

Completion Criterion: Production of deliverables.

Major Activities to be Accomplished:

Prior to 12/31/02:

- Clarify/enhance the structure and/or coordination of LANL's S&S institutional committees for addressing S&S policy;
- Clarify/enhance the structure and/or coordination of LANL's S&S institutional committees for addressing S&S operational planning/execution.

Beyond 12/31/02:

- Implementing and continuously improving the effectiveness of LANL's S&S institutional committees through ongoing Labwide input/feedback.

Key Milestones: (specific progress indicators for UC quarterly review)

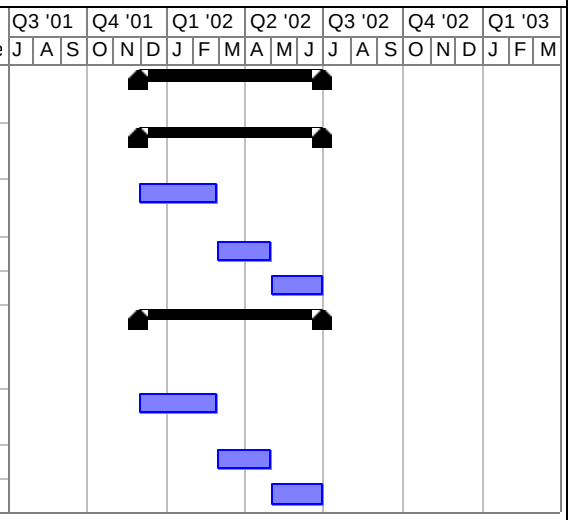
- Gain Senior Executive Team support on implementing recommendations to improve S&S policy decision-making (6/28/02);
- Gain Senior Executive Team support on implementing recommendations to improve S&S operational planning/execution (6/28/02).

Critical Dependencies: None.

Resource Requirements: ~0.5 FTE and Aegis support

LANL Appendix O/ISSM Project Plan
(12-12-01)

ID	Outlin	Task Name	Start	Finish	Resource Name
99	**7**	**S&S Institutional Committees (w/LLNL collaboration & Aegis support)**	**Fri 11/30/01**	**Fri 6/28/02**	**Leifheit/Gibbs**
100	**7.1**	**Clarify/Enhance the Structure/Coordination of LANL's S&S Institutional Committees for Addressing S&S Policy**	**Fri 11/30/01**	**Fri 6/28/02**	**Leifheit**
101	7.1.1	Evaluate effectiveness of existing structure/coordination by involving Lab stakeholders (e.g., workers, managers, SPLs/DSOs)	Fri 11/30/01	Thu 2/28/02	Leifheit
102	7.1.2	Develop recommendations for improving policy decision-making	Fri 3/1/02	Tue 4/30/02	Leifheit
103	7.1.3	Gain SET support	Wed 5/1/02	Fri 6/28/02	Leifheit
104	**7.2**	**Clarify/Enhance the Structure/Coordination of LANL's S&S Institutional Committees for Addressing S&S Operational Planning/Execution**	**Fri 11/30/01**	**Fri 6/28/02**	**Leifheit**
105	7.2.1	Evaluate effectiveness of existing structure/coordination by involving Lab stakeholders (e.g., workers, managers, SPLs/DSOs)	Fri 11/30/01	Thu 2/28/02	Leifheit
106	7.2.2	Develop recommendations for improving management of the process	Fri 3/1/02	Tue 4/30/02	Leifheit
107	7.2.3	Gain SET support	Wed 5/1/02	Fri 6/28/02	Leifheit



Project: LANL ISSM (12-12-01)
Date: Thu 12/13/01

Task		Milestone		External Tasks	
Split		Summary		External Milestone	
Progress		Project Summary		Deadline	

IV. MANAGEMENT REVIEW PROCESS

This *Project Plan* has identified key milestones that will be subject to UC review. UC will establish a quarterly schedule to review these milestones with LANL's ISSM staff. It is intended that the quarterly reviews will precede the quarterly meetings set by NNSA to review the status of the *Action Plan* with UC. LANL's internal management review process will support and augment UC's quarterly review to ensure that ISSM performance expectations are met.

V. CHANGE CONTROL PROCESS

The Associate Director for Threat Reduction, serving as LANL ISSM Champion, must approve proposed changes, including rationale, in the schedule or scope of the key milestones before submittal to the UC Office of the President for approval.

A change control process is needed because the execution of this *Project Plan* is based upon estimates of scope and resources required to accomplish these tasks, which may change as they are undertaken and are more fully understood. The *Project Plan* will be updated upon approval of changes to key milestones and/or on a quarterly basis.

VI. CROSSWALK

The crosswalk between LANL's ISSM gaps and the UC Criteria as shown on the next page maps directly to the individual task summaries provided in Section III.

LANL ISSM Gap Summary	UC Criteria										
	A	B	C	D	E	F	G	H	I	J	K
A. Implementation Support/Delivery of Services											
1. S&S Training & Awareness a. Worker training to ensure awareness of ISSM responsibilities and resources is insufficient. b. Management training to ensure awareness of ISSM responsibilities and resources is insufficient. c. Greater ISSM awareness by all workers and managers is needed through mechanisms other than training.	X		X	X		X	X		X	X	
2. S&S Guidance Tools a. Training, awareness, and implementation tools to support ISSM are insufficient. b. Assessment tools to support feedback & improvement processes are insufficient.		X				X			X	X	
3. S&S Experts a. Several key S&S positions needed to support ISSM are vacant. b. Real-time access to S&S experts in the workplace is insufficient.				X	X			X		X	
B. Feedback & Improvement											
1. S&S Management Walk-Arounds a. Walk-around content and level of worker involvement are insufficient. b. An expected frequency has not been established.		X			X						X
2. S&S Self-Assessments a. Primary responsibility for assessing S&S performance needs to shift from S&S support organizations to the line organizations responsible for performing the work. b. Facility- and activity-specific practices/procedures need to be assessed against new ISSM LPR/LIRs. c. Managers need to consider how well they are managing S&S risks. d. Worker involvement in self-assessments is insufficient.		X			X			X		X	X
3. S&S Incidents & Lessons Learned a. Incident tracking and root-cause analysis (esp. human-error analysis) are insufficient. b. Labwide communication of concerns, lessons learned, and best practices is insufficient.		X			X						X
4. S&S Institutional Committees a. The relationship between LANL's various S&S institutional committees (policy boards, steering groups, etc.) is unclear.		X			X		X	X		X	X

Los Alamos National Laboratory

ISSM Action Plan

(9-21-01)

Los Alamos National Laboratory
ISSM Action Plan

Purpose

Los Alamos National Laboratory (LANL) is totally committed to accomplishing its critical national security mission in a safe, secure, reliable, and cost-effective manner. To this end, LANL Director John Browne launched Integrated Safeguards and Security Management (ISSM) in early 2000, modeling it after Integrated Safety Management (ISM) -- i.e., management commitment, worker involvement, line "ownership," clearly defined roles and responsibilities, work and worker authorization, self-assessment, continuous improvement, etc. Director Browne has since committed to putting ISSM "in place" by December 31, 2002, consistent with contractual expectations (Appendix O) established January 18, 2001, between the University of California (UC) and the U. S. Department of Energy (DOE).

Among the ISSM contractual expectations, LANL is to develop an ISSM Action Plan in response to the LANL ISSM Gap-Analysis Summary Report submitted to UC on August 20, 2001. The ISSM Action Plan must be submitted by UC to DOE by September 28, 2001, for DOE approval, as described in Clause 2.5 of Appendix O. The Action Plan presented here satisfies this requirement and will further LANL's substantial ISSM progress (journey)***** by:

- Further improving our safeguards and security (S&S) management system;
- Further improving "ownership" of S&S by those who own/perform the work;
- Making "work securely" as efficient and user-friendly as possible; and
- Addressing the gaps listed in the LANL ISSM Gap-Analysis Summary Report.

*****Note: At the August 9, 2001, management outbrief of LANL's recent comprehensive DOE Annual S&S Survey, the DOE Survey Team Leader reported that the DOE survey topical leads found… *"Evidence of ISSM at every level."*

Approach

As with the precursive gap analysis, LANL's ISSM Action Plan was developed in accordance with UC "corporate" guidance provided on September 12, 2001, and is responsive to UC-DOE contractual expectations. Both the UC guidance and LANL's Action Plan benefited from excellent cooperation and collaboration among UC, LLNL, LANL, Aegis Research Corporation, and DOE's National Nuclear Security Administration (NNSA). In addition, the Action Plan benefited from extensive workforce involvement led by Director Browne's Senior Executive Team and coordinated by the cross-directorate ISSM Steering Team comprising LANL line, program, and support as well as invited NNSA representation. This extensive workforce involvement is briefly summarized below.

1. More than 10,000 UC/LANL employees and major subcontractors (Protection Technology Los Alamos and Johnson Controls Northern New Mexico) actively participated in Director-launched ISSM Workshops that were highly interactive, tailored to the work of individual divisions, groups, and teams, and aimed at learning about ISSM, identifying concerns/gaps, and making suggestions for improving S&S performance;

2. Multiple worker-based focus teams were formed to simplify and replace LANL's entire set of current S&S institutional requirements (all topical and cross-cutting areas), including soliciting Labwide workforce involvement in developing and critically reviewing the emerging set of new S&S requirements (ISSM LPR/LIRs), identifying concerns/gaps, and making suggestions for improving S&S performance; and

3. LANL's cross-directorate ISSM Positive Security Behaviors Team was chartered to assess the health of LANL's S&S environment by visiting with and listening to workers in the workplace, and to summarize common concerns/gaps and make suggestions for improving S&S performance.

LANL's participatory approach to developing and implementing ISSM since early 2000, including more recent contractual efforts to conduct a gap analysis and develop this Action Plan, almost certainly gave rise to DOE's positive ISSM conclusion from LANL's recent comprehensive DOE Annual S&S Survey (see note above). In addition, LANL's gap analysis gave rise to opportunities for further improving S&S performance through sustained ISSM implementation. These opportunities (gaps) are summarized in the table below as excerpted from LANL's ISSM Gap-Analysis Summary Report. They also are cross-walked with and addressed by this Action Plan as described following the table.

Per UC guidance, LANL's ISSM Action Plan is a performance-based plan that defines the top-level tasks (the "what") for addressing LANL's identified gaps. It includes a concise description of each task's deliverables and completion criteria that define when each task is successfully concluded. Within 45 days following DOE approval of this Action Plan, a Project Plan (the "how") will be developed and submitted to UC for approval. It will serve as the principal means by which the UC Vice President for Laboratory Management (VPLM) and his staff will ensure progress in the systematic integration of S&S into LANL's management and work practices. The Project Plan will be structured to include task leaders, schedules, description of deliverables, resource requirements, and task progress indicators for quarterly review by UC.

LANL's Action Plan and Project Plan will leverage and build on ISSM (and ISM) accomplishments and lessons learned, consistent with LANL's overall pursuit of Integrated Management (IM). Always, gains in efficiency and cost effectiveness must remain basic to our thinking as we strive to improve the security of day-to-day operations. Moreover, sustained "top-down" leadership and active "bottom-up" participation are essential to achieve the buy-in and ownership necessary for success. Hence, extensive workforce involvement, including active solicitation of worker and manager input and feedback, will continue to be the hallmark of LANL's development and implementation of ISSM.

LANL ISSM Gap Summary	UC Criteria										
	A	B	C	D	E	F	G	H	I	J	K
A. Implementation Support/Delivery of Services											
1. S&S Training & Awareness a. Worker training to ensure awareness of ISSM responsibilities and resources is insufficient. b. Management training to ensure awareness of ISSM responsibilities and resources is insufficient. c. Greater ISSM awareness by all workers and managers is needed through mechanisms other than training.	X		X	X		X	X		X	X	
2. S&S Guidance Tools a. Training, awareness, and implementation tools to support ISSM are insufficient. b. Assessment tools to support feedback & improvement processes are insufficient.		X				X			X	X	
3. S&S Experts a. Several key S&S positions needed to support ISSM are vacant. b. Real-time access to S&S experts in the workplace is insufficient.				X	X			X		X	
B. Feedback & Improvement											
1. S&S Management Walk-Arounds a. Walk-around content and level of worker involvement are insufficient. b. An expected frequency has not been established.		X			X						X
2. S&S Self-Assessments a. Primary responsibility for assessing S&S performance needs to shift from S&S support organizations to the line organizations responsible for performing the work. b. Facility- and activity-specific practices/procedures need to be assessed against new ISSM LPR/LIRs. c. Managers need to consider how well they are managing S&S risks. d. Worker involvement in self-assessments is insufficient.		X			X			X		X	X
3. S&S Incidents & Lessons Learned a. Incident tracking and root-cause analysis (esp. human-error analysis) are insufficient. b. Labwide communication of concerns, lessons learned, and best practices is insufficient.		X			X						X
4. S&S Institutional Committees a. The relationship between LANL's various S&S institutional committees (policy boards, steering groups, etc.) is unclear.		X			X		X	X		X	X

LANL ISSM Actions to Address Gaps

A. Implementation Support/Delivery of Services

1. <u>S&S Training & Awareness</u>
Tasks:

a. Enhance worker training to increase awareness of ISSM responsibilities and resources.
b. Enhance management training to increase awareness of ISSM responsibilities and resources.
c. Enhance mechanisms other than training to increase ISSM awareness by all workers and managers.

To accomplish these tasks, LANL will further review and enhance General Employee Training (GET), S&S annual refresher training, and S&S topical training modules to ensure clear communication and reinforcement of Labwide ISSM expectations, including individual and organizational roles, responsibilities, and authorities (RRAs) for meeting S&S requirements in LANL's soon-to-be published ISSM LPR/LIRs. Other awareness mechanisms also will be further reviewed and enhanced to support this objective. Prospective enhancements will be aimed at assisting:

- Senior managers by adequately informing them of their S&S RRAs, including issues and concerns relevant to their areas of responsibility;
- All managers by providing tailored threat information to help them understand and address security threats and unacceptable consequences relevant to their areas of responsibility; and
- All managers and workers by clarifying definitions of, e.g., acceptable residual risk, including differences between compliance- and performance-based risk requirements, and the role of SMEs in assisting with establishing acceptable risk and when to seek their assistance.

In addition, S&S training modules and other awareness mechanisms will be evaluated to determine what, how, and when to provide information through training vs. other mechanisms to increase awareness in a timely, efficient, and integrated manner. One option might be a checklist that would allow manager and/or worker self-evaluation of training needs based on the job assignment so that training could be tailored to the needs of each individual. Another option might be to provide integrated training based on work areas.

Completion criteria: (1) Labwide S&S training modules and other awareness mechanisms have been further reviewed, enhanced, documented, and communicated; and (2) an integrated S&S training and awareness strategy has been developed, documented, and communicated. To verify completion, the documented products will be made available to NNSA/AL and UC. Note that all completed actions will be subject to further improvement through ongoing Labwide input and feedback.

2. <u>S&S Guidance Tools</u>
Tasks:

a. Enhance training, awareness, and implementation tools to support ISSM.
b. Enhance assessment tools to support feedback & improvement processes.

To accomplish these tasks, LANL will further review, enhance, and make readily available user-friendly training, awareness, implementation, and assessment tools (e.g., web-based guidance cards and security plan templates, FAQs, posters, special events, promotional items, etc.) all aimed at supporting and continually improving Labwide ISSM expectations and practices, including the S&S requirements in LANL's soon-to-be published ISSM LPR/LIRs.

Completion criterion: Labwide S&S guidance tools have been further reviewed, enhanced, documented, and communicated. To verify completion, the documented products will be made available to NNSA/AL and UC. Note that all completed actions will be subject to further improvement through ongoing Labwide input and feedback.

3. <u>S&S Experts</u>
Tasks:

a. Permanently fill key S&S positions needed to support ISSM.
b. Enhance real-time access to S&S experts in the workplace.

To accomplish these tasks, LANL will identify and fill key S&S positions with highly qualified personnel and enhance real-time physical access to S&S experts in the workplace. One option for enhancing real-time access is to develop and implement a Labwide value-added deployment model tailored to organizational needs.

Completion criteria: (1) key S&S positions have been identified and filled with highly qualified personnel; and (2) a strategy for enhancing real-time access to S&S experts in the workplace has been developed, documented, and communicated. To verify completion, the documented products will be made available to NNSA/AL and UC. Note that all completed actions will be subject to further improvement through ongoing Labwide input and feedback.

B. Feedback & Improvement

1. <u>S&S Management Walk-Arounds</u>
Tasks:

a. Enhance content and worker involvement.
b. Establish frequency expectations.

To accomplish these tasks, LANL will further review and enhance the expectations for content and level of worker involvement of Labwide S&S management walk-arounds (MWAs) to promote and reinforce positive S&S behaviors. In addition, Labwide expectations for the frequency of S&S MWAs will be established.

Completion criterion: Labwide S&S MWA expectations for content, worker involvement, and frequency have been further reviewed, enhanced, documented, and communicated. To verify completion, the documented products will be made available to NNSA/AL and UC. Note that all completed actions will be subject to further improvement through ongoing Labwide input and feedback.

2. <u>S&S Self-Assessments</u>
Tasks:

a. Shift primary responsibility for assessing S&S performance from S&S support organizations to the line organizations responsible for performing the work.
b. Assess facility- and activity-specific practices/procedures against LANL's soon-to-be published ISSM LPR/LIRs.
c. Engage managers in considering how well they are managing S&S risks.
d. Enhance worker involvement in self-assessments.

To accomplish these tasks, LANL will determine the best approach for shifting primary responsibility for assessing S&S performance from S&S support organizations to the line organizations responsible for performing the work. Emphasis will be placed on line ownership, worker involvement, and managing risk. This will include assessing current facility- and activity-specific practices/procedures against the S&S requirements in LANL's soon-to-be published ISSM LPR/LIRs and taking appropriate action.

Completion criterion: Labwide S&S self-assessment expectations have been developed, documented, and communicated. To verify completion, the documented products will be made available to NNSA/AL and UC. Note that all completed actions will be subject to further improvement through ongoing Labwide input and feedback.

3. <u>S&S Incidents & Lessons Learned</u>
Tasks:

a. Enhance incident tracking and root-cause analysis (esp. human-error analysis).
b. Enhance Labwide communication of concerns, lessons learned, and best practices.

To accomplish these tasks, LANL will further review and enhance tracking, trending, and analysis of S&S incidents and root causes, with special focus on human-error analysis. In addition, Labwide communication of S&S concerns, lessons learned, and best practices will be further reviewed and enhanced to ensure that managers and workers are informed in a timely, efficient, and integrated manner through routine summary information and appropriate "alerts."

Completion criterion: Labwide mechanisms for tracking, trending, and analyzing S&S incidents and root causes and for communicating S&S concerns, lessons learned, and best practices have been further reviewed, enhanced, documented, and communicated. To verify completion, the documented products will be made available to NNSA/AL and UC. Note that all completed actions will be subject to further improvement through ongoing Labwide input and feedback.

4. <u>S&S Institutional Committees</u>
Task:

a. Clarify the relationship between LANL's various S&S institutional committees.

To accomplish this task, LANL will further review and clarify the respective roles, responsibilities, and authorities of its S&S institutional committees (policy boards, steering groups, etc.), consistent with Labwide ISSM expectations.

Completion criterion: The relationship between LANL's various S&S institutional committees has been further reviewed, clarified, documented, and communicated. To verify completion, the documented products will be made available to NNSA/AL and UC. Note that all completed actions will be subject to further improvement through ongoing Labwide input and feedback.

Los Alamos National Laboratory

ISSM Gap-Analysis Summary Report

(August 17, 2001)

Work
Securely
(ISSM)

INTRODUCTION

Los Alamos National Laboratory (LANL) is totally committed to accomplishing its critical national security mission in a safe, secure, reliable, and cost-effective manner. To this end, LANL Director John Browne launched Integrated Safeguards and Security Management (ISSM) in early CY00, modeling it after Integrated Safety Management (ISM) -- i.e., management commitment, worker involvement, line "ownership," clearly defined roles and responsibilities, work and worker authorization, self-assessment, continuous improvement, etc. Director Browne has since committed to putting ISSM "in place" by December 31, 2002, consistent with UC-DOE contractual expectations (Appendix O) established January 18, 2001. Among these expectations, LANL is to conduct a gap analysis comparing its existing safeguards and security (S&S) system to the required ISSM system. This report summarizes LANL's gap-analysis approach and results, which provide the basis for developing an action plan to further LANL's substantial ISSM progress.*

*Note: At the August 9, 2001, management out-brief of LANL's most recent comprehensive DOE Annual S&S Survey, the DOE survey team leader proclaimed that the DOE survey topical leads found… *"Evidence of ISSM at every level."*

APPROACH

LANL's gap analysis was conducted in accordance with UC guidance and benefited from total workforce involvement coordinated by Director Browne's cross-directorate ISSM Steering Team comprising LANL line, program, and support as well as invited NNSA representation. This total workforce involvement is briefly summarized below. Additional details are available at the LANL ISSM website and in the LANL ISSM Communications Plan and related documentation.

1. More than 10,000 UC/LANL employees and major subcontractors (Protection Technology Los Alamos and Johnson Controls Northern New Mexico) actively participated in Director-launched ISSM Workshops that were highly interactive,

tailored to the work of individual divisions/groups/teams, and aimed at learning about ISSM, identifying concerns/gaps, and making suggestions for improving S&S performance;

2. Worker-based focus teams were formed to simplify and replace LANL's entire set of current S&S institutional requirements (all topical and cross-cutting areas), including soliciting Labwide workforce involvement in developing and critically reviewing the emerging set of new S&S institutional requirements, identifying concerns/gaps, and making suggestions for improving S&S performance; and

3. LANL's cross-directorate ISSM Positive Security Behaviors Team was chartered to assess the health of LANL's S&S environment by visiting with and listening to workers in the workplace, and to summarize common concerns/gaps and make suggestions for improving S&S performance.

LANL's participatory approach to conducting its ISSM gap analysis through total workforce involvement over the past year almost certainly gave rise to DOE's positive observation during LANL's most recent comprehensive DOE Annual S&S Survey as noted earlier. It also gave rise to many opportunities and actions for further improving S&S performance through sustained ISSM implementation. Current opportunities (gaps) are summarized below and will be addressed in a LANL action plan that fully leverages and builds on ISSM (and ISM) accomplishments and lessons learned to date, consistent with LANL's overall pursuit of Integrated Management (IM).

SUMMARY RESULTS

The results of LANL's gap analysis and the relationship to the ISSM criteria in the UC guidance are summarized on the following pages. LANL greatly appreciates the strong support from UC and its security subcontractor, Aegis Research Corporation, and from NNSA in accomplishing the gap analysis and initiating development of the companion action plan. Continued teamwork will ensure LANL’s ISSM and mission success.

LANL ISSM Gap Summary	UC Criteria										
	A	B	C	D	E	F	G	H	I	J	K
A. Implementation Support/Delivery of Services											
1. S&S Training & Awareness a. Worker training to ensure awareness of ISSM responsibilities and resources is insufficient. b. Management training to ensure awareness of ISSM responsibilities and resources is insufficient. c. Greater ISSM awareness by all workers and managers is needed through mechanisms other than training.	X		X	X		X	X		X	X	
2. S&S Guidance Tools a. Training, awareness, and implementation tools to support ISSM are insufficient. b. Assessment tools to support feedback & improvement processes are insufficient.		X				X			X	X	
3. S&S Experts a. Several key S&S positions needed to support ISSM are vacant. b. Real-time access to S&S experts in the workplace is insufficient.				X	X			X		X	
B. Feedback & Improvement											
1. S&S Management Walk-Arounds a. Walk-around content and level of worker involvement are insufficient. b. An expected frequency has not been established.		X			X						X
2. S&S Self-Assessments a. Primary responsibility for assessing S&S performance needs to shift from S&S support organizations to the line organizations responsible for performing the work. b. Facility- and activity-specific practices/procedures need to be assessed against new ISSM LPR/LIRs. c. Managers need to consider how well they are managing S&S risks. d. Worker involvement in self-assessments is insufficient.		X			X			X		X	X
3. S&S Incidents & Lessons Learned a. Incident tracking and root-cause analysis (esp. human-error analysis) are insufficient. b. Labwide communication of concerns, lessons learned, and best practices is insufficient.		X			X						X
4. S&S Institutional Committees a. The relationship between LANL's various S&S institutional committees (policy boards, steering groups, etc.) is unclear.		X			X		X	X		X	X

RATIONALE FOR GAP-CRITERIA CROSSWALK

A. Implementation Support/Delivery of Services

1. S&S Training & Awareness - This relates primarily to workers and managers understanding and accepting responsibility (A&C) and managers accepting residual risk (F); secondarily to the S&S institutional support organizations developing and providing the training & awareness (I) and interpreting the DOE requirements (J); and thirdly to managers and senior managers ensuring that it happens (D&G).

2. S&S Guidance Tools - This relates primarily to the S&S institutional support organizations developing and providing the guidance tools (I) and interpreting the DOE requirements (J); and secondarily to users -- both the workers providing feedback for improving security (B) and the managers accepting risk and authorizing work (F).

3. S&S Experts - This relates primarily to managers ensuring appropriately competent staff (D) and that sufficient controls are in place (E); secondarily to the S&S institutional support organizations assisting managers and workers in assessing and reducing S&S risks to acceptable levels (J); and thirdly to optimizing use of Lab resources (H).

B. Feedback & Improvement

1. S&S Management Walk-Arounds - This relates primarily to managers ensuring sufficient controls are in place (E); secondarily to workers providing feedback for improving security (B); and thirdly to the S&S institutional support organizations providing program assessments, lessons learned, and best practices (K).

2. S&S Self-Assessments - This relates primarily to managers ensuring sufficient controls are in place (E) and optimizing use of Lab resources (H); secondarily to workers providing feedback for improving security (B); and thirdly to the S&S institutional support organizations promoting worker involvement (J) and providing program assessments, lessons learned, and best practices (K).

3. S&S Incidents & Lessons Learned - This relates primarily to managers ensuring sufficient controls are in place (E); secondarily to workers providing feedback for improving security (B); and thirdly to the S&S institutional support organizations providing incident analyses, lessons learned, and best practices (K).

4. S&S Institutional Committees - This relates primarily to workers and managers reducing risk (B&E); secondarily to the S&S institutional support organizations interpreting DOE requirements (J) and providing program assessments, incident analyses, lessons learned, and best practices (K); and thirdly to senior managers ensuring that managers are executing their S&S responsibilities (G) and optimizing use of Lab resources (H).

University of California
Office of the President

Guidance for Integrated Safeguards and Security Management Gap Analysis

INTRODUCTION

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

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

UC's ISSM VISION

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

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

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

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

APPROACH

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

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

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

1. **Individual Responsibility and Participation**: Each individual is directly responsible for following security requirements and contributing to secure missions and workplaces.

2. **Line Management Responsibility for Safeguards and Security**: Line management is directly responsible for the protection of the DOE assets. Appropriate risk analysis is performed prior to work being authorized. Residual risk must be accepted by line management and controls must be in place and verified prior to authorization of operations.

3. **Clear Roles and Responsibilities**: Clear and unambiguous lines of authority and responsibility for ensuring S&S must be established and maintained at all organizational levels within the contractor's organization.

4. **Competence Commensurate with Responsibilities**: Individuals must possess the experience, knowledge, skills and abilities necessary to fulfill their responsibilities.

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

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

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

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

Matrix of Criteria to Guiding Principles

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

UNIVERSITY OF CALIFORNIA

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO

SANTA BARBARA • SANTA CRUZ

OFFICE OF THE SENIOR VICE PRESIDENT –
BUSINESS AND FINANCE

OFFICE OF THE PRESIDENT
1111 Franklin Street, 5th Floor
Oakland, California 94607-5206

April 17, 2001

Mr. David A. Gurulé
Area Manager
Los Alamos Area Office
528 35th Street, MS A316
Los Alamos, NM 87544

RE: Integrated Safeguards and Security Management (ISSM) Communications Plan

Dear Mr. Gurulé:

We are transmitting the final "ISSM System Communications Plan" for Los Alamos National Laboratory (LANL). This plan meets the University of California's expectations for an ISSM communications plan and satisfies the Appendix O sub-initiative contained in Clause 2.3 of Appendix O. We are confident that this plan will enable LANL to promote awareness for ISSM and solicit employee feedback so that the worker is actively involved in successfully implementing ISSM at LANL. LANL's communications plan is designed to be flexible so that it can incorporate directions received from NNSA and suggestions provided by LANL workers.

The University of California's expectations for the communications plan were as follows:

1. The plan would satisfy an important element of the criteria developed by General Gordon's Safeguards and Security Management Integration Team (SSMIT) for making an "In Place" declaration for ISSM. This element calls for contractor organizations to deploy ISSM awareness and feedback mechanisms at all worker levels.

2. The plan would help achieve integration of safeguards and security into day-to-day operations.

3. The plan would outline an approach to educate workers on ISSM's guiding principles and explain the processes used to ensure each individual understands their roles and responsibilities in working securely.

4. The plan would describe the mechanisms the Lab would develop and use so that employees know where to obtain information on any security questions they may have.

5. The plan would identify mechanisms the Lab would develop and use to obtain employee feedback on safeguards and security policies and practices, and on other ISSM implementation issues in order to promote continuous improvement.

6. The plan would foster positive security values in the workplace and in a manner which supports the successful execution of the national security and scientific missions.

7. The plan would be sufficiently flexible to accommodate the incorporation of actions directed by NNSA including those "Six Month Actions" attached to General Gordon's March 26, 2001 memorandum regarding ISSM implementation for NNSA.

8. The plan would also provide flexibility to allow for adjustments to support actions identified in the action plan following the gap analysis required in Appendix O.

Sincerely,

Robert L. Van Ness
Assistant Vice President
Laboratory Administration

Attachment:
LANL ISSM Communications Plan

cc: Larry Kirkman, NNSA/AL
Sharon Daly, LAAO
Don Cobb, LANL
Stan Busboom, LANL

LOS ALAMOS NATIONAL LABORATORY

Integrated Safeguards and Security Management (ISSM)

Communications Plan

April 12, 2001

Worker-Based Security Serving Science & Society!

TABLE OF CONTENTS

PURPOSE 1
SCOPE 1
Phase I – Launching ISSM 1
Phase II – Putting ISSM "In Place" 1
Phase III – Continuously Improving ISSM 2
BACKGROUND AND DISCUSSION 2
LANL CY00 ISSM Rollout 2
NNSA CY01 ISSM Rollout 2
Partnering for ISSM Success 3
Laboratory Workers 3
Managers/Supervisors 4
Organizational Security Representatives 4
Institutional Security Subject Matter Experts (SMEs) 5
LANL-NNSA Teamwork 5
LANL Communications Processes 5
PHASE II STRATEGY 6
ATTACHMENT ONE: LANL'S CY00 ISSM ROLLOUT ACCOMPLISHMENTS 10
ATTACHMENT TWO: GENERAL GORDON'S CY01 ISSM ROLLOUT INITIATION 16
ATTACHMENT THREE: LANL COMMUNICATIONS PROCESSES 27
Promoting Employee Awareness 27
Awareness Tools 27
Measurement Tools 28
Process Flow Chart 29
Soliciting Employee Input/Feedback 30
Input/Feedback Tools 30
Measurement Tools 31
Policy Input/Feedback Structure 32
Policy Input/Feedback Process Flow Chart 33

PURPOSE

Los Alamos National Laboratory (LANL or Laboratory) is fully dedicated to accomplishing its vital national security mission in a safe, *secure,* reliable, and cost-effective manner. To this end, LANL Director John Browne launched *Integrated Safeguards and Security Management (ISSM)* in CY00 and has since contractually committed to putting it "in place" by December 31, 2002. This Plan supports this major institutional effort by outlining the Lab's communications strategy for promoting employee awareness and soliciting employee input and feedback for continuously improving the safeguards and security (S&S or simply "security") of day-to-day operations through ISSM. The strategy is based on strong "top-down" management commitment and active "bottom-up" workforce participation to achieve the buy-in and ownership necessary for success.

As a "living document," this Plan will be continually updated as ISSM matures to reflect lessons learned and process improvements. Always, gains in efficiency and cost effectiveness must be basic to our thinking. This first edition was coordinated by the cross-directorate LANL ISSM Steering Team, with NNSA/LAAO membership, and benefited from extensive Labwide input.

SCOPE

As summarized below, this Plan encompasses three distinct phases for the development, implementation, and continuous improvement of ISSM in support of LANL's vital national security mission. Employee awareness, input, and feedback are essential for each phase.

Phase I – Launching ISSM

This past phase focused on the Labwide development, rollout, and initial implementation of ISSM, with strong emphasis on demonstrated management commitment and active workforce participation to achieve buy-in and ownership. It was launched in early CY00 and ended with the January 18, 2001, signing of the new UC-DOE contract, which established ISSM milestones in Appendix O. This phase promoted employee awareness and solicited employee input/feedback for many months before the new UC-DOE contract was signed, and a Labwide employee survey showed it was well received. For a summary of major Phase I actions and accomplishments, see Background and Discussion (below) and Attachment One.

Phase II – Putting ISSM "In Place"

This current phase focuses on putting ISSM in place by building on Phase I efforts to develop and implement ISSM. Briefly, "in place" means meeting all ISSM milestones in Appendix O, which are aimed at continuously improving the security of day-to-day operations. As in Phase I, there is strong emphasis on demonstrated management commitment and active workforce participation to achieve buy-in and ownership. This phase began with the January 18, 2001, signing of the new UC-DOE contract and will continue through September 30, 2002, when Appendix O expires. The strategy for promoting employee awareness and soliciting employee input/feedback during this phase is outlined below (see Phase II Strategy).

Phase III – Continuously Improving ISSM

This future phase will focus on sustaining and continuously improving ISSM implementation. As in Phases I and II, there will continue to be a strong emphasis on demonstrated management commitment and active workforce participation to achieve buy-in and ownership. This phase will begin when Appendix O expires on September 30, 2002. However, unlike the other two phases, it has no defined endpoint because ISSM is a journey, not a destination. The overall strategy for promoting employee awareness and soliciting employee input/feedback during this phase will evolve during Phase II and will continue to be aimed at continuously improving the security of day-to-day operations.

BACKGROUND AND DISCUSSION

LANL CY00 ISSM Rollout

In early CY00, LANL launched the development, Labwide rollout, and initial implementation of ISSM (Phase I), modeling it after Integrated Safety Management (ISM). LANL Director John Browne started this initiative because ISM's basic tenets -- management commitment, worker involvement, line "ownership," clearly defined roles and responsibilities, work and worker authorization, self-assessment, continuous improvement, etc. -- are vital to the success of both safety and security at LANL. Pursuing ISSM offers not only a stronger security culture and enhanced security performance, but a unified management model for accomplishing LANL's vital national security mission in a safe, secure, reliable, and cost-effective manner.

Employee feedback on the initial ISSM rollout, which was highly interactive and tailored to the work of individuals and organizations throughout the Lab, was positive. Participants learned to apply the ISSM 5-step process and openly shared their security questions, concerns, and suggestions. For more information on the ISSM rollout and other major ISSM actions and accomplishments in CY00, see Attachment One and visit the LANL ISSM website: http://int.lanl.gov/orgs/s/issm

NNSA CY01 ISSM Rollout

On March 26, 2001, General John Gordon, NNSA Administrator, signed out two memoranda (see Attachment Two) committing the entire NNSA complex (Federal and contractor) to ISSM. These were prepared by the Safeguards and Security Management Integration Team (SSMIT), which he formed last fall with Federal and contractor (including LANL) membership to develop NNSA's ISSM path forward. His memoranda strongly reflect and further validate LANL's CY00 initial rollout and continuing ISSM efforts, stating "The success of our national security mission depends on a commitment to excellence in all work we perform…" and that ISSM supports this mission "…while protecting our nation's most valuable information and materials."

To this end, General Gordon has consistently stressed that this must be done in a manner that promotes and nurtures the co-existence of science and security, stating "Each of us must understand the safeguards and security program, and what needs to be protected and why. We need to be able to ask security questions, obtain answers, and propose changes that will improve

NNSA security. In summary, each of us must take ownership of safeguards and security responsibilities in the workplace." LANL's ISSM Communications Plan promotes each of these expectations as well as the ISSM guiding principles and core functions (5-step process) shown in one of the attachments to General Gordon's memoranda.

Partnering for ISSM Success

ISSM success will require teamwork between and mutual understanding among all workers and managers. In turn, teamwork and mutual understanding depend greatly on effective and ongoing communications and interactions throughout the organization. Workers must have the means to improve the security processes and requirements by communicating problems and solutions to their managers, and managers must be able to communicate decisions and directions to the workforce. Managers must also be supportive and accessible to the workforce and responsive to their concerns -- seeking, promoting, and rewarding meaningful worker participation. Positive support, recognition, and endorsement of workers by their immediate supervisors for the contributions they make to security are key to having active worker participation. Managers also need to mentor workers to develop security-responsible behaviors for there to be meaningful participation. Additionally, LANL is striving to enhance its institutional processes for promoting employee awareness and soliciting employee input/feedback (see Attachment Three). All of this is essential for creating a worker-based security culture wherein:

- Everyone feels responsible for security and does something about it on a daily basis.
- Everyone goes beyond the call of duty to identify unsecure conditions and at risk behaviors, and they intervene to correct them.
- Secure work practices are supported with rewarding feedback from both peers and managers.
- Everyone "actively cares" continuously for the security of themselves and others and for the protection of security interests.
- Security is not considered a priority that can be conveniently shifted depending on the demands of the situation; rather security is considered a value linked with every priority of a given situation.

LANL is striving to achieve these cultural norms through the implementation of ISSM as supported by this Plan. Some key communications roles are outlined below:

Laboratory Workers

Including managers/supervisors, are responsible for continually:

- Understanding/using the ISSM 5-step process to perform their work securely and helping coworkers do the same, including discussing relative roles and responsibilities.
- Promoting security awareness, including actively sharing lessons learned with their coworkers.
- Seizing opportunities to provide input/feedback, especially for the development, implementation, and continuous improvement of security requirements and ISSM.

- Seeking help from their organizational security representatives and the Security Help Desk on security questions, concerns, and suggestions.
- Participating in security self-assessments and development of corrective actions.

Managers/Supervisors

Are also responsible for continually:

- Demonstrating their strong commitment to ISSM, including regularly communicating and using both the ISSM guiding principles and 5-step process.
- Promoting and reinforcing positive security values, attitudes, and behaviors throughout their organization.
- Promoting security awareness, including actively sharing lessons learned and starting all meetings with "safety and security first."
- Actively soliciting and responding to employee input/feedback, especially for development, implementation, and continuous improvement of security requirements and ISSM.
- Supporting and promoting the important role of their designated organizational security representatives (e.g., OSSOs, OCSRs, ADCs, CDCs et al.).
- Promoting use of the Security Help Desk to assist with security questions, concerns, and suggestions.
- Using management walk-arounds to promote ISSM communications and to engage workers in security self-assessments and development of corrective actions.
- Helping all workers achieve success with ISSM, including maintaining effective and efficient security communications processes within their organization.

Organizational Security Representatives

These personnel serve as a vital link between their own line-organization colleagues and the security subject matter experts (SMEs) who reside in institutional support organizations. Examples include OSSOs, OCSRs, ADCs, CDCs et al. They are responsible for continually:

- Promoting security awareness, including actively sharing lessons learned with all affected workers (including managers/supervisors) in their organization.
- Actively soliciting and responding to employee input/feedback, especially for development, implementation, and continuous improvement of security requirements and ISSM.
- Providing security assistance, including on-the-job security training, to workers within their organization, and encouraging use of the Security Help Desk.
- Assisting with assessments of their organization's security performance and informing their managers/supervisors of security issues requiring their leadership/support.
- Helping all workers achieve success with ISSM, including maintaining effective and efficient security communications processes within their organization.

Institutional Security Subject Matter Experts (SMEs)

These personnel reside in institutional support organizations (e.g., S-Division, CIO/CCN, ISEC). They are responsible for continually:

- Promoting security awareness, including actively sharing lessons learned with all affected workers (including managers/supervisors) Labwide.
- Actively soliciting and responding to employee input/feedback, especially for development, implementation, and continuous improvement of security requirements and ISSM.
- Encouraging all workers to use the Security Help Desk for assistance with security questions, concerns, and suggestions.
- Assisting with assessments of organizational and Labwide security performance and informing managers/supervisors of security issues requiring their leadership/support.
- Helping all workers achieve success with ISSM, including maintaining effective and efficient Labwide security communications processes.

LANL-NNSA Teamwork

Sustaining the LANL-NNSA ISSM partnership already underway, including shared goals/fate and an integrated team approach, will help ensure our ISSM success. To this end, continued joint participation on NNSA's SSMIT and LANL's ISSM Steering Team contribute greatly.

LANL Communications Processes

LANL employs a variety of formal and informal communications processes. To be effective, vertical communications among different levels in the security-responsible line-management chain must be two-way. This means information must be passed up and down the hierarchy without distorting the intent or content. Lateral communication between members of a single organization and between different organizations promotes the sharing of experience, security concerns, and solutions to problems, consistent with the need to know. Lateral communications must also be two-way. LANL is committed to continually improving all of its communications processes for promoting employee awareness and soliciting employee input/feedback to support the accomplishment of our vital national security mission in a safe, secure, reliable, and cost-effective manner. Collectively, these processes must serve to:

- Foster positive security values, attitudes, and behaviors in the workplace through demonstrated management commitment and active workforce participation.
- Continuously promote security awareness among all employees.
- Continuously solicit and respond to employee input and feedback to help ensure programmatic and operational considerations are taken into full account.
- Enhance employee understanding of their security responsibilities and of the resources available to assist them.
- Establish a clear, consistent voice among LANL's security professionals who provide guidance and other assistance.

- Target security communications to specific audiences to ensure relevancy and to avoid information overload.
- Enhance security training for new employees and incumbents, including general, job-specific, and periodic refresher training.
- Identify and communicate incident root causes and lessons learned to enhance awareness and help prevent recurrence.
- Engage the workforce in continually evaluating and improving the effectiveness of communications processes through focus groups, interviews, checkpoint surveys, etc.

To this end, the LANL Public Affairs Office (PAO) serves as a major resource for improving ISSM communications and providing a variety of forums to facilitate communications. They provide technical guidance and assistance in: communicating effectively with internal customers; developing effective communications processes and tools; and providing a central voice to reach all segments of the Laboratory. They also coordinate assistance from external communications experts as the need arises.

PHASE II STRATEGY

As stated earlier, this current phase focuses on putting ISSM in place to support our vital national security mission. It builds on Phase I efforts to develop and implement ISSM, with continued strong emphasis on demonstrated management commitment and active workforce participation to achieve buy-in and ownership. The strategy for promoting employee awareness and soliciting employee input/feedback during this phase is outlined below as major monthly actions, which are supported and augmented by the communications processes listed in Attachment Three. These actions extend only through September 2001 because we intend to update our strategy in that timeframe to specify the actions necessary to support the emergent ISSM gap analysis and DOE-approved ISSM action plan. Note that actions outlined below exceed NNSA expectations shown in the "Six-Month Actions (Mar-Aug 2001)" attachment provided with General Gordon's March 26 memoranda (see Attachment Two).

JANUARY 2001
NNSA Expectation: NONE

LANL Actions:
(1) Continued Labwide postings/briefings of Director John Browne's new "Safety and Security Policy," which begins with the quote, *"We will never compromise safety or security for programmatic or operational needs."*; **(2)** continued starting Labwide meetings with a "Safety and Security First" message, including regular "All Employees" and "All Managers" meetings, weekly Laboratory Information Meetings (LIMs), etc.; **(3)** continued maintaining/updating the ISSM website established in July 2000 to support CY00 Labwide ISSM rollout; **(4)** continued maintaining the "virtual" (telephone and e-mail-based) Security Help Desk, which provides a single point of contact ("one-stop" shopping) for employees with security questions, concerns, and suggestions; **(5)** continued publishing web-based fact sheets and frequently asked questions/

FAQs stemming from the CY00 Labwide ISSM rollout; **(6)** continued publishing key ISSM messages in the Los Alamos Newsbulletin/News Letter, including the new regular feature, "ISSM Corner"; **(7)** continued supporting the large cross-directorate, employee-based ISSM Steering Team (with invited NNSA/LAAO membership) chartered in early CY00 to guide/track ISSM development and implementation, including new CY01 ISSM contractual expectations; **(8)** continued supporting the three large cross-directorate, employee-based focus teams chartered to develop an integrated set of three security Laboratory Implementation Requirements (LIRs) – General Security, Classified Security, and Nuclear Safeguards – to simplify, streamline, and replace the fragmented and overwhelming collection of current Lab security requirements; and **(9)** continued supporting the large cross-directorate, employee-based ISSM Positive Security Behaviors Team chartered last fall by the ISSM Steering Team to assess the health of the Lab's prevailing security environment and make recommendations for improvement.

FEBRUARY 2001
NNSA Expectation: NONE

LANL Actions:
(1) Continued actions (1) – (9) shown for January.

MARCH 2001
NNSA Expectation:
Introduce ISSM at site (e.g., site management letter, all hands); and evaluate current security requirements per NNSA guidance.

LANL Actions:
(1) Accomplished the NNSA expectation for March by proactively completing in CY00 the Phase-I Labwide development, rollout, and initial implementation of ISSM; by continuing actions (1) – (9) shown for January; and by initiating/coordinating Labwide participation in the ongoing NNSA 6-month moratorium (and related "Hamre Commission" effort) aimed at soliciting employee input/feedback on improving current DOE Security Directives and their implementation; **(2)** in addition, completed the final report of the employee-based ISSM Positive Security Behaviors Team, which provides major employee input for the development of LANL's ISSM gap analysis and action plan; **(3)** prominently displayed large outdoor banners (several feet in length/width) at major technical areas, with each banner showing one of the ISSM guiding principles (e.g., work-tailored controls), rotated them weekly, and simultaneously displayed them daily on the Lab homepage; and **(4)** coordinated Labwide input/feedback to this Plan.

APRIL 2001
NNSA Expectation:
Develop ISSM website; develop feedback mechanism (e.g., help desk, e-mail, hotline, focus groups); and conduct awareness campaign (e.g., posters, fact sheets).

LANL Actions:
(1) Accomplished the NNSA expectation for April by continuing actions (1) – (8) shown for January [action (9) was completed in March], including maintaining/updating the ISSM website, maintaining the Security Help Desk, maintaining/updating the web-based fact sheets and frequently asked questions/FAQs, coordinating Labwide input/feedback for developing/ implementing ISSM, including meeting new ISSM contractual expectations, etc.; and by continuing the employee-based NNSA moratorium and ISSM "banner" actions since March; **(2)** in addition, will begin conducting new mandatory General Employee Training (GET) that includes a major new ISSM module; and **(3)** plan to roll out by end of April, for 60-day Labwide review/feedback, the new integrated set of three draft security LIRs [see action (8) for January].

MAY 2001
NNSA Expectation:
Distribute ISSM trinkets/give-aways provided by NNSA; improve two-way communications with employees; and conduct awareness campaign (e.g., posters, fact sheets).

LANL Actions:
(1) Accomplish the NNSA expectation for May by acquiring/distributing ISSM trinkets/give-aways to employees; by continuing actions (1) – (8) shown for January, including maintaining/ updating the ISSM website, maintaining the Security Help Desk, maintaining/updating the web-based fact sheets and frequently asked questions/FAQs, coordinating Labwide input/feedback for developing/implementing ISSM, including meeting new ISSM contractual expectations, etc.; and by continuing the employee-based NNSA moratorium and ISSM "banner" actions since March; **(2)** in addition, will begin conducting new mandatory Annual Security Refresher Training that includes a major new ISSM module; and **(3)** continue coordinating Labwide review/feedback for refining the integrated set of three draft security LIRs developed by employee-based focus teams and rolled out in April.

JUNE 2001
NNSA Expectation:
Update ISSM website; have employees identify opportunities for further security integration/ improvement (e.g., focus groups, surveys); and conduct awareness campaign (e.g., posters, fact sheets).

LANL Actions:
(1) Accomplish the NNSA expectation for June by continuing actions (1) – (8) shown for January, including maintaining/updating the ISSM website, maintaining the Security Help Desk, maintaining/updating the web-based fact sheets and frequently asked questions/FAQs, coordinating Labwide input/feedback for developing/implementing ISSM, including meeting new ISSM contractual expectations, etc.; and by continuing the employee-based NNSA moratorium actions since March; and **(2)** in addition, will finish coordinating Labwide review/ feedback for refining the integrated set of three draft security LIRs developed by employee-based focus teams and rolled out in April, and coordinate management approval for their formal web-based publication.

JULY 2001

NNSA Expectation:
Submit results from security requirements review per NNSA guidance ("hiatus"); and conduct awareness campaign (e.g., posters, fact sheets).

LANL Actions:
(1) Accomplish the NNSA expectation for July by continuing actions (1) – (8) shown for January, including maintaining/updating the ISSM website, maintaining the Security Help Desk, maintaining/updating the web-based fact sheets and frequently asked questions/FAQs, coordinating Labwide input/feedback for developing/implementing ISSM, including meeting new ISSM contractual expectations, etc.; and by completing the employee-based NNSA moratorium actions since March, consistent with NNSA guidance; and **(2)** in addition, will formally publish the management approved set of integrated security LIRs developed by employee-based focus teams to simplify, streamline, and replace the fragmented and overwhelming collection of current Lab security requirements.

AUGUST 2001

NNSA Expectation:
Update ISSM website; provide ISSM feedback; and conduct awareness campaign (e.g., posters, fact sheets).

LANL Actions:
(1) Accomplish the NNSA expectation for August by continuing actions (1) – (7) shown for January [action (8) was completed in July], including maintaining/updating the ISSM website, maintaining the Security Help Desk, maintaining/updating the web-based fact sheets and frequently asked questions/FAQs, and coordinating Labwide input/feedback for developing/implementing ISSM, including meeting new ISSM contractual expectations, etc.; and **(2)** in addition, will provide ISSM feedback to the NNSA community through General Gordon's SSMIT, on which LANL serves as a charter member and active participant.

SEPTEMBER 2001

NNSA Expectations: NONE

LANL Actions:
(1) Continue actions (1) – (7) shown for January, including maintaining/updating the ISSM website, maintaining the Security Help Desk, maintaining/updating the web-based fact sheets and frequently asked questions/FAQs, and coordinating Labwide input/feedback for developing/implementing ISSM, including meeting new ISSM contractual expectations, etc.; and **(2)** in addition, will update our Phase II communications strategy to specify actions necessary to support the emergent ISSM gap analysis and DOE-approved ISSM action plan.

ATTACHMENT ONE: LANL's CY00 ISSM Rollout Accomplishments

In early CY00, LANL initiated the development of Integrated Safeguards and Security Management (ISSM), which is modeled after Integrated Safety Management (ISM). LANL Director John Browne launched this new initiative because ISM's basic tenets -- management commitment, worker involvement, line "ownership," clearly defined roles and responsibilities, work and worker authorization, self-assessment, continuous improvement, etc. -- are vital to the success of both safety and security at LANL. Pursuing ISSM offers not only a stronger Labwide security culture and enhanced security performance, but a unified management model for achieving cost-effective operational excellence (safety and security).

On July 18, 2000, following initial ISSM development, John Browne held a mandatory "all hands" meeting to reaffirm the vital importance of ISSM and to initiate a Labwide rollout. The rollout centered on Labwide ISSM workshops involving the entire workforce and aimed at enhancing security awareness, commitment, and performance. Workshops were strongly supported by line management and highly interactive and tailored to the work of individual divisions, groups, and offices to maximize their value. Participants learned to apply the ISSM 5-step process and openly shared their security questions, concerns, and suggestions. These were addressed during or shortly after the workshops with the help of security experts within the line organizations, S Division, and Internal Security.

The next step in ISSM rollout was the establishment of Individual Performance Objectives (IPOs) for 2000-2001, which employees developed with their supervisors. ISSM IPOs were tailored to individual work duties and security responsibilities. These IPOs serve as a tool for clearly defining security expectations and discussing how best to achieve them. Moreover, IPOs are written in a positive tone to promote positive security behaviors, including encouraging employees to stay involved in the ISSM process and continually seek ways to improve the security of their work and the work around them.

Employee feedback on the initial ISSM rollout was positive. Of the more than 10,000 workshop participants, a random sample of 1000 reported a better understanding of their security roles after the workshops and scored them high. Also, following the workshops, a large cross-directorate ISSM Positive Security Behaviors Team was formed to recommend actions for ensuring a positive Labwide security environment where people feel free to express their views, voice concerns, and report security incidents. Their recommendations are being incorporated into LANL's ISSM path forward. For more information on the ISSM rollout and other major ISSM actions and accomplishments in CY00, see below and visit the LANL ISSM website.

Summary of LANL's major ISSM actions and accomplishments in CY00:

1. The LANL Director committed to Labwide ISSM implementation and informed the LANL workforce, UCOP, DOE, NNSA, and Congress.
2. Appointed Dick Burick/DLDOPS as DIR Champion for ISSM.

3. Appointed Jon Weisheit/X-DO as Technical Division Director Champion for ISSM.
4. Appointed Carl Ostenak/S-DO as ISSM Program Manager.
5. Established cross-directorate LANL-NNSA ISSM Steering Team.
6. Initiated and led Tri-Lab (LANL, LLNL, SNL) ISSM collaborations.
7. Served as LANL rep on NNSA-Contractor S&S Management Integration Team (SSMIT) to develop/guide ISSM.
8. Partnered with UCOP and LLNL to develop the ISSM portion of Appendix O.
9. Developed ISSM concepts, gained SET, OWG, and LIM support, and briefed all LANL managers.
10. Briefed senior DOE, NNSA, and UC officials on ISSM concepts and gained their full support.
11. Developed/issued DIR-approved "Safety and Security Policy" to supersede "ES&H Policy."
12. Initiated "Safety and Security First" (vs. only Safety First) at "All Employees" & "All Managers" meetings, senior management LIMs, and other meetings Labwide.
13. Initiated new LIM "Security First" venue whereby division directors brief DOE-reportable security incidents that occur within their divisions, especially causes and lessons learned.
14. Promoted active use of the Management Walk-around System for safety <u>and</u> security.
15. Developed draft "ISSM System Description" (ISM analog) and solicited Labwide feedback.
16. Developed draft "ISSM Laboratory Performance Requirement (LPR)" (ISM analog) and solicited Labwide feedback.
17. Initiated overhaul of current institutional security requirements by forming three focus teams with line/program/support workers to draft three highly integrated security Laboratory Implementation Requirements (LIRs) -- General Security, Classified Security, Nuclear Safeguards -- for Labwide review/comment.
18. Developed/piloted "Integrated S&S Assessment Visits" whereby security SMEs partner with divisions in jointly performing integrated/full-scope (vs. stovepiped) internal security assessments.
19. Established "one-stop" Security Help Desk to expeditiously coordinate/provide responses to worker questions, concerns, and suggestions.
20. Created ISSM website for Labwide access to ISSM information, including the basic components, approach, FAQs, and employee opportunities to actively participate.
21. Launched Labwide ISSM rollout via LANL Director John Browne's 7-18-00 mandatory "All Hands" meeting followed by highly interactive/tailored worker-based ISSM Workshops, including extensive web-based ISSM exercises/tools for enhancing security awareness, commitment, and performance.
22. Established post-ISSM Workshop "ISSM Individual Performance Objectives (IPOs)" for 2000-2001 by partnering employees with their supervisors to develop ISSM IPOs tailored to their individual work duties and security responsibilities.
23. Formed a large cross-directorate ISSM Positive Security Behaviors Team to recommend actions for ensuring a positive Labwide security environment where people feel free to express their views, voice concerns, and report security incidents.

24. Initiated revision of general employee training (GET) and annual security awareness training to include ISSM expectations.
25. Developed/published ISSM updates in the Labwide Newsbulletin and the new Los Alamos News Letter (regular "ISSM Corner").
26. Provided monthly ISSM progress reports to the SET and distributed to all LANL "Leaders" along with security-incident data/trends.

The three pages that follow show, respectively: (1) LANL's CY00 major ISSM rollout milestones (column headings) and "all green" progress chart; (2) the positive employee feedback received on the ISSM rollout; and (3) the homepage for the ISSM website, which has been up and running since July 2000 in support of LANL's CY00 rollout and ongoing ISSM efforts.

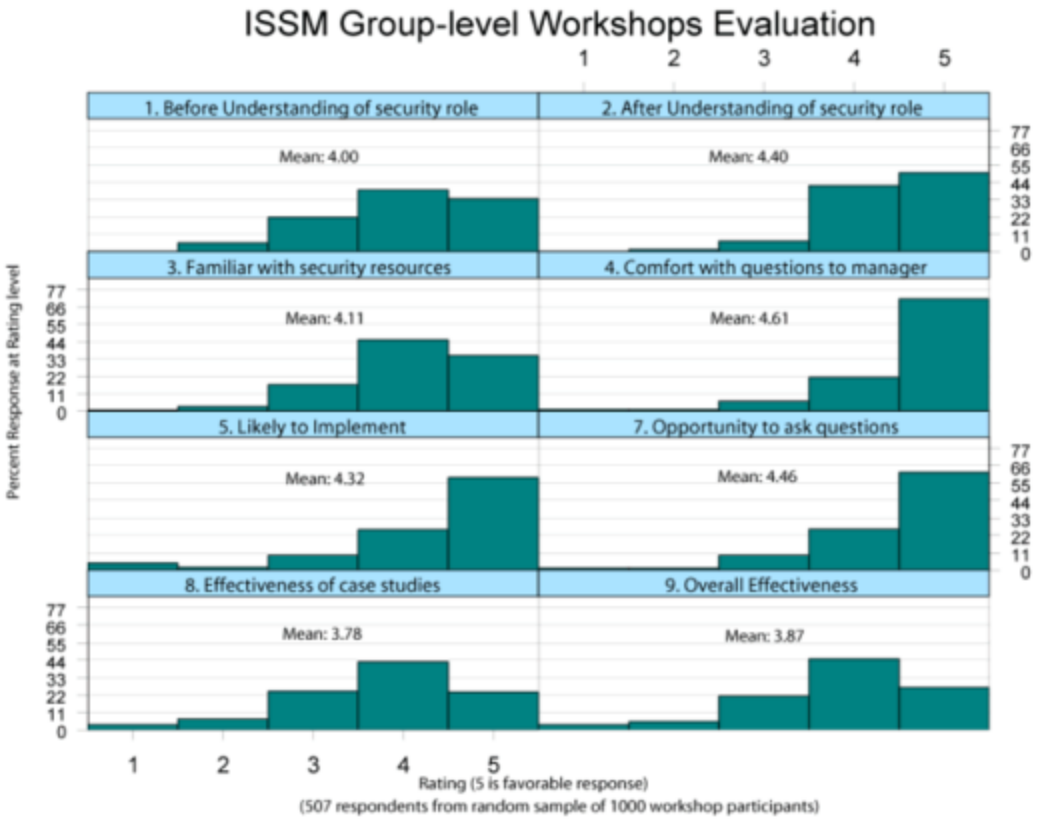
LANL's CY00 Major ISSM Rollout Milestones & "All Green" Progress Chart

Organization	Jul 3 '00	Jul 18	Jul 18	By Aug 31	By Aug 31	By Aug 31	By Aug 31	By Aug 31	By Aug 31	By Sept 15	By Oct 15	By Nov 30 '00
	LANL Director John Browne Sent Memoranda to "All Managers" and "All Employees" Announcing the Labwide ISSM Rollout	LANL Director John Browne Led Mandatory "All Hands" Kickoff Meeting for ISSM Rollout	Division Attended (or subsequently made up) Director John Browne's July 18 "All Hands" ISSM Meeting	Division-level Director Led "All Managers" ISSM Workshop Planning Session for Their Division	Division-level Director Led "All Hands" ISSM Meeting for Their Division (optional)	Group-level Managers Identified "Target Audience" for Their ISSM Workshops	Group-level Managers Led Their ISSM Workshops	Documented/Reported Attendance for Group-level ISSM Workshops	Submitted Group-level Summary Reports to Cognizant Division-level Director, Including Unresolved Questions, Concerns, Suggestions	Submitted Division–level Summary Reports to Cognizant ALD or DLD, Including Unresolved Questions, Concerns, Suggestions	Division Management Team Informed Their Workforce of Actions Taken and/or Underway on Submitted Questions, Concerns, Suggestions	Completed 1-on-1 Employee/Supervisor Meetings to Establish a 2000-2001 Individual Performance Objective (IPO) for ISSM/Security Responsibilities
AA												
B												
BUS												
C												
CCN												
CCS												
CER												
DIR												
DVO												
DX												
E												
EES												
ESA												
ESH												
ESS												
FWO												
HR												
IBD												
IM												
ISEC												
JCNNM												
LANSCE												
LC												
MST												
NIS												
NMT												
NW												
OEO												
OMBUDS												
P												
PM												
PTLA												
QIO												
S												
SNS												
SSR												
STB												
T												
TR												
TSA												
X												

Positive Employee Feedback on LANL's CY00 ISSM Rollout

.

[NOTE: Of more than 10,000 participants, a random sample of 1000 (507 respondents) reported better understanding of their security roles and a high likelihood to implement what they learned about ISSM.]



Homepage for LANL's ISSM Website

[NOTE: This website has been up and running since July 2000 in support of LANL's CY00 ISSM rollout and ongoing ISSM efforts.]

ATTACHMENT TWO: General Gordon's CY01 ISSM Rollout Initiation

[NOTE: This attachment provides General Gordon's March 26, 2001, memoranda committing the entire NNSA complex (Federal and contractor) to ISSM.]

Department of Energy
National Nuclear Security Administration
Washington, DC 20585

March 26, 2001

MEMORANDUM FOR DISTRIBUTION

FROM: JOHN A. GORDON
ADMINISTRATOR

SUBJECT: IMPLEMENTATION OF "INTEGRATED SAFEGUARDS AND SECURITY MANAGEMENT" FOR THE NATIONAL NUCLEAR SECURITY ADMINISTRATION (NNSA)

The success of our national security mission depends on a commitment to excellence in all work we perform throughout all the facilities of the nuclear weapons complex. Each of us must understand the safeguards and security program, and what needs to be protected and why. We need to be able to ask security questions, obtain answers, and propose changes that will improve NNSA security. In summary, each of us must take ownership of safeguards and security responsibilities in the workplace.

To this end, the NNSA is developing an "Integrated Safeguards and Security Management" (ISSM) to integrate safeguards and security into our management and work practices at all levels of effort from policy making to field implementation. Both Federal and contractor employees must merge the Department's safeguards and security program into their day-to-day work so that our mission requirements are accomplished using the best practices available. The Chief of Defense Nuclear Security has chartered the NNSA ISSM Executive Council (Attachment 1) to develop components that will engage each of us in this security process. Over the next six months specific ISSM goals and objectives (Attachment 2) will be implemented that include a moratorium on the implementation of new security policies and the development of mechanisms to receive and respond to suggestions and feedback. These mechanisms or components are described in Attachment 3.

Additionally, I am sending a letter to all employees introducing ISSM, describing the purpose of the moratorium, and soliciting their suggestions and feedback. I need the support of all personnel to ensure we derive the benefits of ISSM.

I recognize NNSA field offices and operating contractors possess intimate site knowledge on how to implement Department of Energy policy to achieve integration of safeguards and security into day-to-day operations. To fully implement ISSM, NNSA offices and contractors will develop site-specific approaches to ISSM.

This effort supports NNSA's national security mission, while protecting our nation's most valuable information and materials. I am counting on your personal support and commitment to ISSM.

Please contact me personally if you have questions concerning this program, or the Chief of Defense Nuclear Security, John C. Todd at (202) 586-2545.

Attachments

Printed with soy ink on recycled paper

DISTRIBUTION:

CN-1
CR-1
DP-1
EH-1
EM-1
GC-1
IG-1
MA-1
MD-1
NA-3
NE-1
NN-1
NR-1
OA-1
SC-1
SO-1
Manager, Albuquerque Operations Office
Manager, Chicago Operations Office
Manager, Nevada Operations Office
Manager, Oakland Operations Office
Manager, Richland Operations Office
Manager, Savannah River Operations Office
Manager, Amarillo Area Office
Manager, Kansas City Area Office
Manager, Kirtland Area Office
Manager, Los Alamos Area Office
President, Sandia National Laboratories
Director, Los Alamos National Laboratory
Director, Lawrence Livermore National Laboratory
Director, Oak Ridge National Laboratory
General Manager, Mason and Hanger, Day and Zimmerman, Inc., Pantex Plant
President, Honeywell Federal Manufacturing Technologies, Kansas City Plant
President, Westinghouse Savannah River Company

NATIONAL NUCLEAR SECURITY ADMINISTRATION
OFFICE OF THE CHIEF DEFENSE NUCLEAR SECURITY

INTEGRATED SAFEGUARDS AND SECURITY MANAGEMENT EXECUTIVE COUNCIL

CHARTER

1. PURPOSE:

This Charter establishes:

a. The organization, responsibilities and procedures for the Department of Energy, National Nuclear Security Administration, "*Integrated Safeguards and Security Management Executive Council*;" and

b. It also formerly establishes the "*Safeguards and Security Management Integration Team*" (SSMIT) as a working group of the Council, and defines its roles and responsibilities.

2. RESPONSIBILITIES:

a. The Executive Council is responsible for the following activities:

- Prepares proposals for safeguards and security program improvements in the NNSA;
- Develops and maintains an annual ISSM program plan;
- Develops strategies for more effective ISSM implementation;
- Coordinates lessons learned, best practices, and cost-effective safeguards and security training and education methodologies with DOE, and other Departments and Agencies;
- Appoints a liaison representative to other safeguards and security committees, quality panels, and focus groups for ISSM;
- Directs SSMIT activities; and
- Prepares an annual report concerning ISSM activities in the NNSA during the preceding calendar year for the Administrator, NNSA.

b. The Chief, Defense Nuclear Security.

- Appoints the Chairman of the Executive Council.
- Coordinates the ISSM Program annual report and forwards the report as necessary to the Administrator, NNSA.

3. CHAIRMAN:

a. The Chairman conducts meetings of the Executive Council, approves the minutes of the meetings, and supervises the activities of the Executive Secretary.

b. The Chairman conducts meetings of the SSMIT and approves minutes of the meetings of that organization.

4. MEMBERS:

a. Headquarters Program Offices, Operations Offices, Area Offices, and contractors of the nuclear weapons complex are invited to nominate members to participate on the Executive Council from the resident safeguards and security management staff. Nominations should be forwarded to the Chairman of the Council for review, comment and concurrence.

b. The initial membership, advisors, and observers list, attachment 1, was developed to continue the participation of individuals who have helped to develop ISSM as a major project initiative.

5. EXECUTIVE SECRETARY:

The Chairman of the Executive Council will appoint a staff member to be responsible for recording and distributing the minutes of the meetings of the Council, and conducting and coordinating other routine Council business.

6. ADVISORS:

Members of the NNSA Safeguards and Security Management Integration Team (SSMIT) are permanent advisors to the Executive Council and may be invited by the Chairman to participate in Executive Council meetings.

7. OBSERVERS:

Observers are welcome from Department of Energy organizations and other U.S. Government Departments or Agencies. Organization heads are requested to nominate permanent observers to the Executive Council, and to notify the Chief Défense Nuclear Security and the Council Chairman in writing of their intention to send observers to meetings.

8. AUTHORITY:

a. Authority and responsibility for the development and implementation of security programs for the Administration by the Chief of Defense Nuclear Security is provided by Public Law 106-65, Section 3232(c).

"(3) The Chief shall be responsible for the development and implementation of security programs for the Administration, including the protection, control and accounting of materials, and for the physical and cyber security for all facilities of the Administration."

b. Authority for specific DOE-NNSA cooperation and coordination on joint safeguards and security policy and implementation was provided by the Administrator in a memorandum subject: *Implementation of Integrated Safeguards and Security Management for the NNSA*.

c. The NNSA ISSM Executive Council makes decisions on a consensus basis. If at any point, members are unable to reach consensus on an issue, by majority vote, the issue will be forwarded to the Chief, Defense Nuclear Security for decision.

d. Upon approval, the Chief Defense Nuclear Security has authority to approve changes to this charter.

9. MEETINGS:

The NNSA ISSM Executive Council holds meetings on a quarterly basis or at the call of the Chairman.

A report of the minutes of each meeting is forwarded to the Chairman by the Executive Secretary for review and approval. The report is subsequently forwarded to the Chief Defense Nuclear Security, and the Administrator for action or information as appropriate.

10. SAFEGUARDS AND SECURITY MANAGEMENT INTEGRATION TEAM [SSMIT]:

The SSMIT is the staff level working group of the Executive Council. It conducts business under a charter approved by the Chief, Defense Nuclear Security.

APPROVED:

John A. Gordon
Administrator

DATE: MARCH 26, 2001

MEMBERSHIP LIST

CHAIR:

Larry Kirkman, NNSA/AL/OSS

MEMBERS:

Wayne Adams, NV
Shirley Baker, Chairperson NSIE* and KCP
Duane Gordon, OAK
Roger Hagengruber, SNL-NM
Kevin Hall, SR
William E. Nay, DOE/HQ/SC-80
Terry Owens, UC (LLNL/LANL)*
Donat St.Pierre, OR
Donald Solich, DOE/HQ/SO -21
Jon H. Todd, NNSA/HQ/NA-3

ADVISORS/SSMIT MEMBERS:

John Abeles, DOE/HQ/SO-33
Lynn Cleland, LLNL
Sharon Daly, NNSA/AL/LAAO
Maurice Daugherty, DOE/HQ/EM
Leo Fisher, NNSA/AL/CI
Bill Gillison, NNSI/WSI
Leigh Gunn, DOE/HQ/EM-5
Kevin Hall, DOE/SR
Brenda Harmeson, NNSA/AL/SPSD
Bill Hensley, NNSA/HQ/DP
Jim Hickok, NNSI/WSI
Pat Hoopes, NNSA/AL/KCAO
Stu Jossey, LLNL
Bill Kilmartin, DOE/HQ/OA-10
Terri Lovato, SNL
Peggy Montoya, SNL
John O'Brien, NNSA/AL/AAO
Carl Ostenak, LANL
Daniel Pellegrino, NNSA/AL/ISRD
Bernard Pleau, NNSA/AL/OPA
Jon Potter, DOE/HQ/SO-211.3
John Przysucha, DOE/HQ/SO-33
Arminda Roberts, DOE/AL/ISRD
Barry Schwartz, SNL
Mark Thornock, DOE/HQ/SC
Edwin Tippens, LLNL
Debbie Volk, NNSA/AL/ISRD
Al West, SNL-NM
D. L. Whaley, DOE/HQ/OA-10
Garry Wisdom, NNSA/AL/AAO
Maggie Wood, NNSA/AL/KAO
Steven Yesner, SNL

* Designates Permanent Members

ATTACHMENT 2
Six Month Actions

MONTH	Owner/Deliverable	Themes	Purpose
March	NNSA-HQ: • Issue NNSA letters on ISSM • Present ISSM at S&S NNSA/Contractor Meeting on March 14 • Place Web Site online • Charter/Convene NNSA ISSM Executive Council SITE: • Introduce ISSM at Site (e.g., site management letter, all hands, video, management walkthroughs) • Evaluate current S&S requirements per NNSA guidance	Security is a real issue. ISSM is the path forward. What and why of ISSM.	NNSA roll-out of ISSM Obtain management buy-in
April	NNSA-HQ: • Prepare Facts Sheet/FAQs • Develop and distribute video SITE: • Develop web site • Develop feedback mechanism (e.g., help desk, email, hotline, focus groups) • Conduct awareness campaign (e.g. posters, fact sheets)	Engage workforce: Everyone is responsible. Your voice counts.	Initiate formal Site Roll-out
May	NNSA-HQ: • Purchase and distribute give-always SITE: • Distribute give always • Improve two-way communications with employees • Conduct Awareness Campaign (e.g., posters, fact sheets)	Continuous improvement-- Your voice counts.	Implementation of ISSM Program
June	NNSA-HQ: • Update and distribute Facts Sheet/FAQs SITE: • Update web page • Have employees identify opportunities for further integration/improvement (e.g., focus groups, surveys) • Conduct Awareness Campaign (e.g., posters, fact sheets)	Integration of security into day-to-day operations. Your voice counts.	Implementation of ISSM Program
July	NNSA-HQ: • Update Web site SITE: • Submit results from requirements review per NNSA guidance • Conduct Awareness Campaign (e.g., posters, fact sheets)	Your voice counts.	Continue the ISSM journey
August	NNSA-HQ: • Analyze feedback and determine path forward • Update and distribute Facts Sheet/FAQs • Develop Awards program SITE: • Update Web site • Provide ISSM feedback • Conduct Awareness Campaign (e.g., posters, fact sheets)	Process improvement.	Feedback & Improvement

ATTACHMENT 3
ISSM COMPONENTS

The NNSA is committed to conducting work efficiently and securely. To this end, ISSM will be used to systematically integrate safeguards and security into management and work practices at all levels so that missions are accomplished securely. Direct involvement of all personnel during the development and implementation of ISSM is essential for success.

The ISSM framework consists of six components:

(1) the objective,
(2) guiding principles,
(3) Core functions,
(4) Mechanisms,
(5) Responsibilities, and
(6) Implementation.

The objective, guiding principles, and core functions of ISSM will be used consistently throughout the NNSA complex. The mechanisms, responsibilities, and implementation components will be established by sites for all work.

COMPONENT 1 ***ISSM Objective***

Perform Work Securely. The ISSM framework will systematically integrate safeguards and security into management and work practices at all levels so those missions are accomplished securely.

COMPONENT 2 ***ISSM Guiding Principles***

The guiding principles are the fundamental policies that guide NNSA and contractor actions:

Individual Responsibility and Participation. Each individual is directly responsible for following security requirements, and contributing to secure missions and workplaces.

Line Management Responsibility for Safeguards and Security. Line management is directly responsible for the protection of the NNSA assets. Appropriate risk analysis is performed prior to work being authorized. Line management must accept residual risk and controls must be in place and verified prior to authorization of operations.

Clear Roles and Responsibilities. Clear and unambiguous lines of authority and responsibility for ensuring safeguards and security must be established and maintained at all organizational levels within the NNSA and its contractors.

Competence Commensurate with Responsibilities. Individuals must possess the experience, knowledge, skills, and abilities that are necessary to fulfill their responsibilities.

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

Identification of Safeguards and Security Standards and Requirements. Before work is performed, the associated risk must be evaluated and an agreed-upon set of safeguards and security standards and requirements shall be established which, when properly implemented, will provide appropriate assurance that NNSA assets are properly protected.

ATTACHMENT 3
ISSM COMPONENTS

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

COMPONENT 3 ***ISSM Core Functions***

These five core ISSM functions provide the necessary structure for any work activity. The functions are applied as a continuous cycle with the degree of rigor appropriate to address the type of work activity and the risk involved.

Define the Scope of Work. Missions are translated into work, potential requirements identified, expectations set, tasks identified, and prioritized, related security assets identified, and resources allocated.

Analyze the Risk. Risk associated with the work is analyzed to determine applicable Requirements.

Develop and Implement Security Measures. Measures and controls are tailored and implemented to mitigate risk. Line management accepts residual risk.

Perform Work within Measures and Controls. Authorized security measures are in place and work is performed accordingly.

Provide Feedback and Continuous Improvement. Feedback information on the adequacy of measures and controls is gathered. Opportunities for improving the definition and planning of work are identified and implemented. Best practices and lessons learned are shared.

COMPONENT 4 ***ISSM Mechanisms***

ISSM mechanisms are the information and tools used to implement the guiding principles and core functions. They may vary between facilities and activities based on the risk and the work being performed.

COMPONENT 5 ***ISSM Responsibilities***

Responsibilities must be clearly defined in documents appropriate to the activity. NNSA responsibilities are defined in internal NNSA directives. Contractor responsibilities are detailed in contracts, regulations, and contractor-specific procedures. Review and approval levels may vary, commensurate with the type of work and risk involved.

COMPONENT 6 ***ISSM Implementation***

Implementation involves integrating specific instances of defining and planning work, formally identifying and analyzing risk, developing and implementing measures and controls, performing work, and monitoring and assessing performance for feedback and improvement.

Department of Energy
National Nuclear Security Administration
Washington, DC 20585

March 26, 2001

MEMORANDUM FOR ALL NATIONAL NUCLEAR SECURITY ADMINISTRATION (NNSA) FEDERAL AND CONTRACTOR EMPLOYEES

FROM: JOHN A. GORDON
ADMINISTRATOR

SUBJECT: IMPLEMENTATION OF "INTEGRATED SAFEGUARDS AND SECURITY MANAGEMENT" IN THE NATIONAL NUCLEAR SECURITY ADMINISTRATION

Your personal efforts in overcoming our security challenges during a period of intense scrutiny are appreciated. I now need your help and commitment to continue enhancing security while keeping focused on our important national security mission.

We have an opportunity to build on past successes and benefit from the lessons we have learned. That's why I chartered the Safeguards and Security Management Integration Team (SSMIT) to develop Integrated Safeguards and Security Management (ISSM). This SSMIT has developed policy and guidance for ISSM. ISSM will integrate safeguards and security into management and work practices at all levels so missions are accomplished securely. It is designed so you will be involved in safeguards and security requirements. Subject matter experts will help you when you need guidance and information. We want to build on current safeguards and security practices to help you work more securely.

I have called for a six-month moratorium on the implementation of new safeguards and security policy. This allows us time to review past policies, identify policy improvements, and determine how policy can most effectively be implemented within NNSA. During this period, your input is critical to the process. Mechanisms will be developed to receive and respond to your suggestions and feedback within this ISSM framework.

Your personal commitment of protecting our nation's vital assets is center stage here. I have confidence that you, too, recognize the need to successfully address our security challenges. Once you learn more about ISSM, I'm sure that you will see it represents a sound approach to enhance security. We can make a difference if we take on this challenge and take control of our own issues and ideas.

Printed with soy ink on recycled paper

ATTACHMENT THREE: LANL Communications Processes

Promoting Employee Awareness

Employee awareness is critical to sustaining and continuously improving the security of day-to-day operations. To further promote and augment employee awareness derived from ongoing manager-worker and peer-peer communications, LANL is striving to enhance the institutional processes by which its security professionals can continually provide clear, simple, and value-adding security information to all employees. Always, care must be taken to avoid information overload by identifying target audiences for specific communications.

Awareness Tools

The primary institutional tools include the following:

- ***"Security First":*** Meetings throughout the Lab generally begin with a "safety and security first" message, including all regular "All Employees" and "All Managers" meetings, weekly Laboratory Information Meetings (LIMs), etc.
- ***ISSM Website:*** Up and running since July 2000 to support Labwide ISSM rollout, it includes information about ISSM components, communications, implementation, tools and resources, frequently asked questions (FAQs), and employee opportunities to actively participate ("Your Voice Counts").
- ***Safeguards & Security Website:*** Provides easily accessible information on all aspects of current security program, including cyber security, classified matter protection and control, personnel security, physical security, nuclear materials control and accountability, OPSEC, classification, etc. as well as FAQs.
- ***General Employee Training (GET):*** Provided to all new employees, it ensures that people joining the Laboratory are given essential security information before they begin work, including ISSM basics.
- ***Annual Security Refresher:*** All employees are required to review Laboratory security requirements annually and pass a self-test. This is a computer-based program being reengineered to include ISSM basics by May 2001.
- ***Additional Security Training:*** An extensive array of security courses, both classroom and computer-based, provides employees additional security training as their jobs demand throughout their Laboratory careers.
- ***State of Security Report:*** The annual State of Security Report outlines the current status and key challenges facing the LANL security program.
- ***Security Fact Sheets:*** Focused on specific topics, security fact sheets provide requirements in an easily understood format.
- ***LabNet Security Updates:*** Using internal television broadcasts, LabNet is a vital communications tool for focusing on security training and updates.

- ***Security Newsletter:*** Providing a periodic newsletter covering current security issues is important in providing employees with information relevant to their jobs.
- ***Biweekly Los Alamos News Letter:*** This general information newsletter includes the "ISSM Corner," which provides on-going information pertaining to the ISSM program.
- ***Daily LANL Newsbulletin:*** The daily on-line Newsbulletin is particularly useful in providing time-sensitive security information.
- ***Lessons Learned Program:*** The lessons learned program is essential to sharing key elements of successful security programs, as well as the events surrounding security "incidents" evaluated as part of the security incident program. Also, the weekly LIM "Security First" venue includes division directors briefing DOE-reportable security incidents that occur within their divisions, especially causes and lessons learned.
- ***Frequently Asked Questions (FAQ) Program:*** Geared toward particular security topics, FAQs can be very useful at providing employees with needed information.
- ***Poster Campaigns:*** Provide visual reinforcement of the need to maintain strong security programs. Examples include "I am Los Alamos Security" and "ISSM: How do you know?"
- ***Appendix-F Performance Measures:*** The metrics contained in the DOE/UC Appendix F program provide feedback on security performance.
- ***ISSM Trinkets/Give-Aways:*** Properly selected and distributed, usable items such as mouse pads, badge holders, pins, etc., can be highly effective in promoting ISSM and keeping security visible to all employees.
- ***Security Video Presentations:*** Videos are particularly useful in addressing a variety of awareness issues and can be widely disseminated to all levels of the organization.
- ***Security Concerns Program:*** This program, under development by Group S-2, will provide a clear path for reporting issues of security concern and will specifically address any classification issues associated with reporting potential security vulnerabilities.
- ***Special-Focus Publicity Campaigns:*** Focused on particular problems or projects, this tool seeks to ensure that employees clearly understand new or changing security requirements or procedures.
- ***Monthly ISSM Progress Reports:*** Provided to the Lab's Senior Executive Team (SET), Labwide "Leaders," and many Labwide line, program, and support managers and workers, it includes major ISSM progress updates as well as security-incident data/trends.

Measurement Tools

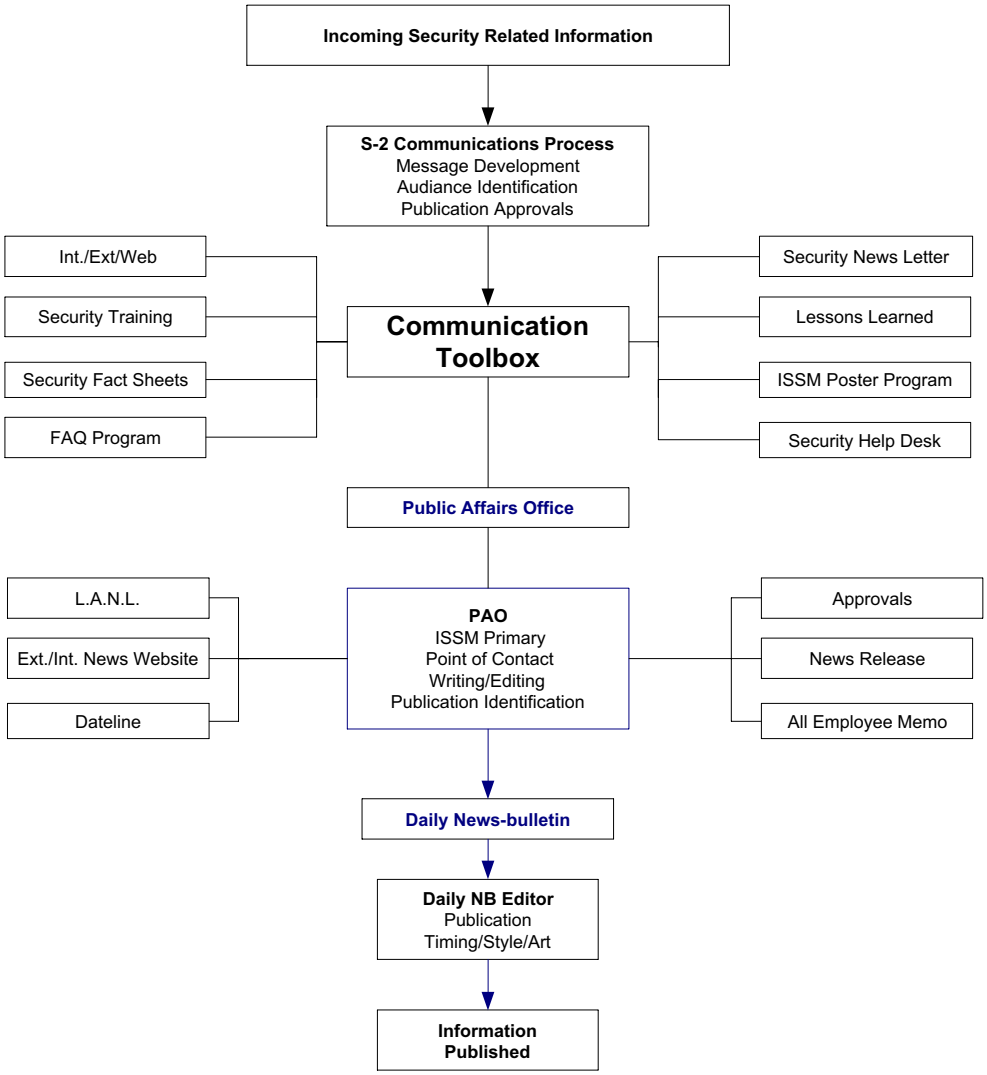
A variety of measurement tools will be used to measure the effectiveness of institutional processes aimed at promoting employee awareness. These include:

- ***ISSM Survey*** – A randomly sampled audience will be surveyed on an ongoing basis to assess their understanding of and satisfaction with ISSM.
- ***Checkpoint Survey*** – The Laboratory's Checkpoint Survey will provide Labwide data on how well Laboratory communications have been received by the workers.

- ***Focus Groups*** – Focus groups will continue to be formed to gather feedback and assess the effectiveness of security resources.
- Evaluation experts will be consulted to analyze data and suggest new evaluation methods.
- Training data will be analyzed and interviews will be conducted to assess retention and knowledge transference to the job.

Process Flow Chart

The flow chart below illustrates many of the institutional tools and pathways for promoting employee awareness:



Soliciting Employee Input/Feedback

Employee input and feedback (e.g., security questions, concerns, and suggestions) are critical to sustaining and continuously improving the security of day-to-day operations. To further promote and augment employee input/feedback derived from ongoing manager-worker and peer-peer communications, LANL is striving to enhance its institutional processes. These processes must effectively capture and respond to all such input/feedback to clearly demonstrate to employees that their voice is being heard and is appreciated.

Input/Feedback Tools

The primary institutional tools include the following:

- ***Security Help Desk:*** The S-Division "virtual" (telephone and e-mail-based) Security Help Desk serves to provide a single point of contact ("one-stop" shopping) for employees with security questions, concerns, and suggestions. The Help Desk is also instrumental in capturing input/feedback on the effectiveness of the Lab's communications, training, and policy formulation processes. Anonymity is an option.
- ***Organizational S&S Officer (OSSO) Program:*** OSSOs are the primary source of interaction between security staff and the line and program organizations.
- ***Security Topical Representatives:*** Representing a particular sub-topical area (e.g., Classified Document Custodians), they provide resident expertise within line organizations, assisting employees with accomplishing their security tasks.
- ***Facility Training Manager's Committee:*** Major training stakeholders from the Laboratory's nuclear facilities meet to resolve cross-facility training issues and to coordinate consistent training approaches.
- ***Designated Training Generalists:*** Training generalists and subject matter experts who provide feedback to the LANL Training Director to ensure a consistent approach to training programs and training tools used throughout the Laboratory.
- ***Laboratory Implementation Requirements (LIR) Focus Teams:*** LIRs serve to establish and communicate the essential institutional security requirements that must be followed when performing work. These teams are populated with major line/program stakeholders to ensure operational and programmatic input into the development of security requirements.
- ***RevCom and Appendix G Requirements Program:*** Under a newly developed process, line organizations are contributing to the review process for draft DOE Orders and to the acceptance process for adding orders to the DOE/UC contract.
- ***Mobile Briefing Program:*** This program, under development by Group S-2, will take security updates to line and program staff meetings, allowing for real-time feedback on important security issues.
- ***Division Security Days:*** This program, under development by Group S-2, will allow line and program organizations to focus employee attention on security-related aspects of their operations.
- ***Management Walk-Around Program:*** Through the use of subject matter guidance cards, this institutional management assessment tool is essential to providing line management

oversight of security activities, as well as serving as a key relationship-building tool for managers and employees.

- ***Self-Assessment Program:*** The assessment program is a critical feedback tool that provides for ongoing input for continuously improving security in support of the overall mission.
- ***Voice of the Customer Program:*** This program, under development by Group S-2, will collect pertinent information regarding the satisfaction of LANL employees with the services provided by the security staff.
- ***Ask the Director:*** Providing a direct link between employees and the Director, the "Ask the Director" program allows employees to communicate issues/concerns with security requirements and practices to the LANL Director. Anonymity is an option.
- ***Lab-Sanctioned Employee Groups:*** Employee groups such as the Employee Advisory Committee provide a formal input/feedback mechanism regarding security.
- ***Electronic Suggestion Boxes:*** This program, under development by Group S-2, will collect pertinent information regarding suggestions for improving the security program, as provided by LANL employees.
- ***Interactions with Security SMEs:*** Through their significant involvement in the line organization operations, SMEs serve as a useful feedback tool, capturing customer questions, concerns, and suggestions and ensuring follow-up actions.
- ***Customer Comment Cards:*** Primarily used in the Badge Office and Personnel Security Office, these cards capture the degree of satisfaction customers have with service delivery and provide the opportunity to capture suggestions for improving security. Source anonymity is an option.

Measurement Tools

Given that this Plan is a dynamic one, a critical goal of the evaluation process is to determine which tools for soliciting employee input/feedback are seen to be the most effective. The evaluation process has two parts:

- Having employees evaluate the survey instruments themselves to determine if the "right" questions are being asked, and
- Once employees help to identify the best survey instruments (i.e., those that ask the "right" questions), expanding the use of these instruments and eliminating or revising those instruments deemed ineffective.

A variety of measurement tools will be used to measure the effectiveness of institutional processes aimed at soliciting employee input/feedback. These include:

- ***ISSM Survey*** – A randomly sampled audience will be surveyed on an ongoing basis to assess their understanding of and satisfaction with ISSM.
- ***Checkpoint Survey*** – The Laboratory's Checkpoint Survey will provide Labwide data on how well Laboratory communications have been received by the workers.
- ***Focus Groups*** – Focus groups will continue to be formed to gather feedback and assess the effectiveness of security resources.

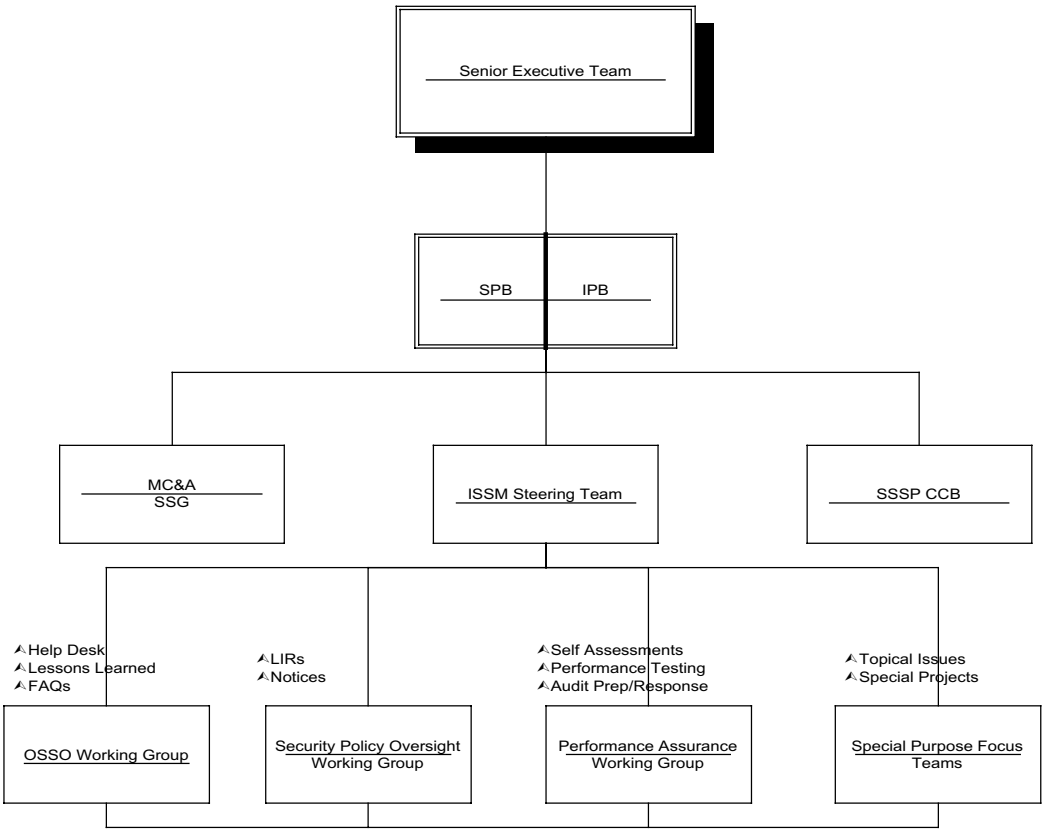
- ***Security Help Desk*** – Data analysis will be conducted to assess usability, trends, and informational gaps.
- Evaluation experts will be consulted to analyze data and suggest new evaluation methods.

Policy Input/Feedback Structure

As operations change or new security threats emerge, it is essential that employees who ultimately have to implement security requirements have a voice in their development. There must also be a clear source of decision-making that serves to prevent "security stovepipes" and that involves all impacted organizations in the decision process. When disputes arise, the policy process must elevate the issues to the appropriate level of line management for arbitration. To this end, the security-policy forums at LANL include the following:

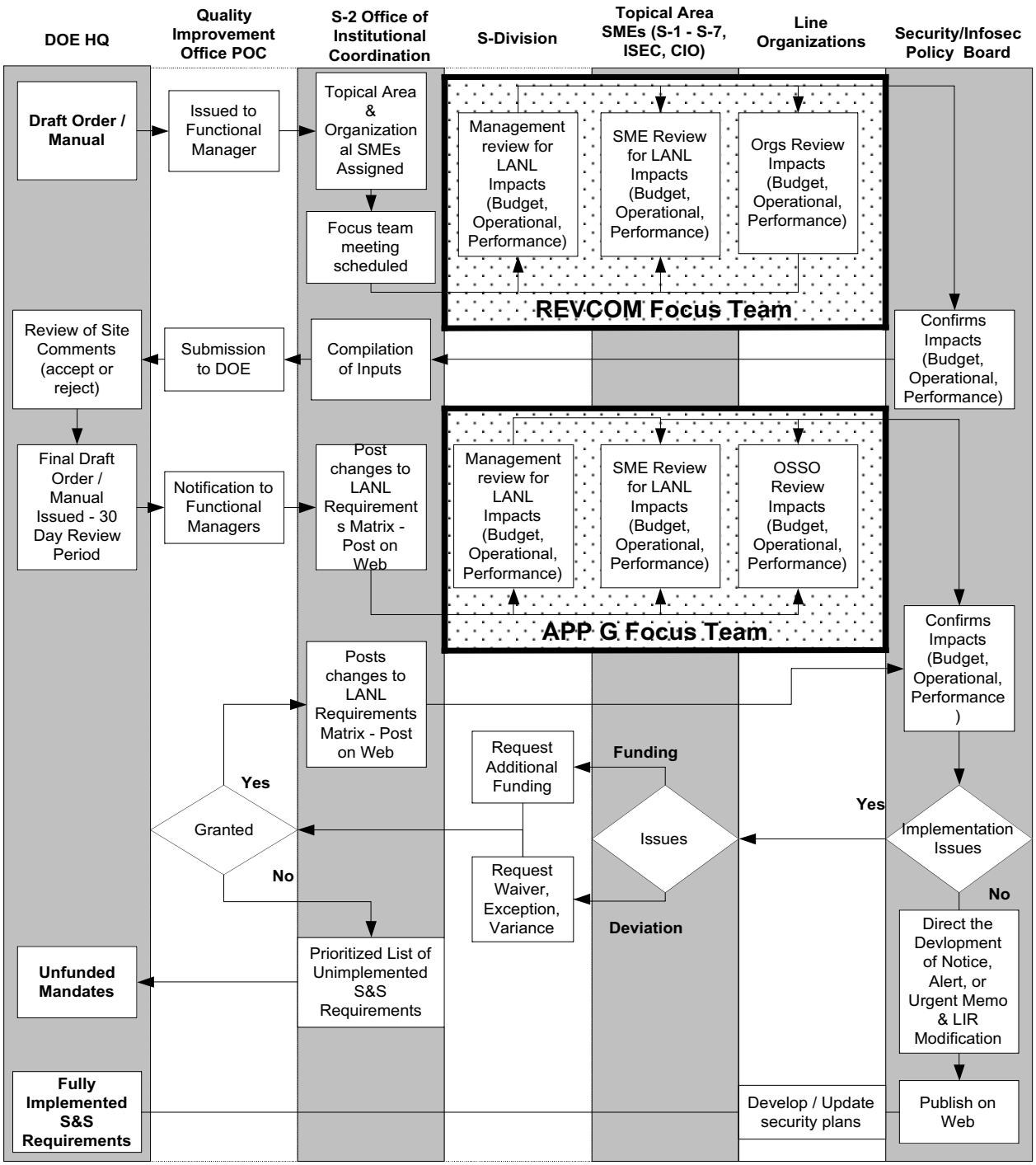
- ***Senior Executive Team (SET):*** The cross-directorate SET serves as the highest-level policy approval body.
- ***INFOSEC Policy Board (IPB):*** The cross-directorate IPB is responsible for guiding, reviewing, and approving all cyber-security policies.
- ***Physical Security/Counter Intelligence Policy Board:*** Referred to simply as the Security Policy Board (SPB), this cross-directorate Board is responsible for guiding, reviewing, and approving security policies, with the exception of cyber-security policy.
- ***SSSP Change Control Board:*** The SSSP/CCB, a joint LANL-NNSA team, comprising LANL line, program, and support personnel, is primarily focused on planning and policy issues regarding the protection of Category I/II SNM.
- ***MC&A Senior Steering Group (SSG):*** The SSG, a joint LANL-NNSA team, comprising LANL line, program, and support personnel, guides and oversees LANL nuclear safeguards.
- ***ISSM Steering Team:*** The large cross-directorate LANL ISSM Steering Team, comprising LANL line, program, and support personnel as well as invited NNSA/LAAO membership, guides and oversees the development and implementation of ISSM and serves as the principal security policy review/coordination body at LANL in support of the IPB and SPB (see above).
- ***LANL Security Working Groups:*** LANL uses a number of cross-directorate working groups to recommend security requirements to the appropriate LANL policy vetting/approval body.

Depicted below is the emerging structure for LANL's security policy process:



Policy Input/Feedback Process Flow Chart

Depicted below is the general process for soliciting and incorporating employee input/feedback in response to DOE's formulation of draft and final security requirements, which, in turn, drive LANL security requirements:


DOE HQ
Quality Improvement Office POC
S-2 Office of Institutional Coordination
S-Division
Topical Area SMEs (S-1 - S-7, ISEC, CIO)
Line Organizations
Security/Infosec Policy Board
Draft Order / Manual
Issued to Functional Manager
Topical Area & Organizational SMEs Assigned
Management review for LANL Impacts (Budget, Operational, Performance)
SME Review for LANL Impacts (Budget, Operational, Performance)
Orgs Review Impacts (Budget, Operational, Performance)
Focus team meeting scheduled
REVCOM Focus Team
Review of Site Comments (accept or reject)
Submission to DOE
Compilation of Inputs
Confirms Impacts (Budget, Operational, Performance)
Final Draft Order / Manual Issued - 30 Day Review Period
Notification to Functional Managers
Post changes to LANL Requirements Matrix - Post on Web
Management review for LANL Impacts (Budget, Operational, Performance)
SME Review for LANL Impacts (Budget, Operational, Performance)
OSSO Review Impacts (Budget, Operational, Performance)
APP G Focus Team
Confirms Impacts (Budget, Operational, Performance)
Posts changes to LANL Requirements Matrix - Post on Web
Request Additional Funding
Funding
Yes
Granted
Issues
Yes
Implementation Issues
No
Request Waiver, Exception, Variance
Deviation
No
Direct the Devlopment of Notice, Alert, or Urgent Memo & LIR Modification
Unfunded Mandates
Prioritized List of Unimplemented S&S Requirements
Fully Implemented S&S Requirements
Develop / Update security plans
Publish on Web

Worker-Based Security Serving Science & Society!

Los Alamos National Laboratory
Integrated Safeguards & Security Management

(5-31-01 Draft Revision)

Authored by the Joint LANL-NNSA ISSM Steering Team:

Carl Ostenak, DIR/ISSM, Chair
Dennis Brandt/Reuben Peck, NMT-DO
Sharon Eklund, S-1
Larry Freestone, S-6
Richard Kendall, DLDSTP/CIO
Kevin Leifheit, S-2
Lee McAtee/Phil Thullen, ESH-DO
Jo Ann Milam/Gerald Reisz, DLDBAO
Evelyn Mullen/Mary Carson, NIS-DO
Jake Perea/Jay Dallman, DX-DO
Susan Seestrom/Steve Greene, P-DO
Barb Stine/Candace Holmes/Jeff Stoddard, ALDNW
Sue Watters/Chris Webster, ALDSSR
Don Willerton, CCN-DO
Joel Williams, NW-M&M
Mary Anne Yates, ALDTR
Sharon Daly/Frank Ward, NNSA/LAAO

Contents

Figures v
Acronyms vi
Safety and Security Policy viii
Preface ix

1.0 INTRODUCTION TO ISSM 1
1.1. Terms of Reference 1
1.2. Worker-Manager Teamwork 2
1.3. Communications 3

2.0. ISSM DESCRIPTION 4
2.1. Objective 4
2.2. Eight Guiding Principles 4
2.3. Five-Step Process 5
2.3.1. Meeting Security Expectations 7
2.3.2. Application of the Five-Step Process 7
2.3.3. Tailoring Versus Uniformity in Application 7
2.3.4. Use of the Five-Step Process in Organizations 8

3.0. ROLES AND RESPONSIBILITIES 11
3.1. Basis in ISSM 11
3.2. Who Is Covered 12
3.3. Security-Responsible Line-Management Chain 12
3.3.1. Definition of the Chain 12
3.3.2. Deployed Personnel 13
3.3.3. Subcontractors 13
3.3.4. Student Mentoring Expectations 14
3.3.5. Official Visitors, Affiliates, and Others 14
3.3.6. Work Off-Site 14
3.4. Responsibilities of Members of the Security-Responsible Chain 15
3.4.1. The Workforce 15
3.4.2. Supervisors and Managers 15
3.5. Specific Members with Additional Responsibilities 16

3.6. Organization-Related Roles, Authorities, and Responsibilities 16
3.6.1. Science and Technology Organizations 17
3.6.2. Program Organizations 17
3.6.3. Facility-Owning Organizations 18
3.6.4. Institutional Service Organizations 20

3.7. Specific Organizations with Additional Responsibilities 20
3.7.1. Director's Office 20
3.7.2. Operations Working Group (OWG) 20
3.7.3. Security and Safeguards (S) Division 21
3.7.4. Internal Security (ISEC) Office 22
3.7.5. Computing, Communications and Networking (CCN) Division 23
3.7.6. Nonproliferation and International Security (NIS) Division 23
3.7.7. Environment, Safety, and Health (ESH) Division 24
3.7.8. Facilities & Waste Operations (FWO) Division 24
3.7.9. Project Management (PM) Division 24
3.7.10. Audits and Assessments (AA) Office 24
3.7.11. Business Operations (BUS) Division 25
3.7.12. Institutional Security Committees 25

4.0. TRAINING 25

4.1 Senior Technical Managers 26

4.2. All Managers and Supervisors 27

4.3. Facility Managers 27

4.4. Workers 27

5.0. REQUIREMENTS PROCESSES THAT SUPPORT THE FIVE-STEP PROCESS 27

5.1. Institutional-Level Processes 29
5.1.1. Contractual and Other DOE Security Requirements 29
5.1.2. Internal Institutional Requirements 29
5.1.3. Technical and Management Requirements 30
5.1.4. Application of the Quality Criteria 31
5.1.5. Offices of Institutional Coordination 31
5.1.6. Points of Contact 31
5.1.7. Work for Others (WFO) 31
5.1.8. Changes and Deviations 32
5.1.9. Applicability and Implementation of Requirements 32

5.2. Facility-Level Processes 33
5.2.1. Facility-Owning Organizations 33
5.2.2. Facility Security Plans 33
5.2.3. Facility Security Plan Levels of Rigor 34
5.2.4. Changing Facility Security Plans 34
5.2.5. Facility-Tenant Security Agreements 35

5.3. Activity-Level Processes: Work Control **35**
5.3.1. Types of Security Interests 36
5.3.2. Types of Security Areas 37
5.3.3. Research and General Office Work 37
5.3.4. Facility Work 38

5.4. Special Approvals or Authorizations **38**

6.0 ASSESSMENT PROCESSES THAT SUPPORT THE FIVE-STEP PROCESS **39**

6.1. Confirming Readiness **39**

6.2. Assessing Results **39**
6.2.1. Line Management Assessments 40
6.2.2. Functional and Independent Internal Assessments 41
6.2.3. UC-DOE Contract Appendix F 42
6.2.4. External Assessments 42

6.3. Issues Management and Corrective Actions **43**
6.3.1. Incident/Near-Miss Assessment 43
6.3.2. Workforce Questions, Concerns & Suggestions 43

7.0. SECURITY-RESPONSIBLE BEHAVIOR **44**

7.1. Introduction **44**

7.2. Accountability and Consequences **44**

8.0. SECURITY RESOURCE ALLOCATION **45**

8.1. General **45**

8.2. Deployed Personnel **46**

8.3. Security Management Plan **46**

BIBLIOGRAPHY **47**

Figures

Fig. 1: Three major expectations of the ISSM five-step process 6
Fig. 2: Applying the ISSM five-step process 8
Fig. 3: Applying the ISSM five-step process at three different levels 9
Fig. 4: Integrating the ISSM five-step process across the three levels 10
Fig. 5: Security-responsible line-management chain 13
Fig. 6: LANL organization 17
Fig. 7: Security interface between facility-owning and tenant management: permitting vs. directing work 19
Fig. 8: ISSM flow down of contractual and other security requirements to the work 28
Fig. 9: Assessments 41

Acronyms

AA—Audits and Assessments Office
AL—Albuquerque Operations Office (under NNSA)
AM—LANL Administrative Policies Manual
BUS—Business Operations Division
CCN— Computing, Communications and Networking Division
CNSI—Confidential National Security Information
DOE—Department of Energy, including the semi-autonomous National Nuclear Security Administration (NNSA)
EDS—Employee Development System
EM&R—Emergency Management and Response Group in S Division
EOC—Emergency Operations Center
ESH—Environment, Safety, and Health Division
ESH-OIO—ESH-Division's Operational Integration Office
ES&H—environment, safety, and health
FM—facility manager
FMU—facility management unit
FMWC—facility management work control
FRD—Formerly Restricted Data
FV&A—foreign visits and assignments
FWO—Facilities & Waste Operations Division
IFMPO—Institutional Facilities Management Program Office
ISEC—Internal Security Office
ISM—integrated safety management
ISSM—integrated safeguards & security management
JCNNM—Johnson Controls Northern New Mexico, Inc.
LAAO—Los Alamos Area Office (under NNSA)
LANL—Los Alamos National Laboratory
LIG—Laboratory implementation guidance
LIR—Laboratory implementation requirement
LPR—Laboratory performance requirement
NIS—Nonproliferation and International Security Division
NM—nuclear materials
NNSA —National Nuclear Security Administration (under DOE)
NSI—National Security Information
OIC—office of institutional coordination
OJT—on-the-job training
OPSEC—operations security program under ISEC
OSSO—organizational safeguards and security officer
OUO—Official Use Only
OWG—Operations Working Group
POC—point of contact
P&T—packaging and transportation

Acronyms (cont'd.)

PTLA—Protection Technology Los Alamos
RD—Restricted Data
SAP—special access program
SCIF—sensitive compartmented-information facility
SFM—safety function manager
SFSP—special facility security plan
SME—subject matter expert
SNM—special nuclear material
SNSI—Secret National Security Information
SRD—Secret Restricted Data
SSSP—Site Safeguards and Security Plan
UC—University of California
UCNI—Unclassified Controlled Nuclear Information
USSQD—unreviewed safeguards and security question determination process
WBS—work-breakdown structure
WFO—work for others

Safety and Security Policy

"We will never compromise safety or security for programmatic or operational needs."

We are committed to achieving excellence in environmental, safety, health, and security performance.

To meet the **moral imperative** not to injure people, the environment, or compromise the safety of our nation while accomplishing our mission, and the **business imperative** to meet the environmental, safety, health, and security requirements of the contract between the University of California and the Department of Energy, the employees, contractors, and guests of the Los Alamos National Laboratory will always strive to have:

- **ZERO injuries and illnesses on the job**
- **ZERO safeguards and security incidents**
- **ZERO injuries and illnesses off the job**
- **ZERO environmental incidents**
- **ZERO ethics incidents**
- **ZERO people-mistreatment incidents**

Los Alamos
NATIONAL LABORATORY

Preface

In early 2000, LANL Director John Browne launched the development, Labwide rollout, and initial implementation of integrated safeguards and security management (ISSM), modeled after integrated safety management (ISM). This was initiated because ISM's basic tenets — management commitment, worker involvement, line "ownership," clearly defined roles and responsibilities, work and worker authorization, self-assessment, continuous feedback and improvement, etc. — are vital to the success of safety as well as safeguards and security (or "security" more generally). Pursuing ISSM offers not only a stronger Labwide security culture and enhanced security performance, but supports LANL's goal of integrated management (IM) — a single integrated management system for achieving LANL's vital national security mission in a safe, secure, reliable, and cost-effective manner.

LANL is fully committed to establishing and maintaining an effective and efficient ISSM system. This is essential to ensure that security is systematically integrated into all management and work practices at all levels so that LANL's mission is accomplished securely by protecting security interests and always striving for "zero safeguards and security incidents" (see LANL Safety and Security Policy). Security interests include all LANL-controlled classified and sensitive-unclassified matter, nuclear materials, and other government resources associated with accomplishing LANL's mission. ISSM spans all areas of security (physical security, information/cyber security, personnel security, nuclear materials control and accountability, etc.) and related cross-cutting areas (export control, foreign travel, etc.).

As with ISM for safety, ISSM is official LANL policy that is to be followed by the entire workforce. ISSM is the single security management system that establishes security expectations for all people performing work at LANL, irrespective of employer. Among these expectations, ISSM requires that all work and all workers must meet the security requirements defined by the LANL requirements system, as documented in the ISSM Laboratory Performance Requirement (LPR), Laboratory implementation requirements (LIRs), and any supplemental requirements defined for a specific facility and/or activity. This is achieved through strong "top-down" management commitment and active "bottom-up" workforce participation to achieve the buy-in and ownership necessary for success.

This latest draft ISSM system description was developed by the Joint LANL-NNSA ISSM Steering Team, which is led by LANL with cross-directorate and NNSA/LAAO membership. It has benefited from extensive Labwide input since the first draft was issued in July 2000 at the start of LANL's ISSM rollout. It incorporates the ISSM expectations in Appendix O of the University of California (UC)-Department of Energy (DOE) contract approved January 18, 2001, consistent with recent guidance from the UC and the National Nuclear Security Administration (NNSA), DOE ISSM Policy 470.1 issued May 8, 2001, and LANL's ISM system description (see Bibliography). This document will continue to be updated as ISSM matures to reflect lessons learned and process improvements. Always, gains in effectiveness and efficiency must be basic to our thinking as we strive to improve the security of day-to-day operations. Comments on this document can be sent to security@lanl.gov.

1.0 Introduction to ISSM

Just as ISM is a system for performing work safely, ISSM is a system for performing work securely. And like ISM, ISSM is not something tangible – it is not a plan or a checklist. Instead, it is a way of doing business, and the focus of the business is work. Here, integration means that security is an integral part of all work planning, performance, assessment, and improvement. It is achieved using ISSM's (adapted from ISM's) eight guiding principles and five-step process (a.k.a. five core functions) because security requirements alone can't make the work or workplace secure. Security (like productivity) can only be accomplished by workers.

ISSM provides a framework to support each worker in fulfilling his/her security responsibilities so that, together, we can meet (1) the moral imperative not to compromise the security of our nation, and (2) the business imperative to effectively/efficiently satisfy the security requirements in our UC-DOE contract. Meeting these imperatives requires a total worker-based security culture, which is achieved through sustained execution of ISSM. The attributes of this desired security culture are described succinctly by E. Scott Geller, adapted here for security (vs. safety):

- *Everyone feels responsible for security and does something about it on a daily basis.*
- *Everyone goes beyond the call of duty to identify unsecure conditions and at risk behaviors, and they intervene to correct them.*
- *Secure work practices are supported with rewarding feedback from both peers and managers.*
- *Everyone "actively cares" continuously for the security of themselves and others and for the protection of security interests.*
- *Security is not considered a priority that can be conveniently shifted depending on the demands of the situation; rather security is considered a value linked with every priority of a given situation.*

(Adapted from *Working Safe: How to Help People Actively Care for Health and Safety*, E. Scott Geller, Chilton Book Company, 1996.)

1.1. Terms of Reference

The following terms are used throughout this document and are defined here for purposes of this document:

- **"Security,"** when used generically, encompasses all aspects of protecting all LANL-controlled safeguards (i.e., nuclear materials-related) and security interests commensurate with defined security threats and associated risk, and consistent with applicable security requirements.
- **"Security interests"** include LANL-controlled classified and sensitive- unclassified matter, nuclear materials (in particular, special nuclear materials and tritium), and other government resources associated with accomplishing the LANL mission.

- **"Safety,"** when used generically, encompasses all aspects of environment, safety, and health (ES&H), including regulatory requirements, pollution prevention, and waste minimization.
- **"Work"** is defined broadly to include all LANL activities undertaken by the workforce, including work-for-others (WFO) activities. Activities undertaken during emergencies should be done as safely and securely as possible, consistent with the nature of the emergency. Emergency actions may be taken outside of the documented requirements of ISM and ISSM.
- **"Worker"** is any person who performs work at LANL (whether on LANL's DOE-owned, leased, or rental property), including UC employees, subcontractors, vendors, external organization employees, affiliates, and official visitors. See Section 3.0.
- **"Risk"** refers to the likelihood and potential severity of theft, loss, and/or unauthorized disclosure of security interests by security threats (internal and/or external personnel) committing intentional or unintentional acts; for the purpose of this document, a qualitative judgment based on knowledge and experience, except where quantitative risk analysis is required.
- **"Controls"** are physical (e.g., security fences) and/or administrative (e.g., access authorization) measures to prevent or mitigate a threat from causing harm to security interests and national security. Security controls and safety controls should be carefully selected to promote synergy (mutual benefit) and to avoid conflict.
- **"Tailoring"** means the physical and/or administrative controls and other measures to prevent or mitigate security risk are tailored (vs. one size fits all) to the work being performed, including its environment (location and configuration). Emphasis is on designing the work and/or controls to reduce or eliminate the security interests and associated risk to prevent compromises of security interests and national security. With tailoring, the degree of rigor and formality in documentation, the nature of security controls, and the extent of performance assurance are commensurate with the security interests and risk associated with specific work.
- **"Need to know"** requires a determination by the person(s) having responsibility for specific classified matter, including information, material, and/or equipment, that a prospective recipient's access to such classified matter is necessary in the performance of his/her official or contractual duties of employment.

1.2. Worker-Manager Teamwork

ISSM success requires teamwork between and mutual understanding among all workers and managers. In turn, teamwork and mutual understanding depend greatly on effective and ongoing communications and interactions throughout the organization. Workers must have the means to improve the security processes and requirements by communicating problems and solutions to their managers, and managers must be able to communicate decisions and directions to the workforce. Managers must also be supportive and accessible to the workforce and responsive to their concerns – always seeking, promoting, and rewarding active worker participation and performance.

A variety of processes support active worker participation in identifying and resolving security concerns and contributing to the continued improvement of ISSM. These include organizational and institutional security committees; meetings with managers and security specialists; participating with managers during

management walk-around activities; performance appraisal activities; and day-to-day interactions on the workfloor. In addition, the S-Division "Security Help Desk" offers one-stop customer service, including coordinating and responding to worker security questions, concerns, and suggestions and providing other security support and services.

Worker participation also includes a "stop work" authority that can be activated whenever a worker perceives a situation believed to jeopardize security interests. Managers support the use of this authority without hint of reluctance or retribution. LANL has a Laboratory implementing requirement (LIR) in its formal requirements system that identifies the conditions and procedures for stopping and restarting work when security concerns arise.

Positive support, recognition, and reward of workers by their managers for the contributions they make to security are key to having active worker participation. To this end, LANL's performance appraisal process requires individual performance objectives (IPOs) on security for all workers, including managers. Managers are expected to model desired security behaviors and to mentor their workers. Meeting security IPOs is an important part of the performance appraisal and accountability processes, which are aimed at promoting and reinforcing strong "top-down" management commitment and active "bottom-up" workforce participation – both essential to achieve the buy-in and ownership necessary for continually improving the security of day-to-day operations.

1.3. Communications

LANL employs a variety of formal and informal communications processes to support ISSM (see LANL ISSM Communications Plan). To be effective, vertical communications among different levels in the security-responsible line-management chain must be two-way. This means information must be passed up and down the hierarchy without distorting the intent or content. Lateral communication between members of a single organization and between different organizations promotes the sharing of experience, security concerns, and solutions to problems, consistent with the need to know. Lateral communications must also be two-way. LANL is committed to continually improving all of its communications processes for promoting worker awareness and soliciting worker input/feedback to support the accomplishment of our vital national security mission in a safe, secure, reliable, and cost-effective manner. Collectively, these processes must serve to:

- Foster positive security values, attitudes, and behaviors in the workplace through demonstrated management commitment and active workforce participation.
- Continuously promote security awareness among all workers.
- Continuously solicit and respond to worker input and feedback to help ensure programmatic and operational considerations are taken into full account.
- Enhance worker understanding of their security responsibilities and of the resources available to assist them.
- Establish a clear, consistent voice among LANL's security professionals who provide guidance and other assistance.
- Target security communications to specific audiences to ensure relevancy and to avoid information overload.

- Enhance security training for new employees and incumbents, including general, job-specific, and periodic refresher training.
- Identify and communicate incident root causes and lessons learned to enhance awareness and help prevent recurrence.
- Engage the workforce in continually evaluating and improving the effectiveness of communications processes through focus groups, interviews, checkpoint surveys, etc.

To this end, the LANL Public Affairs Office serves as a major resource for improving ISSM communications and providing a variety of forums to facilitate communications. They provide technical guidance and assistance in communicating effectively with internal customers; developing effective communications processes and tools; and providing a central voice to reach all segments of the Laboratory. They also coordinate assistance from external communications experts as the need arises.

2.0. ISSM Description

This section describes the ISSM objective, eight guiding principles, five-step process, and tailoring of security expectations to the work and associated security interests.

2.1. Objective

The objective of ISSM at LANL is to systematically integrate security into all management and work practices at all levels so that LANL's mission is accomplished securely by protecting security interests and always striving for "zero safeguards and security incidents" (see LANL Safety and Security Policy). (Note: "zero safeguards and security incidents" means preventing actual and potential compromises to security interests and national security and meeting all applicable security requirements.) This is achieved through effective and efficient integration of security into all facets of work planning, performance, assessment, and improvement. Security is the responsibility of every member of the workforce.

2.2. Eight Guiding Principles

The ISSM guiding principles shown below guide all LANL actions aimed at effectively and efficiently performing work securely and achieving a secure workplace. These guiding principles are consistent with those in Appendix O of the UC-DOE contract, guidance from the UC and NNSA, DOE ISSM Policy 470.1, and those in LANL's ISM system description. Note that the first guiding principle has been expanded to reinforce the importance of line-management commitment in addition to worker responsibility and participation as the foundation for all other guiding principles. LANL workers implement these guiding principles by performing their work in a secure manner in accordance with ISSM. They use a degree of care commensurate with the security interests and risks associated with their work and are personally responsible and accountable for performing their work securely.

1. Management Commitment <u>and</u> Worker Responsibility and Participation. ISSM shall be a worker-based security management system. Each worker (manager and nonmanager) shall be directly responsible for performing work securely, including meeting security requirements and contributing to a secure mission and workplace. Managers shall be visibly committed to the effective and efficient implementation and sustained execution of all ISSM system elements, and workers shall directly

participate in developing, implementing, and continuously improving these elements, including understanding and using them in their work.

2. Line-Management Security Responsibility. Line management shall be directly responsible for protecting all security interests. This includes ensuring security risks are analyzed and that required security controls are in place and verified before accepting residual risk and authorizing work. Every member of the workforce belongs to a line-management organization, which extends in an unbroken chain from external sponsors through the LANL Director to workers "on the floor" (see Section 3.3.). Throughout this line-management chain, security shall be integral to all decisions relating to work performance, including resource allocation, planning, scheduling, and coordination.

3. Clear Roles and Responsibilities. LANL shall establish and maintain clear and unambiguous lines of authority, responsibility, and accountability at all organizational levels. These shall be effectively communicated so that everyone understands their individual and organizational roles.

4. Competence Commensurate with Responsibilities. Every member of the workforce shall possess the experience, knowledge, skills, and abilities necessary to fulfill his/her responsibilities, which is consistent with need-to-know requirements. Supervisors shall ensure that workers are competent to perform their work securely, including meeting security requirements, before authorizing them to perform work.

5. Balanced Priorities. Management shall effectively allocate resources to address security, safety, programmatic, and operational considerations, knowing that achieving programmatic goals is a significant component of achieving national security. Protecting security interests shall be a priority whenever work is planned and performed. Although different considerations often compete, work shall not be performed unless it can be performed securely, including meeting security requirements.

6. Identified Security Standards and Requirements. Before work is performed, the associated security risks shall be analyzed and an agreed-upon set of security standards and requirements shall be established, which, when properly implemented, shall provide sufficient assurance that the security interests are properly protected.

7. Work-Tailored Security Controls. Administrative and physical controls to prevent and mitigate security risks shall be tailored to the work being performed, including the work location and configuration. Emphasis shall be on designing the work and/or controls to reduce or eliminate the security interests and risks. Security controls and safety controls shall be carefully selected to promote mutual benefit and prevent mutual conflict.

8. Authorized Operation. The conditions and requirements to be satisfied for operations to be initiated and conducted shall be clearly established and agreed upon. Certain operations shall be authorized under the UC-DOE prime management and operations contract, while other operations shall be authorized under activity- and/or facility-level security plans jointly approved by LANL and NNSA. In all cases, managers shall authorize the work and the workers before work is performed.

2.3. Five-Step Process

The ISSM eight guiding principles are essential, but give little detail about how to achieve a secure workplace. Therefore, ISSM uses a five-step process (see Fig. 1) to ensure that security expectations

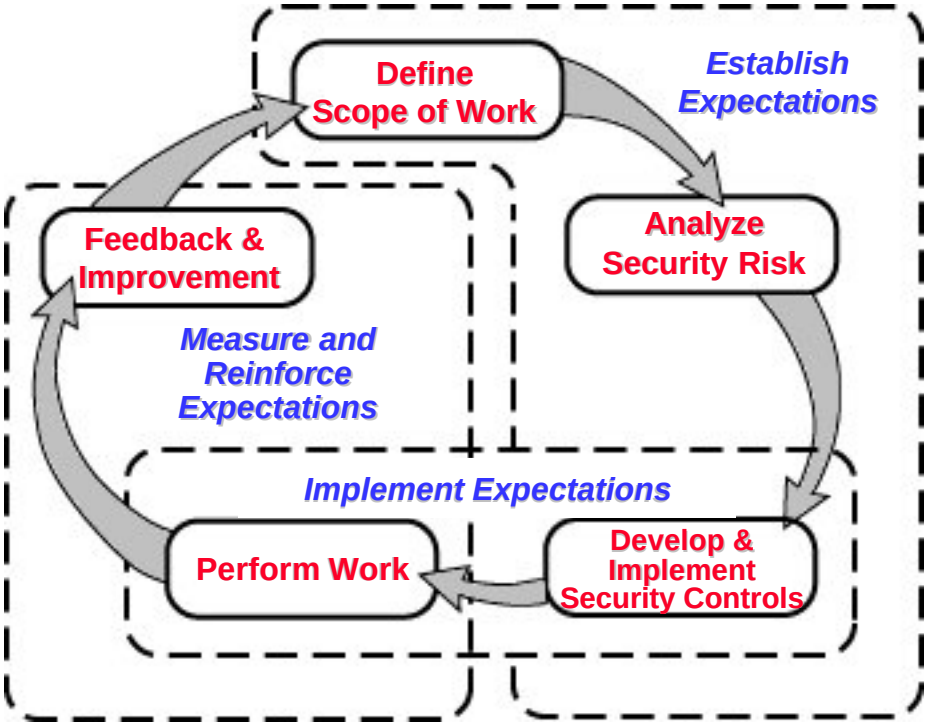


Fig. 1. Three major expectations (italics) of the ISSM five-step process.

are established, implemented, and measured and reinforced in every work activity. As outlined below, the ISSM five-step process defines a systematic approach to actions taken before, during, and after work is performed.

(1) Define the Scope of Work
Translate mission into work, set expectations (e.g., goals and objectives), identify related security interests, identify potential requirements, identify and prioritize tasks, and allocate resources.

(2) Analyze the Security Risk
Identify the security threats and analyze the security risks associated with the defined scope of work.

(3) Develop and Implement Security Controls
Identify security requirements and develop/implement work-tailored security controls to prevent or mitigate security risks. Line management shall accept residual risk before authorizing work.

(4) Perform Work within Security Controls
Confirm that required security controls are in place and then perform work securely within controls.

(5) Provide Feedback and Continuous Improvement (i.e., Ensure Performance)
Collect feedback information on the sufficiency of security controls; identify/implement opportunities for improving work definition, planning, and execution; conduct line and independent assessments; reinforce expected behaviors; and share best practices and lessons learned. This includes continually evaluating LANL's overall ISSM system and, as needed, refining it to ensure its effectiveness and efficiency for performing work securely.

Much of what follows is a description of the ISSM system for implementing the eight guiding principles and five-step process.

2.3.1. Meeting Security Expectations

The five-step process applies to all work at LANL, from keyboarding to designing and assembling nuclear criticality-safety experiments. The effort required for applying the five-step process is determined by the nature of the work and the associated security interests and risk.

For work with minimal security risk, the application of the five-step process may be a simple mental exercise at the start of each workday. For example, addressing the risk associated with keyboarding nonsensitive-unclassified information on an unclassified standalone computer may be as simple as ensuring the proper use of passwords for information protection and a clear understanding of the electronic warning banner.

By contrast, for the design and assembly of nuclear criticality-safety experiments involving large quantities of attractive special nuclear materials such as plutonium or highly enriched uranium, the process may require expert computer-based risk analyses, formal documentation, and third-party review over an extended period.

It is important to note in Fig. 1 that, while the five steps are discrete, their actions overlap. For example, when developing and implementing controls, you may be establishing expectations and implementing physical and/or administrative controls to meet expectations. When you perform work, you may activate the physical controls and see that they are operating properly during the work process.

2.3.2. Application of the Five-Step Process

Figure 2 gives more detail on applying the five-step process. The boxes contain actions typically taken to support each step. The arrows indicate that work begins with some outside direction to take action and that the process is focused on developing a tangible work output. The steps are arranged in a ring to illustrate that this is a process of continuous improvement. It is anticipated that in more complex applications the interrelationships among the different steps may iterate or flow in a different sequence from the directions shown in the figure. The five-step process is the foundation of ISSM and the secure performance of work.

2.3.3. Tailoring Versus Uniformity in Application

LANL is challenged to strike a balance between individual organizations tailoring expectations to their specific facilities and/or activities versus LANL establishing uniform (one-size-fits-all) institutional expectations for all facilities and activities. Tailoring expectations within individual organizations allows flexibility and worker discretion to help ensure: (1) practicable and effective expectations; (2) decision-making at the lowest appropriate level; (3) active worker participation and buy-in; and (4) balanced priorities through integrated risk management. With tailoring, the degree of rigor and formality in documentation, the nature of security controls, and the extent of performance assurance are commensurate with the security interests and risk associated with specific work.

By contrast, uniform institutional expectations offer uniformity in meeting contractual requirements, Labwide application of best business practices, reduced institutional liability and risk, and economy of scale. These benefits are not easily obtained when individual organizations establish tailored expectations that differ between facilities and activities.

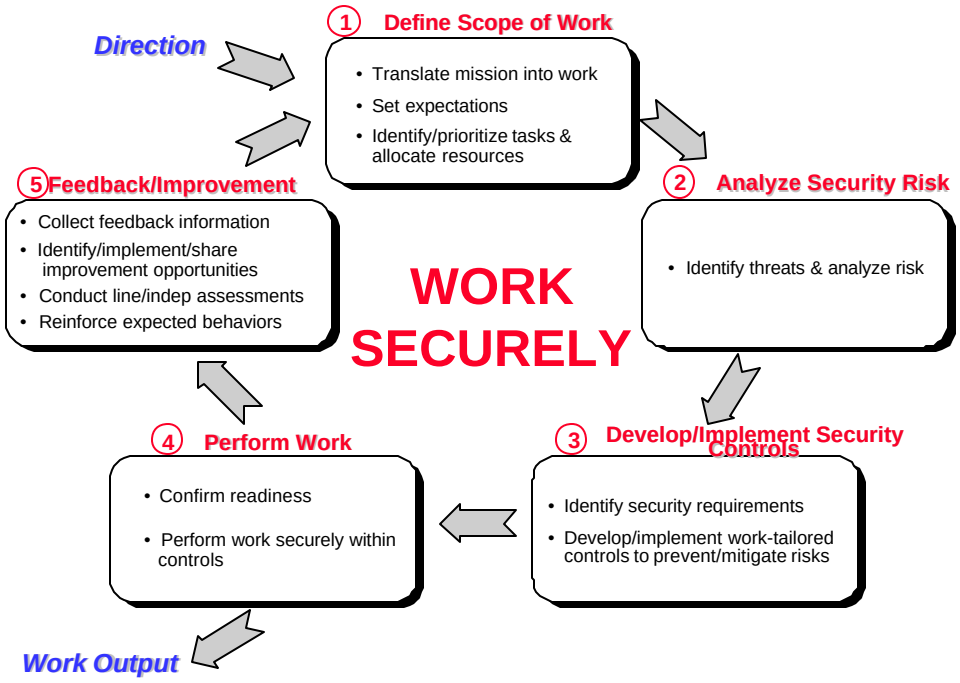


Fig. 2. Applying the ISSM five-step process.

To achieve the benefits of tailoring and uniformity, ISSM uses the five-step process to guide individual organizations in creating tailored expectations for specific facilities and activities, while retaining a required level of institutional uniformity – i.e., work-specific tailoring at the activity level and facility-specific tailoring at the facility level, consistent with an overarching set of uniform expectations at the institutional level.

2.3.4. Use of the Five-Step Process in Organizations

An organization's application of the five-step process to individual acts of work may be simple and straightforward; application to individual facilities and to the entire institution is more complex. Always starting by defining the scope of work, the five-step process is applied at the following three levels: activity, facility, and institutional:

- **Activity level -** discrete work activities performed in the workplace by individual organizations such as preparing a classified document on a stand-alone classified computer or fabricating a classified weapons component. (Note: The five-step process provides a systematic approach for organizations to determine the activity-level controls necessary to perform work securely. For example, maintaining office files containing nonsensitive information requires fewer controls than

maintaining files containing top-secret information. Within each organization, the security-responsible line-management chain, see Section 3.3., is responsible for ensuring that all security interests associated with their activities are properly protected. To this end, an organization may choose to establish a uniform set of organization-wide rather than activity-specific security expectations to ensure all their activities are performed in a secure and consistent manner. See Section 5.3.);

- **Facility level -** collective activities within a specific facility. (Note: The five-step process provides a systematic approach for organizations to determine the facility-level controls necessary to perform work securely. See Sections 3.6.3. and 5.2.); and

- **Institutional level -** collective activities of LANL. (Note: The five-step process provides a systematic approach for LANL to determine the institutional-level expectations necessary, in combination with tailored activity- and facility-specific expectations, to perform work securely. See Section 5.1.).

Figure 3 illustrates all three levels (left side) and how the five-step process is applied to each.

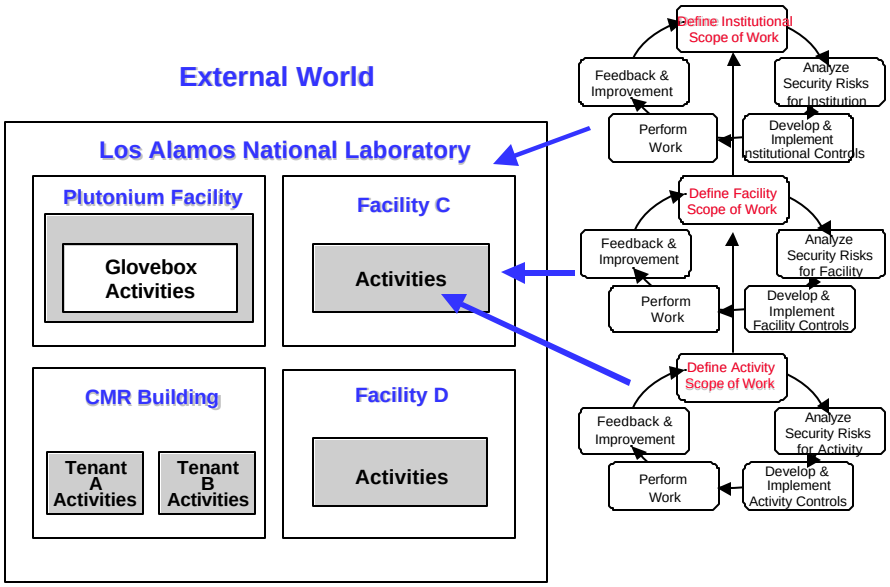


Fig. 3. Applying the ISSM five-step process at three different levels.

Note that "organization" is not shown as a separate level because "activity, facility, and institutional levels" are all inclusive in terms of reflecting increased scope of work vs. who performs the work (i.e., LANL organizations). Instead, individual organizations use the five-step process in creating tailored expectations at the "activity and facility levels." They also participate in the LANL's establishment of "institutional-level" expectations to achieve the necessary level of institutional uniformity (see Section 5.0.). Similarly, "DOE/external" is not shown as a separate level because, as described in Section 5.1., it is incorporated into the "institutional level" as the major driver in establishing institutional expectations. DOE and other external regulatory agencies are ultimately responsible for ensuring that appropriate requirements are established and implemented for the secure performance of work by their contractors.

As illustrated in Fig. 3, institutional expectations for security performance govern all facilities and activities encompassed by the LANL boundary. Each facility (i.e., facility-owning organization – see Section 3.6.3.) adds, as necessary, its own set of tailored expectations to the uniform expectations established by the institution. Moreover, the organization performing the work may add activity-specific expectations as well as expectations common to all their activities (see above and Section 5.3.). The nested boxes on the left side of Fig. 3 depict this nested relationship of institutional, facility-specific, and activity-specific expectations for performing work securely. The right side of Fig. 3 depicts the three-level application of the five-step process for determining these expectations. These determinations are based on the defined scope of work and associated security interests and risks at each level.

Figure 4 results from integrating what is shown on the right side of Fig. 3. It depicts LANL's overall ISSM system, including the major system elements and their interrelationships. It also further illustrates

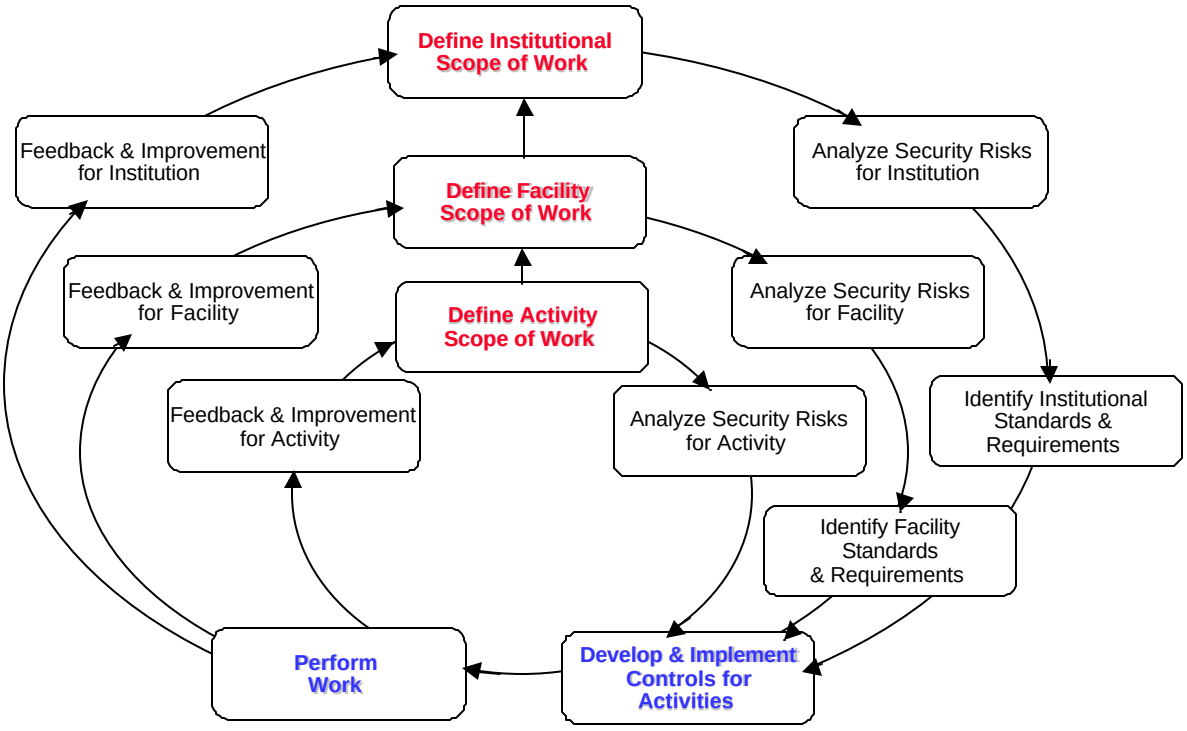


Fig. 4. Integrating the ISSM five-step process across the three levels.

that secure work at LANL is accomplished by applying the five-step process at each of the three levels. Note that all three levels (nested rings) converge on "Develop & Implement Controls for Activities" and diverge after "Perform Work." Defining the scope of a work activity is the starting point for identifying the security interests, analyzing the security risk, and determining the security expectations (i.e., requirements and controls). This figure also depicts the applicability of facility and institutional expectations to individual work activities.

An activity must meet not only the activity-specific expectations derived from its defined scope of work and associated security interests and risk, but also the applicable expectations established for the institution and for the facility where the activity is conducted. This is depicted in Fig. 4 by the third action shown in each of the three rings before "Perform Work," which collectively represent the third step shown in Fig. 2. Institutional and/or facility expectations that are not applicable to the security interests and risk associated with a specific activity need not be addressed by the controls for that activity. Also, institutional and/or facility-specific controls will only be prescribed at the activity level when there is a compelling need for Labwide and/or facility-wide uniformity.

Figure 4 also illustrates that ALL WORK is performed at the ACTIVITY LEVEL. ISSM is structured to control all work at the activity level in accordance with the five-step process. Fundamental to ISSM is that all work will be performed securely and meet the applicable institutional-, facility-, and activity-level requirements. Again, at the activity level, the organization performing the work may establish activity-specific expectations as well as expectations common to all their activities (see above and Section 5.3.). Also, all work is performed in a facility management unit (FMU), which consists of the grounds, structures, and services within geographical areas. Work on the physical structures, systems, and grounds of the facility is called facility work. Tenants of FMUs perform all other types of work, principally R&D and office work.

The remainder of this document describes in greater detail the ISSM system elements and their interrelationships, which collectively define and support the five-step process for performing work securely. Again, the ISSM system is aimed at the secure performance of work, with facility and institutional rings supporting and supplementing the activity ring where all work is performed. At any point during the planning and performance of work, one or more of the institutional, facility- and/or activity-specific requirements may come to bear on the work. Together, these expectations must be necessary, sufficient, and consistent if work is to be performed securely. To this end, the ISSM system is designed to assist workers and their supervisors in selecting and applying the appropriate processes and controls.

3.0. Roles and Responsibilities

3.1. Basis in ISSM

Line managers and other workers of an organization are ultimately responsible and accountable for performing their work securely. Clear and unambiguous roles and lines of responsibility, authority, and accountability at all organizational levels of LANL are necessary to meet the expectations of an integrated management system. In addition, supporting security roles are provided by:

- program organizations that are responsible and accountable for allocating sufficient resources for their program's activities and facilities (see Sections 3.6.2. and 8.0.);
- facility-owning organizations that are responsible and accountable for providing secure facilities (see Sections 3.6.3. and 5.2.); and
- service organizations (e.g., S Division) that are responsible and accountable for providing expertise, assistance, services, and institutional processes (see Sections 3.6.4. and 3.7.).

As established here, the security roles and responsibilities of any given individual at LANL are determined both by the individual's job position in a security-responsible line-management chain and the role of the organization to which he/she belongs. Therefore, the first part of this discussion addresses roles and responsibilities determined by the individual's position in the security-responsible line-management chain, while the second part covers organizational roles and related responsibilities.

3.2. Who Is Covered

The requirements for security responsibility described here apply to the entire workforce and to the protection of all security interests. The workforce comprises all personnel who perform work at LANL (whether on LANL's DOE-owned, leased, or rental property), including UC employees, subcontractors, vendors, external organization employees, affiliates, and official visitors. All LANL workers are accountable for security performance. See AM 702 in the LANL Administrative Policies Manual (AM) and the General Security LIR.

3.3. Security-Responsible Line-Management Chain

3.3.1. Definition of the Chain

Each worker at LANL is part of a security-responsible line-management chain and is charged with performing work securely by protecting security interests and always striving for "zero safeguards and security incidents." Unless this responsibility is formally transferred, all UC workers, subcontractors, official visitors, affiliates, and others are part of the security-responsible line-management chain of the organization to which they belong or by which they are hosted. Figure 5 shows the usual security-responsible line-management chain for UC workers. As shown, this line-management chain starts with any worker and flows upward through the LANL Director (note: some line-management chains do not include an Associate Laboratory Director).

When work is directed by another person, a security-responsible line-management chain exists. LANL has established management and supervisory positions that formalize the direction of work, and these are used to define the security-responsible line-management chain for UC workers. Similar line-management chains exist in LANL's subcontractor organizations, but the particular management titles may differ (subcontractor workers are addressed in Section 3.3.3).

- The UC security-responsible line-management chain starts with any worker and flows upward through the LANL Director. Below the group-leader level, the security-responsible line-management chain includes workers "on the floor" and may include non-management supervisors (such as team leaders, principal investigators, or TEC supervisors) who direct the day-to-day activities of workers under their supervision.
- Starting with the group-leader level and flowing upward through the LANL Director, the line-management chain is defined by the succession of direct reports that establish job assignments, appraise performance, and determine salaries.
- Except by a formal written agreement, a member of one organization cannot be part of another organization's security-responsible line-management chain. At any time, an individual can be a member of only one security-responsible line-management chain.

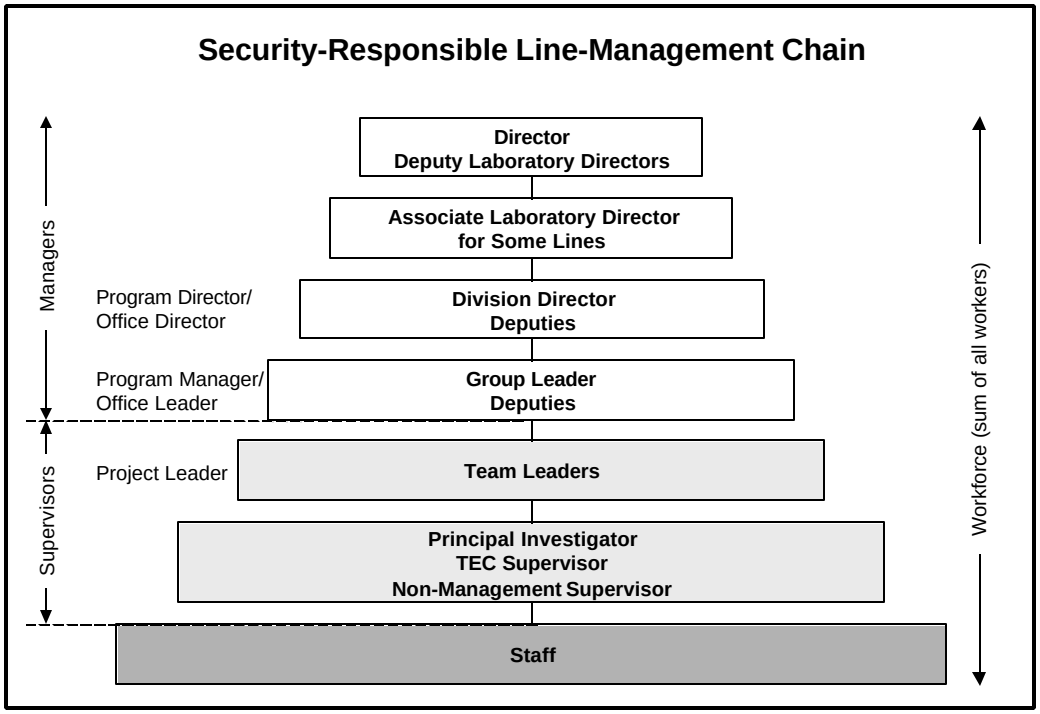


Fig. 5. Security-responsible line-management chain.

- Collectively, the security-responsible line-management chain, from the worker through the LANL Director, is responsible for the security of the work done by the organization, although workers at different levels have different responsibilities and authorities.

3.3.2. Deployed Personnel

The staff of a LANL organization is often augmented by the addition of workers from another organization. This might be the result of deploying workers to support a particular project, organization, or facility. In these instances, the deployed person may not have any contact with his or her organizational line manager for extended periods of time, and the line manager may not have a sufficient understanding or control of the security interests and risk in the deployed person's work environment. In such cases, the line-management security responsibility may be transferred to an accepting organization with the following conditions:

- the transfer of security responsibility must be documented and agreed to by the home and accepting organizations;
- the home organization retains salary and performance responsibility; and
- the accepting organization assumes a security responsibility equivalent to that of its regular employees.

3.3.3. Subcontractors

LANL subcontractors are either contract laborers hired through personal service contracts or independent task-oriented subcontractors. Contract labor, used to augment the staff, permits direct supervision by UC personnel and provides use of LANL facilities and equipment. Contract labor

subcontractors become part of the security-responsible line-management chain of the host LANL organization. In this relationship, the UC line-management chain is responsible for security, but performance, disciplinary, and other personnel actions remain the responsibility of the contract-labor subcontractor organization.

Independent task-oriented subcontractors have specific statements of work identifying discrete tasks and deliverables. These subcontractors work independently of LANL to deliver the specified product. There is no direct UC supervision, notwithstanding technical direction. Task-oriented subcontractors (including PTLA, JCNNM, service/maintenance, and construction subcontractors) are part of a security-responsible line-management chain within their companies. UC workers who request the services of a subcontractor have a supporting security responsibility to coordinate the LANL interface, to provide a secure work environment for subcontractor personnel, and to communicate security expectations to the subcontractor. Subcontractors must meet all LANL security expectations. When these conditions are met and appropriate contracts are established, security responsibility for an activity may be transferred to the subcontractor. Subcontractors are responsible for meeting all applicable security requirements while performing work on the site.

3.3.4. Student Mentoring Expectations

The student population presents unique opportunities and challenges. LANL's security expectations of students are the same as for all workers. However, students are often less experienced in their fields and may not have completed their formal education. In addition, their employment at LANL is often compressed into concentrated periods of time during the summer or during school breaks. Our student population represents our future workforce, and their student work experience at LANL provides an outstanding opportunity to begin the process of inculcating LANL's ISSM expectations.

To ensure proper security management of our student population, the security-responsible line-management chain for each student must be made clear to the student and their supervisor(s) and mentor(s). In addition, each division must ensure each student is assigned a mentor who is supported by a strong and effective mentoring program. This mentoring program must ensure the selection of high-quality mentors; adequate preparation before a student's arrival; proper training, supervision, and appropriate student participation in security during the student's work tenure; and an effective feedback process both during and upon completion of a student's employment.

3.3.5. Official Visitors, Affiliates, and Others

Official visitors, affiliates (including guest scientists and consultants), and others who officially observe and/or perform work at LANL have the same security responsibility as UC employees. However, in these cases, the LANL host organization is the security-responsible line-management chain.

3.3.6. Work Off-Site

UC workers that work off-site from LANL shall generally be integrated into the security-responsible line-management chain of the host organization. It is the responsibility of the worker's LANL line manager to ascertain that this has, in fact, happened. If the security practices of the host site are deemed inadequate by the worker or their line manager, or it is not possible for the worker to be integrated into the host security-responsible line-management chain, the security responsibility remains with the LANL security-responsible line-management chain.

LANL groups use the Nevada Test Site (NTS) to conduct experiments in support of their missions. LANL maintains a small contingent of workers resident at the NTS to provide technical support and facilitate the work of experimenters traveling from LANL. LANL-NTS ensures that the ISSM five-step process is applied to LANL work at NTS. Work performed by LANL workers at the NTS is done in accordance with all commitments specified in NNSA/Nevada Operations Office (NV) orders, policies and the NNSA/NV LANL Activity Agreements and is consistent with the LANL ISSM system.

3.4. Responsibilities of Members of the Security-Responsible Chain

Sections 3.4 and 3.5 address general and specific "member" roles, respectively, and 3.6 and 3.7 address general and specific "organizational" roles, respectively. Details are provided in the General Security LIR.

3.4.1. The Workforce

At LANL, working securely is every worker's responsibility and a condition for employment. Every individual on the LANL site is part of a security-responsible line-management chain charged with creating a secure workplace. As noted in Fig. 5, each person in the line-management chain is a worker who at times may also perform supervisory or management functions, depending upon their role. The responsibilities and authorities for each worker are determined by the function he or she is performing in their job assignment. Each worker has the responsibility and authority to:

- perform their work securely and contribute to the protection of security interests around them;
- ensure their work is authorized and performed in accordance with the ISSM five-step process;
- ensure security requirements applicable to their work are met;
- promote security awareness, including sharing and using lessons learned from any control failures, near misses, or security incidents to pursue system improvements;
- seize opportunities to provide input/feedback, especially for the development, implementation, and continuous improvement of security requirements and ISSM;
- seek help from their organizational security representatives and the Security Help Desk on security questions, concerns, and suggestions;
- participate in security self-assessments and development of corrective actions; and
- stop their work when they have a security concern, and, if they observe a concern in another person's work, inform that person or their supervisor immediately.

3.4.2. Supervisors and Managers

As shown in Fig. 5, supervisors are those persons who direct the work of others. Managers are supervisors when they are functioning to direct the work of others in their security-responsible line-management chain. Supervisors and managers have the authority and are expected to hold their workers accountable for security. In addition to their security roles as members of the workforce, supervisors at all levels have the responsibility and authority to:

- actively and visibly demonstrate their personal commitment to security and ISSM by providing sustained leadership, including promoting, modeling, and reinforcing positive security values, attitudes, and behaviors and meeting all applicable security requirements;

- promote security awareness, including actively sharing lessons learned and starting all meetings with "safety and security first";
- involve workers in all aspects of working securely and provide essential support for performing work securely, including training, systems, and tools;
- authorize work and workers before work is performed, consistent with secure work practices (see Section 5.3.), pursuing joint LANL-NNSA approval when required for specific activities and their associated security interests and risks [see Sections 5.3.-5.4. regarding special facility security plans (SFSPs) and the LANL Site Safeguards and Security Plan (SSSP)];
- review the work of supervised personnel for the use and effectiveness of security controls to identify opportunities for improvement;
- actively solicit and respond to worker input and feedback, especially for development, implementation, and continuous improvement of security requirements and ISSM;
- use management walk-arounds to promote ISSM communications and to engage workers in security self-assessments and development of corrective actions;
- work with S Division, ISEC, and CCN, as appropriate, to mitigate security risks identified by self-assessments;
- identify and communicate the resources necessary to perform work securely (see Section 8.0);
- support and promote use of designated organizational security representatives (e.g., OSSOs, OCSRs, ADCs, CDCs et al.);
- promote use of the Security Help Desk to assist with security questions, concerns, and suggestions;
- resolve disputes and conflicts relating to security; and
- help all workers achieve success with ISSM, including maintaining effective and efficient security communications processes within their organization;

The overall responsibility for ensuring that the appropriate security values, systems, processes, and resources are present increases with the level of management up the security-responsible line-management chain.

3.5. Specific Members with Additional Responsibilities

Certain members of a security-responsible line-management chain, independent of their position in the line-management chain or type of organization, and after advanced institutional training and qualification, may be designated as security representatives by their respective management. These individuals are responsible for providing security guidance and assistance to their respective security-responsible line-management chains. As needed, they are to request security support from institutional service organizations, principally S-Division and ISEC.

3.6. Organization-Related Roles, Authorities, and Responsibilities

In addition to security responsibilities determined by an individual's role in the security-responsible line-management chain, security responsibilities are also based upon the roles of the organization to which he/she belongs. The roles of organizations can be categorized as science and technology (S&T), program, facility, or service. While most LANL organizations predominantly serve a single role, in many

cases, organizations serve multiple roles. For example, the same organization can have both program and S&T roles or both support and S&T roles. All LANL organizations do work and have security-responsible line-management chains. Figure 6 shows a simplified schematic of LANL's organizational structure.

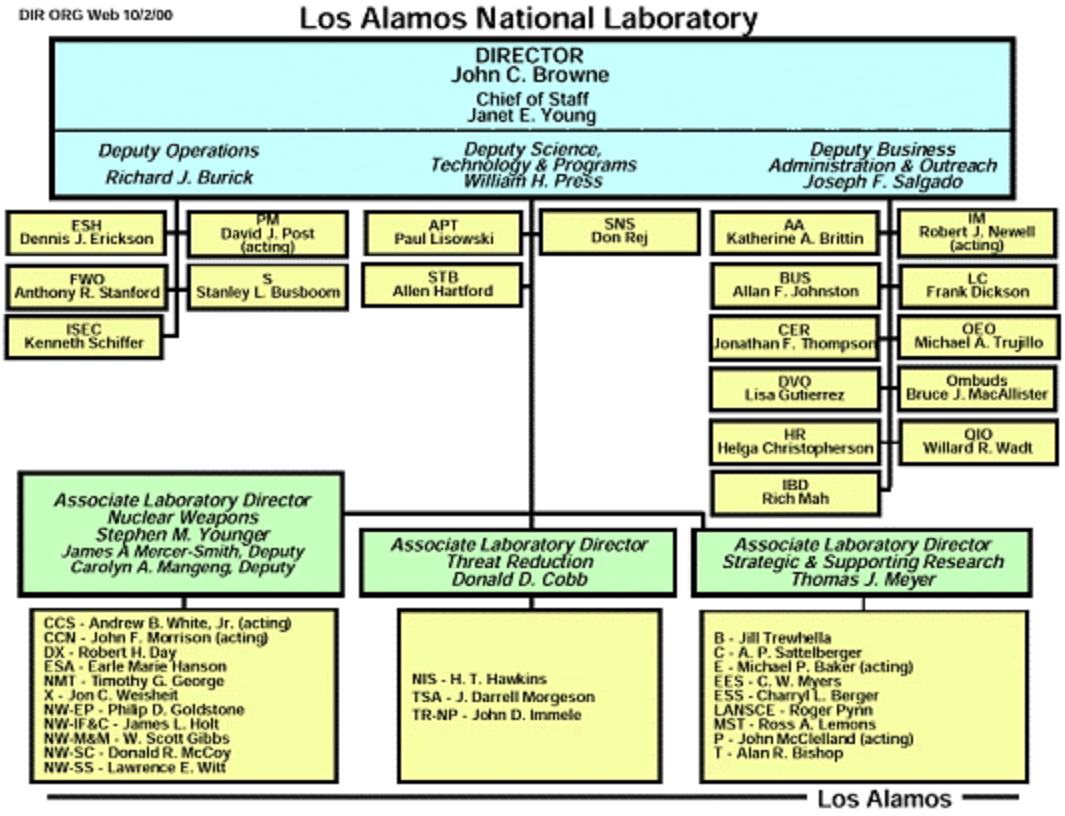


Fig. 6. LANL organization.

Sections 3.6 and 3.7 establish the security responsibilities for LANL organizations having major roles in LANL security. Responsibilities are determined by the assigned role(s) of an organization. Section 3.6 establishes general responsibilities based upon an organization's role(s), and Section 3.7 addresses roles and responsibilities of specific LANL organizations.

3.6.1. Science and Technology Organizations

Science and technology (S&T) organizations perform the programmatic, or mission-related, work of LANL. The responsibilities of individuals working in S&T organizations are those that apply to all types of LANL organizations and are discussed in Sections 3.3 through 3.5.

3.6.2. Program Organizations

Program organizations provide the primary coordination and liaison with outside sponsors for work done at LANL. Unless they are acting in the capacity of a line manager for their organization (e.g., when supervising office staff), program directors, program managers, and project leaders have limited

accountability for security performance. In addition to their security-responsible line-management chain roles, individuals working in program assignments have responsibility and authority for the following:

- establishing expectations and requirements to ensure that LANL standards for security are a visible part of program plans, funding, and project definitions;
- ensuring that security is an integral and discernible part of the work planning, performance, assessment, and improvement process;
- ensuring that resources, plans, schedules, and facilities are sufficient to perform the work in a manner that protects security interests and meets all applicable security requirements; and
- communicating and supporting security schedule and budget requirements to line managers and customers, as required.

3.6.3. Facility-Owning Organizations

LANL uses distributed facility management to provide and maintain facilities to support the safe and secure performance of work. Each LANL facility is "owned" by a division director and managed by a facility manager (FM), who acts as their agent in managing the facility infrastructure. For security, each facility-owning organization formally negotiates and documents with S Division their respective roles, responsibilities, and authorities for (1) establishing facility security operating limits that bound the work that can be done securely; and (2) providing essential facility infrastructure to support secure work in facilities, including facility-related structures, systems, and management processes (e.g., exterior lighting, security fences, vaults, vault-type rooms, local and Labwide computer networks, interior and exterior intrusion-alarm and electronic access-control systems, and facility-wide administrative procedures for monitoring foreign national visitors and assignees). In addition to their security-responsible line-management chain roles, and as negotiated with S Division, each facility-owning division director and/or their designated security representative, who may or may not be a member of an FM team or serving as an organizational safeguards and security officer (OSSO), have responsibility and authority for (also see Section 5.2.):

- establishing and maintaining a facility security plan to define the facility security operating limits and facility-level security requirements necessary to perform work securely;
- participating with S Division in the development of special facility security plans (SFSPs) for temporary operations that require NNSA approval due to the handling of certain quantities of SNM, and/or of LANL's Site Safeguards and Security Plan (SSSP), which requires NNSA approval due to recurring operations or storage of certain quantities of SNM; (Note: Most activities and associated facilities are authorized by the UC-DOE prime contract; however, depending on the associated security interests and risk, an activity- and/or facility-specific security plan may require joint LANL-NNSA approval as currently required for SFSPs and for LANL's SSSP. See Section 5.4.)
- communicating facility security operating limits and requirements to facility tenants and their cognizant line management through facility-tenant security agreements (see Section 5.2.5.); (Note: The facility-owning division directors and/or their designated security representatives must coordinate the development of facility-specific security expectations with affected tenant organizations.)

- periodically reviewing and permitting tenant work in the facility; (Note: For security, this means a facility-owning division director and/or their designated security representative can say yes—the work may be performed; or no—the work may not be performed; or can stop work that presents an immediate security threat to or breach of the facility security operating limits.)
- requiring and supporting the secure management of all facility work such as maintenance, repair, modification, or construction within the facility; and
- communicating security resource requirements to facility funding providers.

The relationship between the facility-owning and tenant organizations is shown in Fig. 7. This illustration shows that both line A and line B must meet the institutional and facility requirements. Activity requirements apply to work being performed by line B. The facility-tenant security agreement and the facility security plan define the interface between the line-A facility-owning organization and the line-B tenant organization. Note that the facility-owning and tenant organizations may or may not be the same. The facility-owning division director and/or their designated security representative permits work, and the activity line manager directs work.

It is the responsibility of tenants of a facility to work within the facility security operating limits. The tenants' line management shall also (1) inform and seek the approval of the facility-owning division director and/or their designated security representative for activities planned in the facility that are not already clearly permitted by the facility-tenant security agreement or the facility security plan; and (2) work with the facility-owning division director and/or their designated security representative to ensure that the integrity of the facility security operating limits is maintained.

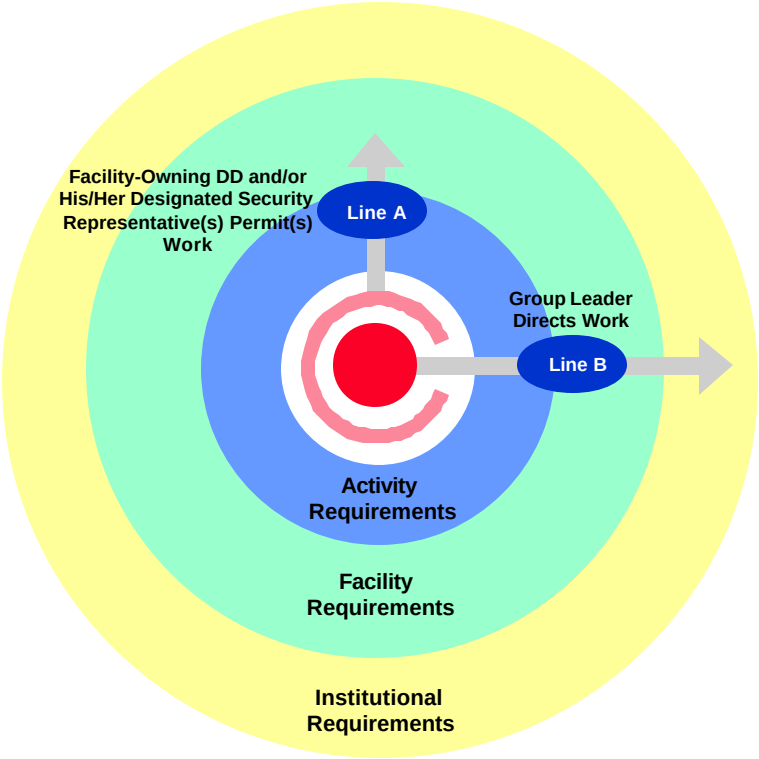


Fig. 7. Security interface between facility-owning and tenant management: permitting vs. directing work.

3.6.4. Institutional Service Organizations

Institutional service organizations provide support and services to help meet the needs of S&T, program, and facility-owning organizations. They also provide coordination across the institution and support institution-wide needs. In addition to their security-responsible line-management chain roles, individuals working in support and service assignments have responsibility and authority for:

- providing vision, leadership, direction, communication, and facilitation to promote continuous improvement and cost-effective security excellence;
- serving as the central point of contact, coordination, and support for interactions with regulators, stakeholders, and the public, involving other LANL organizations in these interactions, as appropriate;
- managing processes to ensure the existence of necessary and appropriate institutional expectations in the form of security standards and requirements;
- providing performance feedback and elevating issues to line management (but not enforcement which is a line management responsibility); and
- communicating resource requirements to funding providers.

3.7. Specific Organizations with Additional Responsibilities

3.7.1. Director's Office

The Director's Office has ultimate responsibility and authority for all four organizational functions: S&T, program, facility, and service. This office includes the LANL Director and the three Deputy Laboratory Directors for the following: Operations; Science, Technology, and Programs; and Business Administration and Outreach. The Deputy Laboratory Director for Science, Technology, and Programs serves as the LANL's principal deputy. The three Associate Laboratory Directors for Nuclear Weapons, Threat Reduction, and Strategic and Supporting Research report to the LANL Director. Being at the top of the line-management chain, these managers have ultimate responsibility and authority for protecting security interests, including establishing, communicating, and reinforcing LANL's security values and vision (see Fig. 6).

3.7.2. Operations Working Group (OWG)

The OWG is the primary management advisory and oversight organization for LANL operations, including security. This group is chaired by the Deputy Laboratory Director for Operations and includes selected division-level directors, the ISM and ISSM Program Managers, and representatives from NNSA/LAAO, JCNNM, PTLA, UC, and the IFMPO. The OWG is responsible for:

- monitoring the effectiveness of security at LANL by reviewing performance measures, assessments, incidents, and related activities;
- developing recommendations for addressing security problems and improvements to the Deputy Laboratory Director for Operations; and
- providing senior managers with relevant security information and engaging them in addressing Labwide issues.

3.7.3. Security and Safeguards (S) Division

S Division is primarily a service organization that provides a wide range of technical and administrative support in areas that include personnel security, information security, physical security, nuclear safeguards, emergency response, protective force services, fire department services, security training, incident assessment, and lessons learned. The division has responsibility and authority for:

- providing staff and subject matter expertise to lead, promote, and facilitate implementation and sustained execution of ISSM, including maintaining a full-time "Security Help Desk" that provides one-stop customer service (see below);
- promoting security excellence and providing security leadership throughout LANL;
- performing security functional assessments to complement and support line self-assessments performed by Labwide security-responsible line-management chains;
- assisting security-responsible line-management chains with self-assessment activities and corrective actions;
- coordinating and maintaining contractual and other DOE security requirements, and coordinating, maintaining, and providing implementing assistance of institutional requirements (LPRs and LIRs) that flow down from the contract;
- serving as the central point of institutional contact, coordination, and support for interfaces with security regulators, stakeholders, and the public, including the DOE and other federal, state, and local regulatory and law enforcement agencies;
- providing security performance feedback, elevating issues, and making recommendations to LANL organizations; and
- providing security support and services, including technology improvement, compliance/performance guidance, and developing measures and objectives aimed at ensuring effective protection of Labwide security interests.

The ISSM Program Office is located in the S-Division Office and is assisted by the Joint LANL-NNSA ISSM Steering Team chaired by the ISSM Program Manager. Working in close cooperation with the ISM Program Office, the ISSM Program Office has responsibility and authority for guiding, coordinating, and tracking the institutional implementation and sustained execution of ISSM.

The Emergency Management and Response Group (S-8/EM&R) in S Division has responsibility for institutional emergency planning and response for emergencies occurring on DOE/LANL property. EM&R has responsibility and authority for:

- training and maintaining personnel to respond to emergencies, including incident commanders, other response personnel, and LANL emergency directors;
- maintaining the Emergency Operations Center (EOC) and alternate EOC in an operational readiness condition;
- interfacing with surrounding jurisdictions and entities on emergency response, planning, and preparedness matters;

- responding to emergencies, including assessment, classification, notification, mitigation, and recovery;
- establishing and implementing a drill and exercise program; and
- coordinating, maintaining, and providing implementing assistance for LANL's Emergency Management Plan and other institutional requirements (LPRs and LIRs) relating to emergency response.

The protective force services for LANL are provided by Protection Technology Los Alamos (PTLA) under contract with the University of California and under the direction of S Division. PTLA has the responsibility to provide well-trained and qualified personnel to protect special nuclear materials (SNM), classified matter, and other government property from theft, diversion, sabotage, and other malevolent acts. To this end, the protective force is responsible for:

- ensuring that personnel are properly badged for entry or exit from certain secure areas;
- randomly checking safes, vaults, vault type rooms, and locked doors to ensure that classified matter and other government property have been secured properly;
- performing searches of personnel and vehicles, on a regular or random basis dependent on the facility requirements, to ensure that no prohibited articles are introduced into and that no SNM or property are improperly removed from facilities; and
- providing emergency response to known or possible security incidents.

The full-time "Security Help Desk" that provides one-stop customer service is operated by Group S-2, Program Integration. This service is responsible for:

- creating a one-stop shop capable of handling the majority of security-related questions, concerns, and suggestions posed by Labwide workers in the performance of their work;
- providing an "urgent" dispatch function to send the right "service" technician to the aid of the caller;
- initiating follow-up conversations, via phone or e-mail, to ensure the customer concerns are resolved in a satisfactory manner;
- directing customers to published sources of security guidance/information and following-up to ensure customers are satisfied; and
- continually collecting data concerning common concerns or areas of confusion, analyzing the data, and using the results in a lessons-learned program aimed at addressing Labwide problems with institutional solutions.

3.7.4. Internal Security (ISEC) Office

ISEC has three major security responsibilities: overseeing LANL's counterintelligence program, managing LANL's foreign visits and assignments (FV&A) program, and managing LANL's operations security (OPSEC) program. ISEC has responsibility and authority for:

- ensuring appropriate procedures are in place to meet the DOE requirements for conducting counterintelligence activities, including providing security awareness training to LANL personnel on specific counterintelligence threats and techniques;

- ensuring administrative requirements are developed and adhered to regarding the unclassified visits and assignments by foreign nationals; and
- maintaining a comprehensive OPSEC program to ensure unclassified information cannot be used to an adversary's advantage.

3.7.5. Computing, Communications and Networking (CCN) Division

Within CCN Division, the Integrated Cyber Security Initiative Office provides institutional management for internal and external technical computer security programs. This Office has responsibility and authority for:

- providing LANL with a balanced institutional view of the threats, risk, mitigations and solutions in the cyber security arena;
- providing programmatic leadership, management, and coordination for external DOE technical cyber security programs (e.g., DOE security architectures, Tri-Lab initiatives);
- providing programmatic leadership, management, and coordination for the LANL institutional technical cyber security program;
- providing leadership and support in maintaining an evolving, adaptive, and innovative technology-based desktop and network architecture consistent with state-of-the-art cyber protections in a "federated" management structure;
- providing technical leadership and coordination for LANL system administrators and organizational security representatives for cyber security programmatic involvement and compliance;
- serving as an institutional resource for identifying, developing, coordinating, and promoting good workstation and network security management practices;
- supporting the security-relevant technical training and certification of system administrators and network administrators; and
- providing technical support for the Senior Technical Information Security Policy Board (IPB) chaired by the Principal Deputy Laboratory Director.

3.7.6. Nonproliferation and International Security (NIS) Division

NIS Division is a science and technology organization with the mission to develop and apply preeminent science and technology to deter, detect, and respond to nuclear proliferation, and to ensure that U.S. and global nuclear security challenges can be met. With respect to LANL security, the division provides methods and application of radiation detection and information technologies for the protection of nuclear materials and for related nuclear safeguards and nonproliferation issues, including cyber security, and has responsibility and authority for:

- providing technical leadership and support for the measurement, control, and accounting of nuclear materials and for cyber security;
- providing technical products, including instrumentation, software, and studies, to LANL organizations in support of the measurement and tracking of nuclear materials and of cyber security; and
- providing research and development for improved nondestructive assay methods, automated information analysis, and nuclear safeguards and nonproliferation policy analysis.

3.7.7. Environment, Safety, and Health (ESH) Division

ESH Division is primarily a service organization that provides a wide range of technical expertise and assistance in areas that include worker health and safety, environmental protection, facility safety, nuclear safety, hazardous materials response, ES&H training, occurrence investigation and lessons learned, and quality. With respect to LANL security, the division has responsibility and authority for:

- managing the institutional requirements system, which must be used for the development and issuance of all LPRs and LIRs, including those for ISSM.

3.7.8. Facilities & Waste Operations (FWO) Division

FWO Division is primarily a service organization that assures that current and future facilities and infrastructure are planned, built, operated, maintained, and provided with appropriate facilities support and services. This includes facilities engineering, maintenance and operations services, fire protection services, utilities, coordination of facility management, and facilities planning. With respect to LANL security, the division has responsibility and authority for:

- managing waste disposal, recycle programs, and salvage operations, which allow FWO and JCNNM personnel to serve as a "safety net" to detect any unauthorized disposal of classified or sensitive information, material, or equipment.

3.7.9. Project Management (PM) Division

PM Division is primarily a service organization that provides project management, engineering, and construction expertise and assistance in areas relating to the planning, design, and construction of LANL facilities and other physical assets. Services include application of formal systems engineering controls to manage project resources, engineering services, and construction services that drive successful project completion. With respect to LANL security, the division has responsibility and authority for:

- providing the central institutional base for the project management core competency at LANL;
- managing line-item, expense, and general plant construction projects;
- establishing and controlling project technical scope, cost, and schedule baselines to support successful completion of construction projects;
- directing the LANL's acquisition and management of engineering, construction, and design/build contractor services; and
- managing LANL's comprehensive site planning process.

3.7.10. Audits and Assessments (AA) Office

The AA Office provides formal audits, assessments, and evaluations of LANL facilities and operations. With respect to LANL security, AA has responsibility and authority for:

- evaluating division-level self-assessments and security function evaluations to provide a comprehensive, integrated summary of LANL security performance to the LANL Director; and
- manage the safety function manager (SFM) program, which includes security as a functional area. Responsible for ensuring important security-related information is brought to the attention of senior managers through the SFM reporting channels.

3.7.11. Business Operations (BUS) Division

BUS Division manages and coordinates LANL's institutional processes for resource planning, prioritization, and management and for establishing subcontracts. They also provide services for packaging and transportation (P&T) of radioactive and hazardous materials. With respect to LANL security, BUS has responsibility and authority for:

- providing effective institutional processes for managing resource planning and prioritization to meet security needs;
- providing effective processes for managing the security needs of contractual relationships with LANL subcontractors; and
- providing P&T support and services throughout LANL.

3.7.12. Institutional Security Committees

Institutional (vs. organization-specific) security committees provide specialized expertise for meeting specific institutional requirements. These committees (1) have a strong relationship to security issues; (2) have a technical or operational, rather than organizational focus; and (3) have a Labwide scope. Committees are chartered in response to specific laws, LIRs, or best work practices. Committee members comprise experienced LANL personnel and security subject matter experts (SMEs), with some committees having members external to LANL. Every committee is accountable, auditable, and reports to a specific LANL manager. The role of this manager is to serve as champion for the committee and includes issue resolution; approval of funding, as appropriate; membership; reporting; and communicating with LANL senior management.

Committees can be authorized either to approve work activities or to serve only in an advisory role. In either case, the security-responsible line-management chain retains the ultimate responsibility for authorizing and directing the work and ensuring it is done safely and securely. However, some committees have the authority to permit or prohibit work, as described in their committee charter.

Charters for each committee contain a discussion of the committee's purpose and a statement of their authority. Charters also establish provisions for membership appointment and terms, reporting structure, funding mechanisms, and other information relating to the functions of the committee. LANL security committees are created and dissolved as requirements change, and charters contain sunset clauses to ensure that justification for continuation is reaffirmed periodically. The Deputy Laboratory Director for Operations is responsible for overseeing the committees, establishing essential funding mechanisms, and ensuring that these requirements are met.

A listing of LANL security committees and current committee chairs is maintained by S-DO and can be accessed through the LANL home page under the general topic of security.

4.0. Training

An essential aspect of preparing for work is ensuring that the workforce possesses the experience, knowledge, skills, and abilities necessary to securely and effectively discharge their responsibilities.

The LANL training program builds the knowledge, skills, and abilities of the LANL workforce, commensurate with their assigned jobs, to support the secure performance of LANL work. LANL's systematically designed training program, delivered by decentralized organizations with centralized program management, provides the workforce with institutional, facility, and job-specific training, as appropriate.

Labwide training organizations offer training courses and programs to train the workforce in accordance with applicable LIRs. Line managers ensure that workers receive training commensurate with job assignments. As appropriate, LANL facilities identify and design worker qualification and certification programs for workers performing jobs that have higher risk.

The institutional LANL training requirements are based on LPRs, LIRs, and Appendix G of the UC-DOE contract. Facility- and job-specific training requirements are based on the security interests and associated risk specific to each facility. Job-specific training takes into account security knowledge and skill requirements. The LANL Training Questionnaire (in LIR-300-00-04) is a tool to assist managers and workers in identifying required training based on job functions performed. The Employee Development System (EDS) is LANL's official database of training records for UC and contract employees, including the training records of subcontractors. Training data recorded and reported in EDS includes course and worker training histories, training plans, training notifications, and training status reports. Electronic training plans in the EDS enable LANL to track a course or group of courses required for specific workers to perform specific job functions and to check whether the training has been completed or has expired. These plans are an important electronic tool supporting the worker authorization process, including onsite access authorization.

OJT (on-the-job-training) is an instructional method in which LANL workers learn job-specific knowledge and skills in the work environment. OJT is delivered in a systematically developed and consistent manner and documented. A tailored approach to OJT is used at LANL and takes into account the level of risk to determine the amount of formality to apply to OJT. The higher the risk, the greater the formality in the preparation and delivery of the OJT.

LANL also provides opportunities for workers to enhance their professional growth and development through educational and career development opportunities, as defined within the UC-DOE contract.

4.1 Senior Technical Managers

Senior technical managers are line managers at the level of division director and above. This includes division directors, Associate Laboratory Directors, Deputy Laboratory Directors, and the LANL Director. Senior technical managers must have demonstrated technical understanding of the work and security interests and risks associated with the missions of their organizations. Facility-owning division directors must understand the security authorization bases for the facilities and operations they own and be qualified for unescorted access to these facilities consistent with security requirements. During each year, the LANL Director will host speakers that are recognized experts in the field of security. Attendance by senior technical managers is required for these sessions.

4.2. All Managers and Supervisors

To demonstrate and sustain LANL's commitment to security and to ensure the continued integration of security into all aspects of LANL's work activities, managers at all levels must seek ways to continuously improve their understanding of security. This includes:

- required ISSM training for new managers and supervisors, consistent with the ISSM content in general employee training (GET) required for all new workers and in annual security awareness training required for all workers; and
- any additional ISSM training for managers and supervisors, as required by the LANL Director.

4.3. Facility Managers

In addition to the training stated above, training and qualification for FMs shall be consistent with the requirements of LIR 280-01-01, "Facility Management Training and Qualification (FMTQ) Program," which includes the requirement for the secure management of all facility work such as maintenance, repair, modification, or construction (see Section 5.3.4.). This training is coordinated by the IFMPO and is provided through institutional training organizations. The FMTQ Program consists of two components: core requirements and FMU-specific requirements (see LIR 280-01-01).

4.4. Workers

All new workers are required to take GET, which provides basic knowledge regarding ISSM and specific security topics. Annual security awareness training required for all workers reinforces this initial training. Additional security training required for workers is based on the job function, the location of the work, and the individual work activities each worker performs. For example, before assuming duties as an OSSO, an organizational computer security representative, a classified document custodian, an authorized derivative classifier, a nuclear material custodian, etc. (see Section 3.5.), you must receive the required training to enable you to meet the associated responsibilities. UC workers, JCNNM, PTLA, and contract-labor personnel complete a training questionnaire, which includes security, to determine the appropriate training and training plans. The training questionnaire is validated on a yearly basis during performance appraisal time or whenever a job function, work location, or activity changes significantly. Additional OJT may be added to individual training plans, as appropriate.

Subcontractors, other than the aforementioned, ensure that all personnel working on a project or at a facility are trained and qualified to conduct the work in a secure and cost-effective manner.

5.0. Requirements Processes that Support the Five-Step Process

The foundation of ISSM is an organization structured according to the eight guiding principles, using the five-step process to perform work securely. There are a number of processes that are required to structure the organization and implement the use of the five-step in the workplace. Again, line managers and other workers of an organization are ultimately responsible and accountable for performing their work securely.

Expectations (requirements) for the secure performance of work at LANL are established at the institutional, facility, and activity levels and, collectively, make up LANL's overall institutional

requirements system. Institutional expectations are created by reviewing the work throughout LANL, then flowed down as requirements to the facility and activity levels (see Figures 4 and 8 and Section 5.1.). Facility-"level" security requirements comprise all relevant institutional security requirements plus any facility-"specific" security requirements. Activity-"level" security requirements comprise all relevant institutional security requirements and facility-"specific" security requirements plus any activity-"specific" security requirements. Institutional, facility- and activity-specific requirements are identified via prescribed institutional processes (see Sections 5.1.-5.3.). This provides an integrated set of requirements for all LANL work that consists of a sufficient combination of relevant institutional requirements plus any facility- and activity-specific requirements.

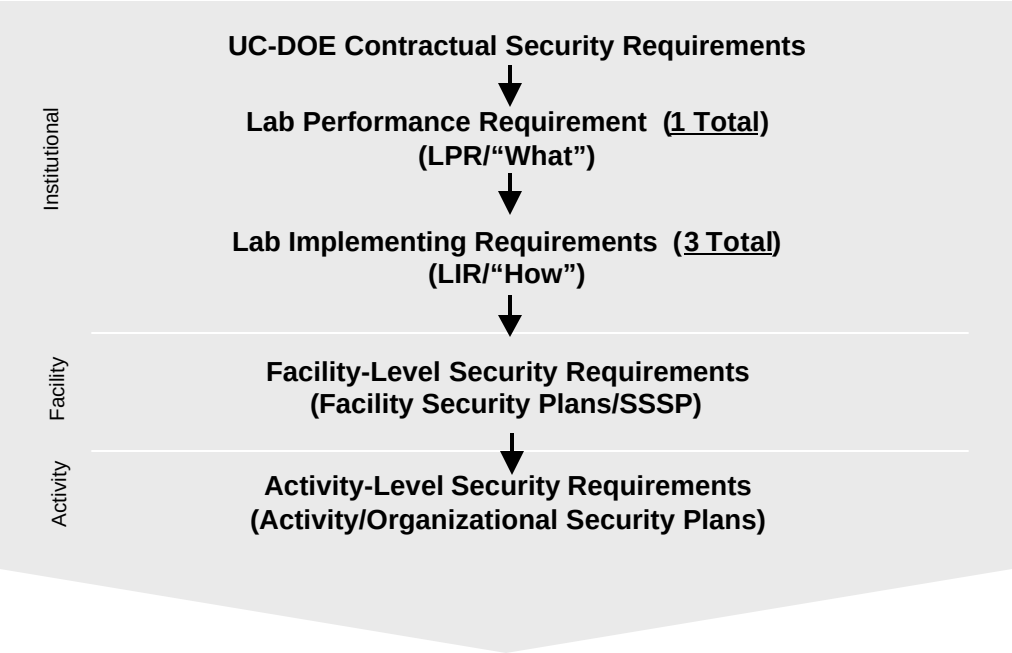


Fig. 8. ISSM flow down of contractual and other security requirements to the work.

Figure 8 shows the flow of institutional security requirements from the UC-DOE contract down through the ISSM Laboratory Performance Requirement (LPR) and Laboratory implementation requirements (LIRs), and further down through facility- and finally activity-level security requirements that govern the secure performance of work "on the floor." Fundamental to ISSM is that all work will be performed securely while meeting the applicable institutional-, facility- and activity-level expectations. To achieve integration of these three levels of expectations, LANL has tools that provide the necessary communication between the levels.

Within the institutional requirements system, the ISSM LPR and LIRs, derived from contractual and certain other DOE requirements, communicate institutional requirements that govern all LANL work

(see Section 5.1.). Facility security plans communicate facility-level security requirements (see Section 5.2.). Activity security plans communicate activity-level security requirements (see Section 5.3.) for research and general office work. For a given organization, activity security plans may be combined into a single organization-wide document called an organizational security plan to govern an organization's

entire set of activities (see Section 5.3.3.). Facility management work control (FMWC) communicates activity-level security requirements (see Section 5.3.4.) for facility work (i.e., work on facilities). Through the use of facility-tenant security agreements (see Section 5.2.5.), the activity security plan controls and/or organizational security plan controls are integrated with the associated facility security plan controls. All of these requirements must be mutually consistent and integrated if work is to be performed securely and cost effectively.

5.1. Institutional-Level Processes

Institutional-level processes and requirements govern all LANL work. These expectations derive from statutory requirements, contractual agreements between UC and DOE, and LANL practices. LANL commits to meet all applicable federal, state, and local laws and regulations and other contractual obligations, unless formal relief is obtained from the cognizant agency.

5.1.1. Contractual and Other DOE Security Requirements

Contractual and certain other DOE security requirements form the basis for the security expectations at LANL, consistent with contract clauses 5.5 and 10.1-10.6 of the UC-DOE contract. The contractual requirements are listed in Appendix G of the UC-DOE contract. In addition to the contractual requirements, certain other DOE security requirements are observed by LANL as a matter of operational policy, consistent with guidance from LANL Legal Counsel. The determination of the set of DOE security requirements mandatory at LANL is based on the nature and scope of LANL's work and associated security interests and risk. All DOE security requirements are aimed at ensuring sufficient protection of security interests for national security.

5.1.2. Internal Institutional Requirements

Contractual and certain other DOE security requirements are numerous, subject to interpretation, and not easily applied by workers. To effectively deploy these security requirements in the workplace, LANL has established and maintains internal institutional security requirements derived from these DOE security requirements. The highest level internal security requirement is the ISSM LPR, which establishes institutional performance expectations for performing work securely and references mandatory DOE security requirements. Meeting the performance expectations in this LPR, including the performance criteria, helps ensure that DOE security requirements will be met. Changes to this LPR follow the process cited in LIR 301-00-00, "Managing Change Control of Laboratory Operations Standards and Requirements."

Because LANL management has determined the need for some Labwide consistency in how the ISSM LPR is met, including the referenced mandatory DOE security requirements, LANL has established and maintains three security LIRs: General Security, Classified Security, and Nuclear Safeguards. This integrated set of LIRs is grouped by the three major types of work and associated security interests at LANL, instead of being grouped by the numerous DOE security topical areas, which would have yielded a much larger, less integrated set of LIRs. Note that the first LIR (General Security) applies, in whole or part, to all LANL organizations, whereas the other two apply only to those organizations having classified matter and/or nuclear materials. Each LIR must flow directly from the ISSM LPR and provide more detailed implementing requirements for the secure performance of work. Contents of these LIRs derive substantially from the contractual and certain other DOE security requirements. The ISSM LPR and three subordinate LIRs have a responsible SFM and a cognizant OIC. The OIC

coordinates the development and maintenance of the LPR and LIRs to ensure their sufficiency with respect to addressing the expectations contained in the contractual and certain other DOE security requirements. Generally, the need for new or revised internal institutional security requirements (LPR and LIRs) is identified by the cognizant SFM or OIC, who submits proposals to their line management and to ESH-Division's Operational Integration Office (ESH-OIO).

In addition to the three mandatory LIRs, Laboratory implementation guidance (LIG) documents provide discretionary (i.e., non-mandatory) guidance, or good business approaches, relating to security practices, and are coordinated by the cognizant OIC. In special cases, LANL requirements and guidance can also be expeditiously established and communicated throughout LANL via urgent memoranda, alerts, and notices. The urgent memoranda, alerts, and notices are similar in purpose, but vary somewhat in their urgency, distribution, and formality of purpose. All LPRs, LIRs, LIGs, urgent memoranda, alerts, and notices are official LANL documents and are published for workers and managers on the web through the LANL home page.

LANL processes for developing, revising, documenting, communicating, maintaining, and managing LIRs, LIGs, urgent memoranda, alerts, and notices are established and described in detail in LIR 301-00-01, "Issuing and Managing Laboratory Operations Implementation Requirements and Guidance." This LIR is supplemented by LIG 302-100-03, "Guide for Developing Laboratory Operations Implementation Requirements and Guidance." The processes established in this LIR and LIG are managed and coordinated by ESH-OIO. As described earlier, LPRs and the overall institutional operational requirements hierarchy are managed through processes described in LIR-301-00-00.

The SFM and/or OIC solicit input from affected workers, security SMEs, the NNSA, and others, as appropriate, and then draft and complete new or revised documents. Conflicts among different organizations are resolved via an established process of management review up through the Deputy Laboratory Director for Operations, as required. Upon final approval by the OIC's division-level line manager, new requirements documents are placed on the web by ESH-OIO and communicated to all LANL organizations.

The official record and listing of institutional security expectations exist electronically on the web under the "Official Documents" section of the LANL home page. In addition to LPRs, LIRs, and LIGs, there are unclassified listings of security lessons learned, as well as security forms and templates. Only institutional requirements documents residing on the web are official LANL requirements.

5.1.3. Technical and Management Requirements

LANL requirements generally fall into two major categories: those that establish required management processes and those that establish technical requirements or specific security controls. The three security LIRs include both management processes and technical requirements.

Required management processes to be used by LANL line organizations, facilities, and workers include formal processes used throughout LANL for establishing requirements at the institutional, facility, and activity levels. Examples include the Labwide processes for establishing LIRs, facility security plans, activity security plans, and facility-tenant security agreements. These management processes define the

explicit institutional consistency, formality, and rigor needed for establishing these expectations, while also allowing appropriate tailoring to meet the specific needs of widely disparate facilities and activities.

Technical requirements identify and prescribe explicit physical and/or administrative controls for specific security interests and associated risk. The required controls are mandatory anywhere throughout LANL where the related security interests and associated risk exist as part of the work activity. For example, a technical requirement might establish specific controls that are necessary for protecting and controlling classified matter or special nuclear materials. Some technical requirements also establish specific performance criteria for controls. For example, in conducting nuclear material physical inventories, if a statistical sampling plan is used, the plan must specify the nuclear material population, confidence level, minimum detectable defect, definition of a defect, and action to be taken if a defect is encountered.

5.1.4. Application of the Quality Criteria

LANL incorporates quality assurance into internal institutional requirements. LPR 308-00-00, "Quality," specifies LANL's approach to meeting its contractual requirements in the quality arena. As such, the scope of LPR 308-00-00 includes all work conducted at LANL, regardless of whether the work is conducted in a nuclear or non-nuclear facility. LPR 308-00-00 serves as the quality umbrella document for all LPR and LIR documents. All such documents must explicitly address the applicable requirements of LPR 308-00-00. Furthermore, all new or revised LPRs and LIRs are subject to an independent review to determine whether the 10 criteria of LPR 308-00-00 have been adequately met, and organizations that draft or revise LPRs and LIRs must take steps to ensure that review findings are adequately addressed prior to publishing the LPR or LIR.

5.1.5. Offices of Institutional Coordination

LANL assigns an OIC for each LIR. The OIC is normally the LANL group or office responsible for establishing, coordinating, and supporting the implementation of a requirement and any associated guidance. When requested, the OIC shall provide subject matter expertise to LANL organizations. This expertise shall include that OICs provide consistent institutional interpretation(s) of requirements contained in standards, laws, and regulations that are promulgated as requirements in the LIR(s) they are assigned. ESH-OIO maintains a current list of OICs and their assigned LPRs, LIRs, and LIGs.

5.1.6. Points of Contact

Per LIR 301-00-01, each division director, program director, and office director appoints a POC, who acts on behalf of their organization to coordinate communication on institutional requirements among their organization, the OICs, and ESH-OIO. For security, POCs are supported by the designated security representative(s) within their organization. The POCs determine and communicate to ESH-OIO the organizational relevance, or applicability, of institutional requirements. If an organization's work does not involve the security interests or directly relate to the subject LANL requirements, then the requirements are not relevant to that organization. The POCs solicit input for creation and revision of requirements, communicate new requirements to their organization, and monitor and "self-report" the implementation status of all LIRs applicable to their organization.

5.1.7. Work for Others (WFO)

WFO is work that is sponsored by a funding agency other than the DOE, including other government agencies and private industry. ISSM and associated Labwide security requirements apply to WFO and

work for DOE with the same force and effect. WFO activities must meet all applicable institutional, facility, and activity requirements. The security-responsible line-management chain is responsible for the secure performance of their work. Classification of a program shall not shield the activity from working within LANL's ISSM system. Work that cannot be performed securely will not be started, and work that is not being performed within the security requirements will be stopped and restarted only after appropriate upgrade and review of the security systems.

5.1.8. Changes and Deviations

LANL has formal processes by which organizations can pursue changes to and/or deviations from LANL requirements. Proposed changes or interpretations of institutional expectations (ISSM LPR, LIRs, or LIGs) can be submitted in writing by any member of the workforce through their organization's POC to the cognizant OIC. This process is defined in the General Security LIR. Also, with valid justification, organizations can pursue deviations from established institutional requirements as long as equivalent or compensatory measures are in place. Deviations must be approved by the cognizant OIC, their division-level line manager, and, where required, by NNSA. The NNSA/AL Manager has committed to work closely with LANL to achieve security objectives in a defensible, efficient, and cost-effective manner. This includes, when justified and formally documented, seeking relief from DOE security requirements that do not withstand cost-benefit scrutiny at LANL.

5.1.9. Applicability and Implementation of Requirements

LIR 301-00-01 requires that POCs declare which LIRs are applicable to their division and when the applicable LIRs are implemented. POCs also must notify ESH-OIO when a notice has been received, indicating that if requirements are stated and applicable, they will be implemented. For POC declarations to be meaningful across the institution, the definitions of applicability and implementation must be understood and applied uniformly.

A LIR is applicable in an organization if it covers work, including administrative tasks, being performed by anyone in the organization. This means that the organization must have a thorough understanding of the work performed by every individual and a thorough understanding of LANL's requirements. The understanding of the work can be derived from, e.g., facility security plans, activity security plans, facility-tenant security agreements, or work inventories as required in the General Security LIR. It is the responsibility of the POC to understand the content of LANL requirements and make the necessary connection with the work being performed. It is the responsibility of the cognizant division director, program director, or office director to assess both the performance of the POC in making the determination and the organization in meeting the LANL requirement.

A LIR is implemented within an organization if the work, including administrative tasks, is performed according to the requirements of the relevant LIR(s), or a deviation has been granted to perform the work to another suitable requirement. This means that the individuals performing and managing the work are aware of the LIR(s) and understand and meet the work requirements.

Institution-wide implementation is achieved when all organizations have established and consistently employ work practices that meet the requirements of the ISSM LPR and applicable LIR(s), and any deviations have been approved through the formal LIR change process. A satisfactory level of

implementation can include some local defects and opportunities for improvement. Where requirements are new, deficiencies may not be evident until implementation is attempted.

5.2. Facility-Level Processes

5.2.1. Facility-Owning Organizations

All LANL space, including land, physical structures and facilities, is assigned to facility-owning division directors and becomes part of an FMU. An FMU can include multiple facilities, buildings, other structures, and large areas of land. For each facility or building within an FMU, facility-specific security expectations must be established, as appropriate, and met along with all applicable institutional security expectations.

Facility-specific security expectations comprise defined limits, boundaries, and facility processes to ensure that the current security capabilities of the facility (also referred to as the facility security operating limits or security envelope) are not exceeded and that institutional expectations are met. These expectations also establish the requirements for interfaces between the facility-owning division director and/or their designated security representative, tenants, the facility management team, and support organizations. Note that the facility-owning and tenant organizations may or may not be the same. Facilities that support the performance of work document security operating limits in their facility security plans (see below). Through these and facility-tenant security agreements, facilities communicate their expectations for the secure performance of work and may establish specific requirements for inclusion in secure work practices (see Section 5.3.).

5.2.2. Facility Security Plans

The facility security plan (analogous to the facility safety plan) is the primary mechanism for establishing, documenting, and integrating facility-level security expectations. The purpose of a facility security plan is to systematically evaluate and document the work in a facility, the associated security interests and risk, co-located tenant activities that may be incompatible, and facility-level security controls from the standpoint of facility-wide security operating limits. Similar to establishing institutional expectations, establishing a facility security plan must involve the people doing the work, SMEs, and others, as appropriate, to ensure appropriate tailoring to the work, including its location, and conformance with applicable institutional requirements. The requirement for facility security plans is established here and in the General Security LIR.

The facility security plan describes the collective work of an FMU (or facility, building, or other subset, depending upon the security interests and associated risk). The plan includes an analysis of a facility's security interests and associated risk and identifies facility-level (including any facility-specific) expectations and controls to effectively manage risk (i.e., fulfills the first three steps in the five-step process). The facility security plan contains a definition of the facility's security operating limits (or security envelope) and a description of the facility's physical and administrative controls. It includes and is consistent with applicable institutional expectations (i.e., ISSM LPR, LIRs**,** and other institutional requirements). Given the dynamic nature of experimental operations, it may be necessary for facility security plans to incorporate mechanisms for the selective review of activity security plans to ensure that work stays within facility security operating limits.

Facility-owning division directors and/or their designated security representatives formally negotiate and document with S Division their respective roles, responsibilities, and authorities for establishing and implementing facility security plans, including (1) establishing facility security operating limits that bound the work that can be done securely; and (2) providing essential facility infrastructure to support secure work in facilities, including facility-related structures, systems, and management processes (e.g., exterior lighting, security fences, vaults, vault-type rooms, local and Labwide computer networks, interior and exterior intrusion-alarm and electronic access-control systems, and facility-wide administrative procedures for monitoring foreign national visitors and assignees). These structures, systems, and management processes are called facility-level controls. These facility-level controls and expectations are documented in facility security plans, which may be included, in whole or part, in the LANL SSSP, and all of which, as negotiated with S Division, are the shared responsibility of S Division and the cognizant facility-owning division directors and their designated security representatives, who may or may not be a member of an FM team or serving as an OSSO. Facility-owning division directors and/or their designated security representatives must also coordinate the development of facility-specific security expectations with affected tenant organizations (see Section 5.2.5.). To simplify and expedite the development and use of facility security plans, simple templates and other user-friendly forms and guidance are provided by S Division.

The facility security plan may be a single document with appropriate references or a compilation of other applicable documents, such as facility-tenant security agreements, facility procedures and manuals, emergency plans, quality management plans, tenant operating envelopes, and conduct-of-operations plans. The level of detail of the work description, the rigor of risk analyses, and the nature of required facility processes and controls in a facility security plan are commensurate with the security interests and risk associated with the facility, consistent with applicable LIRs.

5.2.3. Facility Security Plan Levels of Rigor

Two distinct levels of rigor exist for facility security plans -- one for facilities requiring only LANL approval and another for those requiring joint LANL-NNSA approval. The former facility security plans may be short and mainly reference institutional programs and/or a few facility-specific documents, such as emergency evacuation plans. The latter facility security plans reflect much more extensive analysis and formality of operations, consistent with the facility and associated collection of security interests and risk, as currently required for special facility security plans (SFSPs) and the LANL SSSP (see Section 5.4.).

5.2.4. Changing Facility Security Plans

The facility security plan also addresses how the facility-level security expectations are maintained, and establishes mechanisms to ensure revision of the facility security plan, as appropriate, when work and/or associated security interests and risk change. Maintaining expectations may include processes such as facility-tenant security agreements; review of activity security plans; change control; configuration management; and assessments. The facility security plan addresses the means for identifying changes in activities or facility conditions and associated security interests and/or risk that could result in a need to revise expectations established in the facility security plan. It may also address processes for allowing deviations to the facility security plan or other changes based upon input by workers, experts, and/or regulators. For major SNM facilities, revisions may involve the unreviewed safeguards and security

question determination (USSQD) process, which is managed by the joint LANL-NNSA SSSP Change Control Board.

Except when covered by an agreement with a regulatory party, the facility security plan and referenced documents —but not institutional expectations—can be changed at the discretion of the facility-owning division director. Proposed changes or interpretations are submitted in writing by any member of the workforce to the facility-owning division director. Disagreements regarding the security expectations in the facility security plan shall be resolved within the supervisory chains of the facility-owning division director and the organization proposing the change. Ultimately, the facility-owning division director has the authority to determine facility-specific requirements in the facility security plan, consistent with applicable LIRs. In addition to ongoing changes, the facility security plan and referenced documents shall be systematically reviewed and updated at least annually by the facility-owning division directors and/or their designated security representatives.

5.2.5. Facility-Tenant Security Agreements

Facility-tenant security agreements are described in the General Security LIR. Their purpose is to formally establish and help ensure mutual understanding of the security roles and relationships between the facility-owning organization and the tenants doing work in the facility. They are written for all LANL facilities, and their completion is the responsibility of both the facility-owning division director and/or their designated security representative and the tenant organization. These agreements place restrictions on the work that can be performed in a facility and upon the systems and services provided by the facility to their tenants. They are jointly approved by the facilities and their tenants. There are requirements on changing activities and their controls and changing facility services and controls that must be met by the facility and their tenants. This means that, once a facility-tenant security agreement has been signed, there are agreed-upon communications that must occur concerning work activities and their controls. All work controlled through secure work practices (see below) must stay within the limits and control capabilities defined in the facility security plan and, conversely, the facility must maintain the controls and systems that allow work to be performed securely in the facility.

5.3. Activity-Level Processes: Work Control

Once again, ALL WORK is performed at the ACTIVITY LEVEL. ISSM is structured to control all work at the activity level in accordance with the five-step process. Fundamental to ISSM is that all work will be performed securely and meet the applicable institutional, facility-, and activity-specific security requirements. Moreover, all work is performed in an FMU, which consists of the grounds, structures, and services within geographical areas. Work on the physical structures, systems, and grounds of the facility is called facility work (see Section 5.3.4.). Tenants of FMUs perform all other types of work, including research and general office work (see Section 5.3.3.).

LANL uses secure work practices (see General Security LIR) and facility management work control (FMWC) to establish minimum expectations for the secure performance of work (see Sections 5.3.3. and 5.3.4., respectively). These institutional processes require that all work be authorized at the lowest appropriate security-responsible line-management level, commensurate with the security interests and risk associated with the work, and the sufficiency of the security control system. Similarly, workers are authorized to perform work based on their management's acceptance of their knowledge, skills, and abilities to conduct work securely within the authorized security control system. When LANL needs to

use the services of a vendor to perform work (such as maintenance on equipment), there is a contracting mechanism to do this. Part of the contracting mechanism is a process to identify and communicate the security expectations that must be agreed to and met by the vendor to ensure their work is performed securely. The security portion of the contracting mechanism is contained in "Notice 10" of the institutional requirements system. "Notice 10" supplements both secure work practices and the FMWC because either may use vendors.

At the activity level, the work scope may be narrowly defined to encompass only one or a few specific tasks such as opening, closing, and checking a classified safe, or broadly defined to include a collection of activities and associated security interests and risks such as those embodied by the pit manufacturing program. In both cases, the workforce establishes and implements activity-level security expectations using the first three steps in the five-step process: define the scope of work, analyze the security risk, and develop and implement the security controls. Security-responsible line managers authorize work only after the first three steps have been completed. Security-responsible line managers must know their workers' work and the associated security control systems sufficiently to be satisfied that the work can be authorized and is within their workers' competence. Formality, rigor, and the extent to which workers perform the first three steps are determined by line management (see Sections 5.3.3. and 5.3.4.) and are commensurate with the security interests and risk associated with the work. Although most activities are authorized by the UC-DOE prime contract, the NNSA may be involved in jointly authorizing specific LANL work depending on the security interests and risk associated with the work.

5.3.1. Types of Security Interests

The following is a general listing of the types of security interests that may be associated with a specific work activity and, therefore, would be subject to risk analysis and control as well as work and worker authorization before the work is performed (see General Security LIR):

- **Nonsensitive matter:** This category of unclassified "matter" (i.e., information, material, and equipment such as electronic and hardcopy documents and/or data, machined parts, photographic and magnetic media, etc.) requires minor work-control measures and minimal work and worker authorizations.

- **Sensitive unclassified matter:** This category contains matter that may be designated as unclassified controlled nuclear information (UCNI), official use only (OUO), proprietary, etc. Work and worker authorizations must address need-to-know access and controls to ensure effective protection against unauthorized access or disclosure. Controls will depend on operational conditions such as:

  - form of the matter (e.g., electronic or paper)
  - location of the matter (e.g., within a security area, property protection area, leased facility, etc.)
  - presence or access of individuals without appropriate need-to-know
  - special considerations, such as the presence of foreign nationals

- **Classified matter:** This category contains matter specifically designated as classified. It may contain Restricted Data (RD), Formerly Restricted Data (FRD), or National Security Information (NSI). Work and worker authorizations must address accountability, access control, in-depth

physical security layers, and need-to-know access authorization. Controls in place must ensure effective protection against unauthorized access or disclosure. Controls will be based on the type of matter being protected such as:

- top secret/accountable
- top secret (RD, FRD, NSI)
- SAP/SCIF
- secret (RD, FRD, NSI)
- confidential (RD, FRD, NSI)

- **Special nuclear material (SNM):** This category contains nuclear material specifically designated as special nuclear material by the DOE, consistent with the 1954 Atomic Energy Act as amended. Work and worker authorizations must address accountability, access control, in-depth physical security layers, and need-to-know access authorization. Controls in place must ensure effective protection against unauthorized access or disclosure. Controls will be based on the attributes of the SNM being protected such as:

  - SNM type (e.g., plutonium or high-enriched uranium)
  - SNM quantity and attractiveness (category I, II, III, or IV)

5.3.2. Types of Security Areas

For an organization to perform its work securely, it may need to establish a security area(s). Security areas must meet applicable institutional, facility-, and activity-specific security requirements as documented in associated security plans (e.g., the LANL SSSP and/or activity security plans, which organizations may combine into a single organization-wide document called an organizational security plan – see Section 5.3.3.). The following are specific types of security areas that must be established depending on the security interests associated with specific work (see General Security LIR):

- limited areas
- exclusion areas
- protected areas
- material access areas
- vital areas

5.3.3. Research and General Office Work

This type of work involves the majority of work activities at LANL (see Section 5.3.4. for the other type of work, i.e., facility work). The “secure work practices” approach in the General Security LIR (analogous to safe work practices in ISM) addresses this type of work by embedding the five-step process in its work and worker authorization process. This approach is to be followed by all line management organizations for establishing activity-level (including any activity-specific) security expectations for this type of work. This approach establishes requirements for the authorization of work and workers, based upon a formal process for defining the scope of work, analyzing security risk, and developing/implementing appropriate security controls. This approach also establishes the institutional requirements for documenting activity-level security analyses and controls for this major type of work.

Applying secure work practices is the responsibility of the security-responsible line-management chain for the activity or collection of activities to be authorized and performed. The controls developed by applying this approach are documented in activity security plans (analogous to hazard control plans) or combined into a single organizational security plan. Both types of plans are the responsibility of the security-responsible line-management chain for the activity or collection of activities to be authorized and performed. Note that activity security plans should not be combined into a single organizational security plan if doing so would diminish clear communication of activity-specific security interests, risk, and controls to the affected workers. Also, depending on the activity and associated security interests and risk, an activity or organizational security plan may require joint LANL-NNSA approval as currently required for SFSPs and for the LANL SSSP (see Section 5.4.). To simplify and expedite the development and use of activity and organizational security plans, simple templates and other user-friendly forms and guidance are provided by S Division.

The secure work practices approach establishes levels of rigor in the authorization of the work and the workers, consistent with applicable security LIRs that define the management level of authority necessary to authorize work. In general, activities with higher associated risks must be reviewed and authorized by higher line management, while lower risk activities can be authorized at commensurably lower management levels. As part of secure work practices, the security-responsible line-management chain must identify relevant institutional and facility requirements and incorporate them as part of the activity-level controls.

5.3.4. Facility Work

In general, facility work covers all activities involved in the construction and maintenance of the constructed environment and other physical assets of the facility. Facilities and facility work are defined in LIR 230-03-01, "Facility Management Work Control (FMWC)." In combination with the General Security LIR, this LIR defines the process for controlling work on facilities, including defining the scope of work, analyzing security risk, and developing and implementing appropriate security controls before facility work is authorized by the cognizant FM. Together, these two LIRs embed the five-step process in a formal process that provides for the authorization of facility work to be performed by authorized individuals under secure conditions. This ensures that the security and integrity of the facility and its systems are maintained during and after completion of the facility work. Moreover, before performing facility work, facility-owning division directors and/or their designated security representatives, who may or may not be a member of an FM team or serving as an OSSO, must ensure that the proposed work has been coordinated with all affected organizations and that it will not pose an unacceptable risk to security interests (see Section 5.2.5.).

For security-related facility work -- i.e., work involving facility infrastructure that provides facility-level security control (e.g., exterior lighting, security fences, vaults, vault-type rooms, local and Labwide computer networks, and interior and exterior intrusion-alarm and electronic access-control systems) -- facility-owning division directors and/or their designated security representatives formally negotiate and document with S Division their respective roles, responsibilities, and authorities (see Section 5.2.2.).

5.4. Special Approvals or Authorizations

Most LANL activities (work) and associated facilities are authorized by the UC-DOE prime contract. However, depending on the associated security interests and risk, an activity and/or facility security plan

may require joint LANL-NNSA approval – i.e., LANL and NNSA may mutually agree to special authorization of a specific work activity and/or associated facility. The security plans describing this work identify (sometimes by reference) the risk and associated mitigation measures required for authorizing the specific work activity and/or associated facility. LANL's cognizant security-responsible line management and the NNSA determine the conferring parties and basis for authorization or security plan approval. The following are types of special approvals or authorizations.

- **Site safeguards and security plan (SSSP):** The LANL SSSP supplements the UC-DOE prime contract by defining the overall protection strategies for LANL security interests – i.e., LANL-controlled classified and sensitive-unclassified matter, nuclear materials (in particular, special nuclear materials and tritium), and other government resources associated with accomplishing the LANL mission.
- **SAP/SCIF authorizations:** Prior to activating a special access program (SAP) or sensitive-compartmented information facility (SCIF), appropriate authorization must be received from the cognizant agency. This authorization is based on the sensitivity of the material involved and the specific controls implemented to ensure proper protection.
- **Special facility security plans (SFSPs):** SFSPs define the above-baseline scope of work, special security interests, and specific controls that must be implemented to ensure proper protection. With S-Division support, SFSPs are developed by the organization planning to perform the work, and must be approved by NNSA before the work begins.

6.0 Assessment Processes that Support the Five-Step Process

6.1. Confirming Readiness

Confirming readiness ensures that all necessary actions are complete prior to performing work. Depending upon the security interests and associated risk, confirmation may range from relatively informal walk-downs by appropriate members of the supervisory chain to formal readiness assessments performed jointly with NNSA.

Cognizant line management observes the activities of their workforce to ensure they meet activity, facility, and institutional expectations. This includes assessing results, identifying process improvements, taking effective corrective actions, and sharing lessons learned. Facility-owning directors, in cooperation with tenant line management, ensure that work within their facilities meets facility and institutional expectations.

6.2. Assessing Results

The fifth step in the five-step process -- provide feedback and continuous improvement (i.e., ensure performance) -- is aimed at ensuring that work is securely and effectively performed to expectations. This is principally accomplished through self-assessment. Self-assessment activities include all internal performance reviews by UC workers (managers and staff) and UC contractors. These reviews include personnel directly responsible for the work and associated results, as well as reviews by personnel independent of the work and those who perform it. All of these reviews provide the basis for follow-up actions taken by management to improve security performance.

Assessments to ensure performance involve a variety of activities: collecting feedback information on the sufficiency of security controls; evaluating security incidents, including precursors and root causes; taking corrective action in response to incidents, including near-misses; identifying and implementing opportunities for improving work definition, planning, and execution; conducting line, functional, and independent assessments; reinforcing expected (desired) behaviors; and periodically reviewing LANL's overall ISSM system and, as appropriate, refining it to ensure it is a cost-effective, value-adding tool for performing work securely.

Performance assurance activities may be accomplished through mechanisms such as performance assessments, performance measurements, workplace observations, and audits. These mechanisms include processes to ensure performance data are analyzed and lessons learned are shared throughout LANL, consistent with the need to know. The LANL workforce monitors its work, assesses the results, and identifies and implements needed improvements at the activity, facility, and institutional levels to ensure that work performance meets expectations.

Security self-assessments are conducted by cognizant line management and staff, facility owners, institutional service organizations (S Division and ISEC), and the SFM as indicated in Fig. 9. The objective is to understand the behaviors and processes that support security performance expectations. The assessment process helps prevent major unexpected security incidents by enabling continuous security improvement and showing when corrective actions are needed. Assessments are based upon methods and measures selected by and tailored to meet the needs of the assessing and the assessed organizations. Assessment measures indicate performance levels, including the degree to which expectations are met, corrective actions are completed, and incidents are evaluated to prevent recurrence. Assessment results are documented and reported to the cognizant line managers, who take appropriate corrective actions.

6.2.1. Line Management Assessments

Line management is ultimately responsible for security and conducts self-assessments to ensure that their organizations meet all applicable institutional, facility (e.g., facility security plans and facility-tenant security agreements), and activity security expectations. Line management self-assessment processes include management walk-arounds. Management must tailor their self-assessments to meet their organization's needs. Line management self-assessments reinforce good practice and lead to correction of issues and improvement of processes and behaviors.

Management walk-arounds focus on worker behavior in the workplace. They are not inspections directed toward compliance, but instead are cooperative, no-fault efforts between managers and their workers designed to identify needed security and/or work performance improvements and noteworthy practices. Managers perform walk-arounds to ensure that the security interests and risk associated with work are understood and controlled by those supervising and those performing the work. Managers are responsible for documenting their walk-around findings and corrective actions. LANL developed a management walk-around database to increase awareness and understanding of the program and communicate lessons learned.

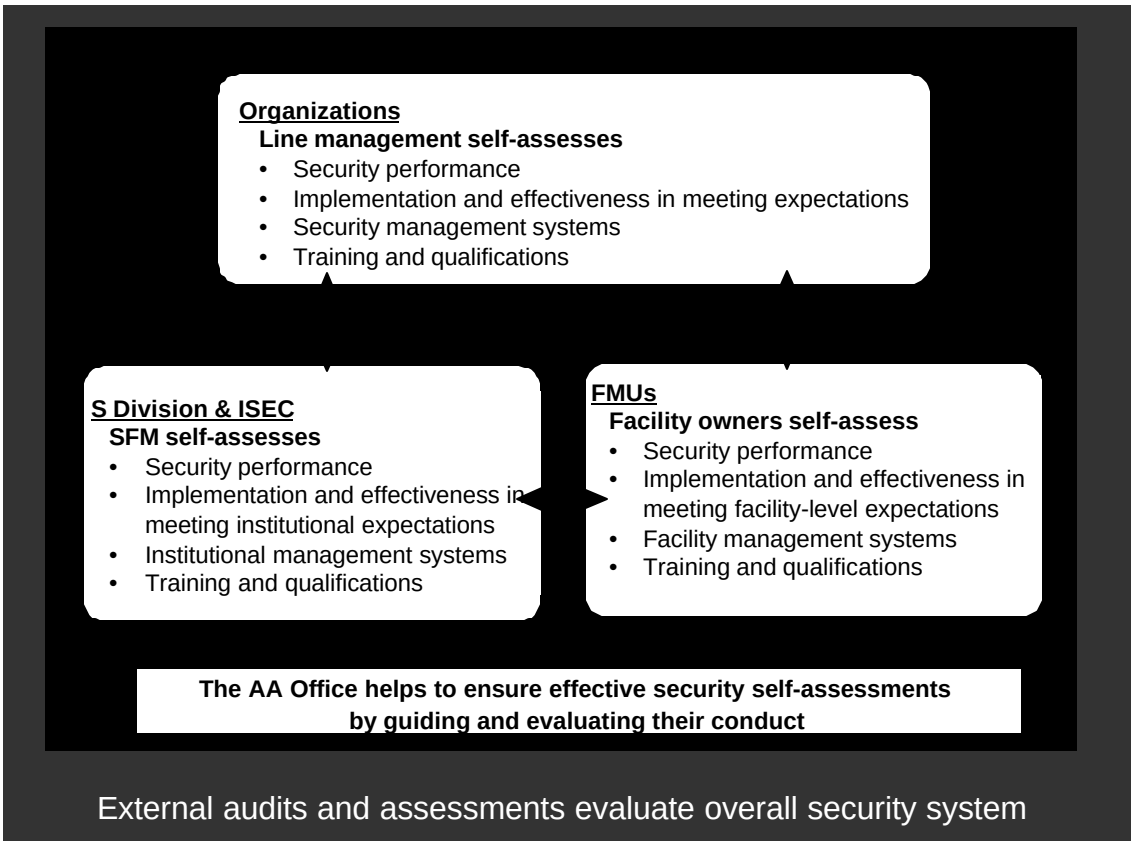


Fig. 9. Assessments.

Similarly, facility self-assessments are tailored to meet the needs of each facility. Facility-owning division directors are responsible for ensuring that expectations established in their respective facility security plans are appropriate. In addition, they have responsibility, along with cognizant tenant line management, for ensuring that expectations in the facility security plans are met by workers in the facility. Because tenant line management is responsible for assessing the security of their activities, duplication is possible. Hence, tenant line-management and facility self-assessments should be coordinated within a facility to avoid duplication.

Tenant line-management and facility self-assessments complement functional and independent institutional assessments (see below) and are performed routinely by all security-responsible line-management chains. These routine line "organizational" self-assessments by each organization are essential for evaluating and ensuring security performance.

For process and reporting requirements regarding division-level organizational self-assessments, see the Self-Assessment LIR.

6.2.2. Functional and Independent Internal Assessments

The LANL Director has appointed a SFM for security. The security SFM is responsible for assessing and reporting on the performance of the institution in the security functional area, including identifying

and developing opportunities for improvement, consistent with requirements established in the Self-Assessment LIR. These functional security assessments are a key element of LANL's overall performance assurance program.

Functional security assessments address all applicable security topics (e.g., nuclear safeguards, classified matter protection and control, and foreign visits & assignments). Integrated Safeguards & Security Assessment Visits (ISSAVs) are a major component of these assessments. ISSAVs are full scope and jointly coordinated and conducted by S Division, ISEC, and cognizant division-level line organizations. They are aimed at evaluating each organization's effectiveness in implementing applicable institutional security expectations and evaluating the expectations themselves. They are also aimed at jointly resolving identified security concerns. ISSAVs are designed to avoid duplication with tenant line-management and facility self-assessments.

AA-2 is the LANL OIC for independent internal assessments and is responsible for the development and implementation of LANL's overall independent internal assessment program. They also analyze the SFM security reports and provide an integrated summary of LANL's security performance to the LANL Director. An additional and important role for AA-2 is to coach line management on conducting effective self-assessments, including evaluating results.

For process and reporting requirements regarding functional and independent internal assessments, see the Self-Assessment LIR.

6.2.3. UC-DOE Contract Appendix F

LANL security performance is tracked and assessed through the use of performance measures, which provide agreed-upon objectives, measures, and targets for security performance. At LANL, performance measures are defined jointly by LANL, NNSA, and UC and are added to Appendix F of the UC-DOE contract. Success in achieving the objectives defined by Appendix F and the performance measures depends upon the effectiveness and implementation of the expectations established at the institutional, facility, and activity levels.

LANL performance is evaluated against the Appendix-F measures through a number of internal and external processes. In addition, LANL representatives meet quarterly with UC and NNSA to discuss both Appendix-F performance versus expectations and related issues and trends. Also, the OWG meets semiannually with UC and NNSA to discuss key metric performance and to describe actions being taken to improve systems and programs. Annually, the LANL, UC, and NNSA each develop comprehensive assessments of LANL's Appendix-F performance.

For process and reporting requirements regarding the self-assessment process for Appendix F measures, see the Self-Assessment LIR.

6.2.4. External Assessments

DOE and NNSA provide security oversight of LANL. This oversight includes periodic audits and reviews. The UC also provides security oversight. LANL self-assessment results, not including the management walk-around database, are provided to DOE, NNSA, and other external reviewers, as appropriate.

6.3. Issues Management and Corrective Actions

LANL maintains issues-management and corrective processes to ensure that important issues (internal and external) are captured and resolved. This includes evaluating and prioritizing issues, assigning them for resolution, tracking corrective actions to completion, verifying that completed actions resolved the issue, and communicating lessons learned. Line management is ultimately responsible for tracking and correcting all security issues. Issues are prioritized and resources are allocated for corrective actions based on appropriate risk-based, cost-benefit analyses. Issues management and corrective actions are evaluated by LANL assessments.

6.3.1. Incident/Near-Miss Assessment

LANL recognizes the value of feedback from operating experience to improve performance and is committed to fostering a “reporting culture.” Security incidents, including near misses, are valued by line management as a source of important data for analysis and improvement. The security SFM also assesses this data to ensure that institutional issues are identified and resolved. Workplace conditions that could affect security are also identified and critiqued in a process coordinated by cognizant line management, involving institutional service organizations, as appropriate. Analysis results, including root causes, corrective actions, and lessons learned, are tracked institutionally to ensure corrective actions are completed and data are trended.

Many security incidents are recognized as consequences of human error and, as such, improvements in security can be expected from the application of concepts and techniques to enhance human reliability in performance. By applying proven techniques to security operations, improvements are likely to be achieved more effectively and efficiently than has been the case for such traditional corrective approaches as standdowns, general security awareness training, and disciplinary actions. In the short term, assessments will provide the foundation on which focused, effective corrective actions (e.g., enhanced training interventions and procedure improvements) can be built.

6.3.2. Workforce Questions, Concerns & Suggestions

Security can be effective only with the full participation of the workers “on-the-floor” -- LANL's front-line experts in workplace security. To this end, many workers throughout LANL have received advanced security training and been designated as security representatives by their respective management (see Sec. 3.5.). These individuals (e.g., OSSOs) are responsible for providing security guidance and assistance to their respective security-responsible line-management chains. They also request security support from institutional service organizations, principally S-Division and ISEC, as needed. All LANL workers can request this same support, including use of the "one-stop shopping" Security Help Desk. This Help Desk can be reached at 665-2002 or by e-mailing your unclassified (and nonsensitive) security questions, concerns, and suggestions to security@lanl.gov. Moreover, the Management Walk-Around Program includes security as a topic and is supported by an unclassified interactive database that allows any manager to identify, communicate, and assign corrective actions to appropriate workers.

7.0. Security-Responsible Behavior

7.1. Introduction

The primary incentive for security is the moral imperative not to compromise the security (i.e., safety) of our nation. Hence, security is a key value at LANL. To perform all LANL work securely, the entire workforce must consistently demonstrate proper security behavior. Here, the term “behavior” is broadened to include attitudes that influence workforce behaviors. LANL promotes proper security behavior through various mechanisms. For these mechanisms to be effective, all workers (including managers) must have well-defined roles, responsibilities, authorities, and accountability. Mechanisms include training, peer (worker-to-worker) security assistance and vigilance, employee performance appraisals, awards programs, disciplinary actions, and analyzing behavioral precursors such as perceptions and reinforcing antecedents.

Additionally, the term “culture” can be defined as "the way it is around here." It reflects the way institutional values are demonstrated. It is also at the heart of how security is implemented. An organization's culture clearly announces everyday to every worker whether security is a key value. It dictates how a worker will act and how they will be treated. As a result, it also dictates workplace behavior. To a large degree, it determines the number of security incidents and whether a security program will succeed or fail. To enhance LANL’s security culture, the entire workforce should frequently be reminded at all-hands meetings, training, etc., regardless their job assignment (nuclear-weapons designer or cafeteria-menu designer) of the vital national importance and sensitivity of the LANL's primary mission -- nuclear weapons technology. Moreover, frequent Labwide management walk-arounds send a clear message that management genuinely cares about their workers and about promoting proper security behavior.

7.2. Accountability and Consequences

All members of the workforce are held accountable by their line managers for meeting LANL’s security expectations. Accountability includes both the positive reinforcement of workers (including managers) who meet security expectations and the negative consequences, including disciplinary actions, for those who do not. Line managers are accountable for having effective processes in place to establish, implement, measure, and reinforce security expectations and to foster proper security behavior.

When an incident occurs that affects or potentially affects security, LANL evaluates the incident to understand the active errors (i.e., the action or inaction of the worker believed responsible for the incident) and the latent errors (i.e., contributors, often in the supervisory/management chain, that happen in advance of the incident and “set up” the worker action/inaction) that contributed to the incident. A logic model is applied to ascertain the relative contributions of the worker involved in the incident, their supervisor, and institutional or organizational factors (e.g., policies, procedures, and management systems).

Although rare, workers (including managers) sometimes willfully violate physical and/or administrative controls put in place to ensure security. The philosophy used in determining culpability is that workers generally take actions they believe are the “right” thing to do under the circumstances. The approach is to look to see if there were circumstances outside the control of the individual that “set up” the action

such that another person given the same situation would likely have acted in the same manner. If this is the case, "blame" is likely to be most appropriately placed somewhere in the management chain or with the institution itself. Cases where there is a management or institutional contributor are aggregated and further analyzed to determine whether the problem is isolated or systemic.

In cases where the worker is found to be "at fault," LANL uses progressive discipline to correct behaviors that are not consistent with LANL expectations. LANL's disciplinary policy is documented in the Administrative Manual as AM 112. Additionally, LANL has adopted a consequence matrix for poor security performance to guide appropriate disciplinary actions for all members of the workforce, including managers. This consequence matrix establishes accountability all the way up the security-responsible line-management chain and allows for adjustment of the consequence severity based on the degree of willfulness involved in the incident. The presence of systemic institutional security issues could result in disciplinary action being applied throughout the line-management chain, up to and including the LANL Director.

In cases where it is determined that an "honest mistake" was made or that a systemic institutional problem caused the action, necessary corrective actions are taken. Such corrective actions can range from advising the worker (including manager) to prevent a recurrence, to additional training, to completely reengineering a LANL process.

8.0. Security Resource Allocation

8.1. General

LANL program and line managers are responsible for planning work and for ensuring that expectations for performing work securely are incorporated into all work plans and addressed in resource prioritization and allocation. Security costs include not only administering the basic security program, but management time spent responding to security incidents and legal actions that can arise when security expectations are not met. There is clear benefit in doing things responsibly each and every time. By meeting security requirements, LANL can avoid security incidents and the associated high cost (financial and political) of responding to them.

Since FY01, NNSA security activities are separately identified and funded as a direct mission program. Accordingly, the "FS" series of budget and reporting (B&R) is used to record all security program activities beginning October 1, 2000. As with all other DOE programs, direct funding provided for security activities during a fiscal year represents a firm limitation to fund programs at a specified level. As such, security program costs are constrained to the amount of direct funding provided. Any unforeseen funding requirements identified during the fiscal year that cannot be accommodated within the security funding provided are addressed through normal processes and procedures. LANL works with its cognizant NNSA Field Office and cognizant Lead Program Secretarial Officer (LPSO) to manage, review, and prioritize all security activities. When new security requirements emerge, the LPSO provides guidance as to the proper priorities and in finding lower priority security activities to offset the cost of emerging higher priority activities.

ISSM is owned by the institution—not a single central organization. This distributed ownership necessitates that people in support and operating organizations perform security-related work at the request of the institution. Questions then arise about payment for this work. The answer is based on ISSM's fundamental tenet that security is part of everyone's job and of all work performed at LANL. In this spirit, the following outlines expectations regarding organizational charges for institutional security work:

1. When a requirement for an institutional ISSM-related activity is approved by the LANL Director's Office, the cost associated with the implementation of this requirement will be borne by the individual divisions or groups and charged to the appropriate program code. Examples of such requirements include serving on focus teams for the creation of security LIRs.

2. If LANL requires the services of staff to work on unique or extraordinary projects that are clearly institutional in nature and do not fall within individual division or group security responsibilities, the institution will provide funds. In most situations, however, staff required to develop requirements that will ultimately be deployed in LANL should be charged to their individual divisions or groups.

3. Divisions or groups that foresee requiring the services of other organizations should contact those organizations so they can budget and rank these requests for services in the annual planning process.

8.2. Deployed Personnel

The changing programmatic environment requires flexible customer-driven deployment of security staffing, including protective force services, to support activity- and facility-specific security functions in the field. Effective integration of security into work requires all program and line managers to plan explicitly for security in their annual budget cycle and for on-going resource management, including prioritization. Security resource planning and allocations by program and line management are based upon systematic needs analysis performed jointly with support organizations. Long-term planning of core institutional security functions and staffing is also essential due to the broad mix of security challenges at LANL.

8.3. Security Management Plan

LANL prepares and annually updates a security management plan. This plan identifies all funded and unfunded security activities for the current year and out years. Data is available by functional area, as well. This planning document, which is closely linked to the SSSP, covers projected tasks and their drivers, milestones, and the costs associated with managing risk and achieving security expectations. Maintaining the security management plan enhances LANL's ability to manage security risks and achieve security expectations in an operationally efficient and cost-effective manner.

BIBLIOGRAPHY

Selected documents that provide the basis for the ISSM system being implemented at LANL:

1. "Safeguards and Security Management Improvements Initiative," in Appendix O of the UC-DOE Contract No. W-7405-ENG-36, Modification No. M507, January 18, 2001.

2. "Implementation of Integrated Safeguards and Security Management for the National Nuclear Security Administration (NNSA)," General John A. Gordon, NNSA Administrator, March 26, 2001.

3. "Integrated Safeguards and Security Management (ISSM) Policy," DOE Policy 470.1, May 8, 2001.

4. "LANL ISSM Communications Plan," Los Alamos National Laboratory, April 12, 2001.

5. "Integrated Safeguards and Security Management Laboratory Performance Requirement," LPR 406-00-00.0 (Draft), Los Alamos National Laboratory, April 30, 2001.

6. "ISSM website http://int.lanl.gov/orgs/s/issm," Los Alamos National Laboratory, since July 18, 2000.

7. "Integrated Safety Management," LA-UR-98-2837, Rev. 3.1, Los Alamos National Laboratory, April 24, 2000.

ISSM Workshop Guidance for Division-Level Directors

Guidance for Division-Level Directors

ACTION	RESOURCES
Hold All-Managers Meeting for division (before 8/4 if possible)	Guidance for Division-Level Directors, including slides & handouts
Hold All-Hands Meeting for division (Optional – if practical)	Guidance for Division-Level Directors, including slides & handouts
Ensure groups conduct group-level workshop. Ensure attendance is tracked and reported.	Guidance for Group-Level Managers Workshop attendance and reporting procedures
Collect reports from groups on questions, concerns & suggestions for improving security performance	Questions, Concerns & Suggestions Collection & Report Guidance
Respond to questions, concerns & suggestions	Questions, Concerns & Suggestions Collection & Report Guidance
Meet individually with all division managers to review security responsibilities. Agree on Security Performance Objectives for 2000/2001.	ISSM Individual Performance Objectives Worksheet

Division-Level Planning Session
Facilitation Guide for Division-Level Directors

Purpose:

Division-level directors will use this planning session to inspire commitment to enhanced security performance. Division-level directors will communicate his or her personal commitment to ISSM to their management team and clarify expectations for subsequent group-level workshops. The ultimate goal of ISSM is to achieve zero safeguards and security incidents.

Objectives:

1. Division-level directors will clarify expectations in regards to the implementation of ISSM within their respective divisions and offices.
2. Division-specific concerns regarding safeguards and security will be identified that can be discussed in greater detail in the group-level workshops.
3. Division-level directors will encourage the identification of ways to improve security performance within the division and will commit to addressing questions, concerns & suggestions that are identified and forwarded from the group-level workshops.

Division-Level Planning Session (cont.)
Facilitation Guide for Division-Level Directors

Session Preparation:

1. Schedule the planning session in a room large enough to accommodate all division managers. Recommend a 60 to 90-minute meeting.
2. Invite the ALD/DLD that you report to.
3. Require all managers in the division to participate. Encourage them to send a representative only if they cannot personally attend.
4. Invite the security support staff that are affiliated with your division (e.g., OSSOs, OCSRs, CDCs). Encourage the security support staff to attend and participate in the group-level workshops as well to enhance their visibility in the division and to assist in answering questions and concerns that may come up during these workshops.
5. Visit the ISSM workshops Web site to download copies of the materials you will need for the workshop or print this PDF. Look for "ISSM Workshop Guidance for Division-Level Directors." This will include the following:
   - A set of viewgraphs you can use.
   - The procedure group-level managers should follow to determine who needs to attend the group meetings and to track and report attendance.
   - The procedure and tools associated with collecting questions, concerns, & suggestions during the group workshops.
   - A collection of handouts that every manager attending the workshop should receive.

Division-Level Planning Session (cont.)
Facilitation Guide for Division-Level Directors

Session Preparation: (cont.)

6. Preview the recommended slides for this planning session. Customize the presentation to address questions or concerns that may be specific to your division. If you have any questions about the slides or what else to include in your presentation, contact the Security Help Desk at 5-2002 or secure@lanl.gov.
   - If your division handles classified assets routinely, remind managers that discussion of potential security vulnerabilities is classified, and that workshops will have to be conducted with appropriately cleared workers and in appropriate areas.
7. Review the recommended procedures for tracking and reporting attendance at subsequent group-level workshops and for reporting on these sessions. (ISSM workshops Web site, click on “Logistics.”) You should be able to discuss these procedures and clearly communicate your expectation that these procedures be used before and after the workshops.

Division-Level Planning Session (cont.)
Facilitation Guide for Division-Level Directors

Session Preparation: (cont.)

8. If it is practical, you may want to consider having an all-hands meeting following the meeting with your managers. This will not replace the group-level workshops (which need to be more interactive) but will provide you the opportunity to directly communicate your commitment to enhancing our security performance and your expectation for participation in the group-level workshops.

Division-Level Planning Session (cont.)
Facilitation Guide for Division-Level Directors

Planning Session:

Opening & Introductions:

- IMPORTANT NOTE: Ensure all in attendance have the appropriate clearance and “need-to-know” for expected discussion.
- Introduce any guests that may be attending: ALD/DLD, division Safeguards and Security support staff. (All division managers should know who their security resources are.)
- State the purpose of this effort. Describe your personal commitment to ISSM. Explain why this is a critical topic and practice for the Laboratory at this time.

Division-Level Planning Session (cont.)
Facilitation Guide for Division-Level Directors

Planning Session: (cont.)

Setting the Context:

- Using the recommended slides provided as well as any additional points you want to make, provide a broader context for the need to review our security responsibilities at this time. Use the slides to describe ISSM and how it parallels ISM. Review the 5-step process and how it applies to work in the division.
- Use the slides to highlight John Browne's commitment to and expectations in regards to safeguards and security. Emphasize the "zero safeguards and security incidents" goal.
- Explain the relevance of ISSM for your division. (Anticipate and answer the question that may be on some of your managers' minds: "Why should I care about this? We didn't/don't have a problem with this.")

Division-Level Planning Session (cont.)
Facilitation Guide for Division-Level Directors

Planning Session: (cont.)

Sharing Your Expectations:

- If managers missed John Browne's all-hands meeting, they should watch the video of the session ASAP, available via LabNet or on the Web.
- All group-level managers are expected to conduct an all-hands workshop for everyone in the group. These should be completed by August 31. Attendance at the group-level workshops is mandatory and must be tracked and reported.
- Managers must identify participants on-line via links on the ISSM workshops Web site. Click on "Logistics." This should be done ASAP and BEFORE group workshops.
- Managers/group offices will also record attendance directly, also via links on the ISSM workshops Web site.
- Managers will be responsible for following up with all those who should attend the workshops but are absent. Large groups may consider multiple workshops (e.g., Team or project-level) to accommodate all group members. Smaller groups may elect to follow up with staff individually.

Division-Level Planning Session (cont.)
Facilitation Guide for Division-Level Directors

Planning Session: (cont.)

- Managers should be encouraged to be familiar with and use the resources posted on the ISSM workshops web site for the group-level workshops. These include recommended slides for content and a facilitation guide for the interactive portion of the workshops. Managers will also have the option of requesting a facilitator to assist with the group-level workshops.
- The group-level workshops should focus on safeguards and security issues that are specific to the group. Group staff will be encouraged to ask questions, identify concerns and make specific suggestions for improving security practice and performance within the group. All of these should be captured using the recommended procedure in the workshop materials posted on the ISSM workshops Web site. Group-level managers should be encouraged to address many of these questions, concerns or suggestions at the group level during the workshop. Questions, concerns & suggestions that should be addressed division- or Laboratory-wide should be included in a report to the division office. A template for this report is included with the other workshop tools already described.

Division-Level Planning Session (cont.)
Facilitation Guide for Division-Level Directors

Planning Session: (cont.)

- Reminder: If your division handles classified assets routinely, remind managers that discussion of potential security vulnerabilities is classified, and that workshops must be conducted with appropriately cleared workers and in appropriate areas. If groups have both cleared and uncleared staff, separate workshops should be considered.
- Tell them you will review all questions, concerns & suggestions that come from these workshops. You will take action on any you can directly and refer others to the appropriate person or office. We will communicate back to the groups about what action we take.
- Ask them to let you know when their group workshops are scheduled. Tell them you will try to attend as many of their workshops as possible.
- Invite your division security officers (e.g., OSSOs, OCSRs, CDCs) to attend group-level workshops. They will be able to answer some of the questions that may come up.
- Let managers know that some participants in the group-level workshops may be contacted to participate in an evaluation of this training effort at its conclusion.

Division-Level Planning Session (cont.)
Facilitation Guide for Division-Level Directors

Planning Session: (cont.)

Discussion:

- Ask: In addition to some of the specific issues or areas of concern regarding safeguards and security that I have already identified, what other areas should we specifically address during the group-level workshops?
  - Capture and discuss how best to handle these.
- Ask: What questions, concerns or suggestions do you have regarding safeguards and security practice within the divison?
  - Capture. Address as many questions, concerns or suggestions as you can directly and immediately. Commit to following through on any that must be referred. Report on status of follow-through at subsequent managers meetings.
- Ask: What questions do you have regarding what you need to do to prepare for and conduct the subsequent workshops in your groups?

Division-Level Planning Session (cont.)
Facilitation Guide for Division-Level Directors

Planning Session: (cont.)

Wrap-Up:

- Thank managers for attending, participating, and committing to ISSM.
- Refer managers to the ISSM Web site, where they can find the tools and resources needed for the group-level meetings.
- Encourage managers to ask for help and direct any questions about this effort to you or your designee (possibly your deputy, chief of staff, OSSO, or designated training generalist).

Division-Level Planning Session (cont.)
Facilitation Guide for Division-Level Directors

After the Planning Session:

- Follow up with any managers who missed the meeting, either directly or through your designee. All managers should be briefed on the expectations and procedures for the mandatory group-level workshops.
- Attend as many of the group-level workshops as you (and your division-office staff) can attend.
- Monitor completion of the group-level workshops. (The designated training generalist in your division can pull a report from EDS on the percentage who completed the group-level workshops in the division.)
- Have a one-on-one meeting with each manager after the workshop to review security responsibilities. (This could be done at the same time you discuss overall individual performance objectives for 2000-2001.)
- Read and act on the reports from the group-level workshops. Communicate back to the groups what action you have taken or expect to take, what questions, concerns & suggestions you have referred, and how you plan to track responses to anything you referred. You should make every attempt to respond to each group report within 30 days.

Division-Level Planning Session (cont.)
Facilitation Guide for Division-Level Directors

After the Workshop:

- By September 15, submit a report to your respective ALD or DLD (with a copy to the Security Help Desk) that summarizes the results of the group-level workshops. (See the procedures for "Questions, Concerns, and Suggestions Collecting and Reporting" included with this facilitation guide, also available on the ISSM Workshops Web site under "Templates").

Case Studies

Case Studies:
Scenarios Based on Actual Incidents

Directions

Select case studies that are relevant to the work in your group, and continue the discussion on application of the ISSM 5-step process.

Lab-Wide Security Issues

- Vu-Graph Classification
- Badges
- Suspicious Packages
- Passwords
- Faxing
- Foreign Visits
- Theft
- Sensitive Unclassified
- “Unclassified” Processing
- “Unclassified” Presentation
- TSCM

Area Access

- SNM Material Access Area (MAA)
- Foreign Visits & Assignments

Case Studies:
Scenarios Based on Actual Incidents (cont.)

Classified Information

- Accountable Classified
- Misplaced Classified
- Copying Classified Information
- Classified Data Transfer
- Classification
- Shredding Materials
- E-mail
- Excess Material
- Classified Faxing
- Security Containers

Case Studies:
Scenarios Based on Actual Incidents (cont.)

Lab-Wide Security Issues

Vu-Graph Classification:

Scenario: Derivative Classifer Review

Circumstances: You create a view graph and have your derivative classifier review the content. It is not classified. Several days later you make a few modifications and ask your uncleared administrator to put the content into Power Point with a lead and closure slide as well. Someone sees the presentation and declares that it is classified. Your derivative classifier agrees. The changes you made were enough to change the classification.

Badges:

Scenario: Wearing Badge in Public Places

Circumstances: You see a fellow LANL employee in a bank in town with her badge clipped to her collar. She has the yellow PSAP appliance / clip showing as well.

Case Studies:
Scenarios Based on Actual Incidents (cont.)

Lab-Wide Security Issues (cont.)

Suspicious Packages:
Scenario: Suspect Briefcase or Package Unattended in Your Office
Circumstances: You see a package in the hallway just outside your office door. There is no tag or identification on the package.

Passwords:
Scenario: Shared Password.
Circumstances: Fred is on vacation, and he has been working on a document from which you need some information for the boss. You mention your frustration to a coworker and she says "I can get that for you. I know Fred's password."

Faxing:
Scenario: Fax Error
Circumstances: You have just faxed a six-page document on an unclassified Fax machine and the completion report indicates there were seven pages. As you look through the document you find a page in the middle marked Secret.

Case Studies:
Scenarios Based on Actual Incidents (cont.)

Lab-Wide Security Issues (cont.)

Foreign Visits:
Scenario: Foreign Visit Rules
Circumstances: You are the host for a foreign visitor who will arrive tomorrow. You receive a priority letter and an e-mail stating that the original visitor, Bill, will not be coming, and James will now be coming in his place.

Theft:
Scenario: Possible Theft of Government Property
Circumstances: You are a team leader, and one of your employees advises you that a fellow team member has been leaving work each evening with briefcase in one hand and a box in the other arm.

Sensitive Unclassified:
Scenario: Protection of Sensitive / Unclassified Information
Circumstances: During closure and lock-up of your building, you discover a list of employees in the recycle bin. The list includes Z numbers and other numbers in a column marked “performance rating.”

Case Studies:
Scenarios Based on Actual Incidents (cont.)

Lab-Wide Security Issues (cont.)

Sensitive Unclassified # 2:

Scenario: Protection of Sensitive / Unclassified Information

Circumstances: As you are making copies, you see the division budget and a list of mission impact statements in the trash can beside the copier. Some of these impacts involve reduction in the number of employees and inability to properly secure materials.

Unclassified Processing

Scenario: Processing Classified on Unclassified Computer

Circumstances: You are processing data on your unclassified computer. After saving your work, you notice that you typed classified information on your unclassified system.

Case Studies:
Scenarios Based on Actual Incidents (cont.)

Lab-Wide Security Issues (cont.)

Unclassified Presentation

Scenario: Presentation Turns Classified

Circumstances: You are attending a presentation and the slides being presented are unclassified. However, during the presentation the presenter verbally presents material you know is classified.

TSCM

Scenario: Cell Phones in Security Areas

Circumstances: After entering a security area, you notice that you have your personal cell phone with you.

Case Studies:
Scenarios Based on Actual Incidents (cont.)

Area Access

SNM Material Access Area (MAA):
Scenario: Improper Access
Circumstances: You and a coworker enter an area which requires a minimum of two people entering the area together for access to that area. You discover a worker working alone in the area.

Foreign Visits:
Scenario: Foreign Visit Escort
Circumstances: You are the host for a group of seven foreign visitors. You are giving a tour in a security area, and you and another escort discover one of the guests has wandered away from the tour.

Foreign Visits & Assignments:
Scenario: Foreign Visit Escort
Circumstances: You are working in a security area and you encounter a visitor with a red badge who should be under escort. You know this, as it was just announced on the loudspeaker. The visitor is walking around without an escort.

Case Studies:
Scenarios Based on Actual Incidents (cont.)

Classified Information

Accountable Classified:

Scenario: Control of Accountable Classified Material

Circumstances: Alice passes an accountable classified document which is stored in her safe to Bill, and after using it, Bill stores the document in his safe. Later the classified document custodian (CDC) performs an inventory, and the document is not found in Alice's safe.

Misplaced Classified:

Scenario: Control and Location of Classified Material

Circumstances: You open your safe to look for a document you created. You can't find it. You remember that you think you may have given it to Joe to critique for you. Or was it Larry? Joe says, "I remember it. I made comments on it, but gave it back to you last month." Larry is on vacation.

Case Studies:
Scenarios Based on Actual Incidents (cont.)

Classified Information (cont.)

White-Board Copier:

Scenario: Copier, White Board.

Circumstances: You have a classified drawing of a security component for a new building design and you are presenting the drawing to a group of workers and are using a white board in a limited-area conference room. As you draw the design on the white-board (which is capable of making copies) and make a copy for each participant, you recall that you have done this before and have seen others do the same. You realize the white-board copier has not been certified for classified copying.

Xeroxing Classified Documents

Scenario: Classified Document Found on Copier.

Circumstances: A classified document is found on the copying machine. What responsibility does the person have if 1) he knows who owns the document and returns it to the person, 2) he knows the group that owns the document and returns it to the group office, or 3) he does not know the owner of the document?

Case Studies:
Scenarios Based on Actual Incidents (cont.)

Classified Information (cont.)

Xeroxing Classified Documents:

Scenario: Classified Document Lost in Jammed Copier.

Circumstances: You are copying classified material on an approved copier in a secure area. The copier jams. You remove what you think is the jam, but the copier still will not function. What should you do? Subsequently, another individual finds material that is marked classified jammed in the copier.

Classified Data Transfer:

Scenario: Data Transfer between Different Forms of Media

Circumstances: You are working late and are just about to leave for an appointment. You are in fact a bit late. Coworker Bill, the only other employee in the building, asks you to observe as he transfers classified data from his hard drive to his A:/ drive. You explain you can't but will help first thing in the morning. When you come in the next day you offer to help but Bill says "It's O.K. I did it last night."

Case Studies:
Scenarios Based on Actual Incidents (cont.)

Derivative Classifier

Classification:

Scenario: Classification of a Document

Circumstances: You have just completed a memo for your counterpart at DOE, and you are not sure if the document is classified. You think it might be. Your group has two authorized derivative classifiers (ADCs) but one is on vacation and the other is on travel.

Shredding Materials:

Scenario: Destruction of Sensitive or Classified Materials by Shredding

Circumstances: You are a team leader, and the building custodian comes to you with a bag of shredded paper he was taking to the dumpster. You can see that he has discovered a partially shredded document with complete classified paragraphs still legible.

Case Studies:
Scenarios Based on Actual Incidents (cont.)

Derivative Classifier (cont.)

E-Mail:
Scenario: E-Mail Error
Circumstances: You have just received an e-mail from a co-worker who is on travel in Washington, DC . As you read the e-mail, you discover that it contains classified material.

E-Mail:
Scenario: E-Mail Error
Circumstances: A staff member is collaborating with a colleague from the United Kingdom Atomic Weapons Establishment. The colleague sends e-mail that he/she believes is unclassified, but you know it to be classified by DOE standards. What do you do?

Excess Material:
Scenario: Excess Classified Material
Circumstances: You are assigned to a position of a coworker who has retired, and you inherit her office and safe. You discover "volumes" of marked and unmarked documents, all of which you believe to be classified. Much of the material is 12-14 years old.

Case Studies:
Scenarios Based on Actual Incidents (cont.)

Derivative Classifier (cont.)

Classified Faxing:

Scenario: Fax Error

Circumstances: You have just received a Fax document on an unclassified Fax machine. As you read the document, you know that it contains classified material.

Security Containers:

Scenario: Security Container Left Open.

Circumstances: As you are working late one evening, you see a two-drawer safe in an open office down the hall from your office. It is in a limited area, and it is 6:30 p.m. The safe has a "LOCKED" sign on it, but the lower drawer is open about 3 inches.

Case Studies:
Scenarios Based on Actual Incidents (cont.)

Derivative Classifier (cont.)

Security Containers:

Scenario: Security Container Check.

Circumstances: A safe checker spins the dial on a “locked” safe but fails to pull the drawers. Subsequently, a security guard pulls on the drawer, and it opens. It is discovered that the safe has had a mechanical failure. Can the owner of the safe get a security infraction? Can the safe checker receive a security infraction? What if there is no written procedure for safe checking?

Printable PDF of This Document

Opening the Printable PDF

If you would like to print this document in compact format, just click on the button below. Once you have that file open, you can print it for a hard copy.

OPEN THE PRINTABLE PDF DOCUMENT

Workshop Handouts and Worksheets

- ISSM 5-Step Process
- Sample Applications of the 5-Step Process
- Enhancing Our Security Awareness: Behaviors Can Lead to Incidents
- Resources Quick Reference List
- Report Guidance for Division-Level Directors
- Report Guidance for Group-Level Managers
- ISSM Individual Performance Objectives Worksheet

Printable PDF of This Document

Opening the Printable PDF

If you would like to print this document in compact format, just click on the button below. Once you have that file open, you can print it for a hard copy.

OPEN THE PRINTABLE PDF DOCUMENT

The 5-Step Process

The 5-Steps	Questions to ask yourself at the start of each day…
1. Define Scope of Work ➢ Translate mission into work ➢ Set expectations (e.g., goals and objectives) ➢ Identify and prioritize tasks ➢ Allocate resources	What outcome is expected of me today? Who is helping me? Do others need to know what I'm doing? Do I have the appropriate equipment? Am I authorized to do the work? Am I comfortable proceeding? Should I stop work?
2. Analyze Security Vulnerabilities ➢ Identify and analyze the security vulnerabilities associated with performing specific work	What are the vulnerabilities? Have they changed? Are they adequately controlled? How can my work be compromised? What can go wrong? What has gone wrong before? Should I stop work?
3 Develop and Implement Security Controls ➢ Identify appropriate standards and requirements ➢ Develop/implement cost-effective security controls to prevent or mitigate the work-associated vulnerabilities	What are the governing requirements? Is there an "activity security plan"? Are special approvals needed? Is special training/authorization required? Is special equipment required? Prohibited? Do I understand the controls? Am I comfortable with them? Are the controls realistic? Will they get implemented? Should I stop work?
4 Perform the Work Work within Controls ➢ Confirm readiness ➢ Perform work securely within established security controls	Is everything the same today as it was yesterday? Is all equipment working/authorized? Do I know enough to perform the work securely? Am I feeling rushed or pressured to do this job? Do I need help? Should I stop work?
5 Ensure Performance ➢ Collect feedback information on the adequacy of security controls ➢ Identify and implement opportunities for improving the definition, planning, and execution of work ➢ Conduct line and independent assessments ➢ Reinforce expected behaviors	Did the experiment "work?" Did we identify problems and correct them? Are process changes needed? Are secure/better methods possible? Were responsibilities clear? Do I ever want to do this again? What will I do differently next time?

Sample Applications of the ISSM 5-Step Process

Shown below are two applications of the ISSM 5-step process to two entirely different work activities within the Laboratory. The first work activity is performed by every employee – i.e., engaging in performance evaluation with one's supervisor. This activity involves unclassified, but sensitive information. The second work activity is performed by a large percentage of employees at the Laboratory – i.e., establishing a stand-alone classified computing system. This activity involves classified information. In all cases, the ISSM 5-step process begins with defining the scope of work, and then identifying and analyzing the associated security vulnerabilities, developing and implementing security controls, performing the work, and finally evaluating and improving performance. A given control may not fully mitigate an analyzed vulnerability, but combination with others may. Though these two sample applications may not be exhaustive in terms of identifying and controlling vulnerabilities, they nevertheless illustrate how each of the 5 steps should be viewed and executed to help ensure that all Laboratory work is performed securely.

Application #1: Employee Performance Evaluation

1. Define Scope of Work: engage in performance evaluation with supervisor

<u>translate into work activities</u>
1) employee prepares accomplishments/results for supervisor
2) employee meets with supervisor
3) supervisor writes performance summary, ORC score
4) employee reviews online performance summary

<u>set expectations</u>
1) this material is treated as sensitive, unclassified material
2) the new on-line web-based system is used

<u>prioritize tasks</u>
1) various deadlines apply to the process

2. Identify and Analyze Vulnerabilities

<u>identify vulnerabilities</u>
1) inadvertent inclusion/disclosure of classified information
2) inadvertent disclosure of sensitive, unclassified information
3) loss of information from system malfunctions

<u>analyze vulnerabilities</u>
1) disclosure caused by multiple users of processing computer
2) transmission of sensitive, unclassified information over non-sensitive networks (e.g., working from home)
3) persons with classified assignments mistakenly include classified information in their accomplishments/results summaries
4) computer files or hardcopy left laying uncontrolled
5) various computer malfunctions cause data loss

3. Develop and Implement Controls

identify standards and requirements
1) consult HR guidance on handling of performance appraisals
2) consult LANL computer security requirements for processing of sensitive, unclassified information

develop controls to prevent or mitigate vulnerabilities
1) employees prepare write-ups in private, at work, on computer prepared for handling sensitive, unclassified information (1,2)
2) use individual's personal computers with access control, or common computers with separate account access controls, or use separate media and individual backups (1,5)
3) employees save information on removable media or hardcopy which are reasonably secured against unauthorized access (1,4,5)
4) employees conducting classified work review sections of write-up with an ADC (3)
5) use of encryption on files (1,2) [may not be a practical control at this time]
6) use of smart card required for system access (1)
7) use of online access control protocols to limit read access to employee's direct line supervisors (1)
8) mark hardcopy and removable media appropriately (1,4)
9) identify resources and experts capable of providing useful information about or help during the process (all)

*Note: parenthetical notes refer to the analyzed vulnerabilities addressed in 2. above

4. Perform Work

1) use the selected/required controls while performing the work
2) confirm readiness to engage in the work (e.g., controls are operative, time is available, needed resources/tools are available)

5. Ensure Performance

collect feedback/identify improvement opportunities/make changes
1) gather and act on suggestions and lessons learned for improving the process

oversight & enforcement/reinforcement & accountability
1) engage your OCSR on issues or concerns about sensitive, unclassified computing
2) managers engage in self assessments (walkarounds) of the process in action
3) compare process with any applicable security plans

Application #2: Classified Computing System

1. Define Scope of Work: establish a stand-alone classified computing system

translate into work activities
1) determine level and category of information to be processed
2) determine needed system parameters (speed, memory capacity, peripherals and their connectivity, external communications needs, ...)
3) determine location for system
4) determine how data will be transferred in/out of system
5) procure hardware
6) procure software
7) prepare appropriate documentation for accreditation
8) obtain required reviews

set expectations
1) system will conform with requirements of LANL Master AIS Security Plan for Single-User Systems Processing Classified Data

prioritize tasks
1) review Master AIS Security Plan
2) establish hardware/software in selected work area
3) review with S-5 for accreditation approval process
4) introduce classified materials into system

2. Identify and Analyze Vulnerabilities

identify vulnerabilities
1) loss of control or compromise of classified information
2) loss of classified information to system failure

analyze vulnerabilities
1) unauthorized access to information or work area
2) tempest-based disclosure of information
3) insider threat
4) inadvertent access to information or work area
5) failure of various system components

3. Develop and Implement Controls

identify standards and requirements
1) consult LANL Master AIS Security Plan for Single-User Systems Processing Classified Data http://int.lanl.gov/orgs/s/s5/docs/entire_SUC_master_plan.pdf
2) consult LANL Computer Security Handbook http://int.lanl.gov/orgs/s/s5/handbook.shtml
3) consult with TSCM experts
4) consult LANL vault/vault type room and secured repository (safe) requirements

develop controls to prevent or mitigate vulnerabilities
1) incorporate LANL-approved physical barriers to work area (including tempest restrictions), with restrictive access controls (1,3,4)
2) position monitor display so as not to be visible from doors, windows, or other openings into work area (1,2,4)
3) employ encryption technology (1,2,3,4)
4) fix position of cable runs to eliminate significant cross talk (2)
5) work with OCSR to ensure correct installation (1,2,4,5)
6) limit access to personnel with a need-to-know and who have proper clearances (1,3,4)
7) develop SOP for classified system operation (all)
8) review setup with S-5 (1,2,4)

*Note: parenthetical notes refer to the analyzed vulnerabilities addressed in 2. above

4. Perform Work

1) use the selected/required controls while performing the work
2) confirm readiness to engage in the work (e.g., controls are operative, time is available, needed resources/tools are available)

5. Ensure Performance

collect feedback/identify improvement opportunities/make changes
1) gather and act on suggestions and lessons learned for improving the work area, system, or security plan

oversight & enforcement/reinforcement & accountability
1) engage your OCSR on issues or concerns about classified computing
2) managers engage in self assessments (walkarounds) of the work area with owner, users and security personnel
3) owner, users and security personnel compare work are and system with the security plan

Use the back button (◀◀) from the main menu bar at the top of the page to get back to your previous page.

Integrated Safeguards & Security Management

"Behaviors Can Lead To Incidents"

Property: Theft, Protection, Usage, Disposal, Loss, Fraud, Accountability

_ When on travel don't leave lap-top-computers, pagers and cell phones unattended or unlocked.
_ As you leave your office put valuables in the proper storage place and lock doors.
_ Tempted to take that worn and "already replaced" item home rather than turning it in to your property representative? Bad Choice.

Facilities: Access, Protection, Usage, Badges, Visitors, Securing

_ As a group of "strangers" walk unescorted through your workplace, engage or challenge them to determine: their need to be there and how you might help them find their destination.
_ If you are only "pretty sure" you locked the building as the last one out, it will be worth your time and peace of mind to go back and check. You may need a better "lock up system".
_ When at the bank, store, or Dentist's office, your badge should NOT be hanging around your neck. The badge is for Lab business on Lab property. Otherwise stow it, don't show it!

Information: Classification, Document, Vu-Graf, Speech, Media, Passwords

_ Review the documents on your desk before you leave. Different documentation and information require different protection. If you are not sure, find out, before you risk compromise.
_ Use your Authorized Derivative Classifier (ADC) on a regular basis. Develop rapport. Build in the review time. Use S-7 for emergencies or to resolve classification issues.
_ Determine "what" you are working with, who is the audience, and "where" you are going with the project before you choose the media and release the product. Sensitive? Classified?

_ **Communication:** Telephone, Cell phone, FAX, E-Mail, Mail, Voice, STU-III
_ If you receive a communication, which looks as though it may be classified, but is not marked as such, report the situation and determine the appropriate actions.
_ Private cell phones for private, non-LANL matters should not come to work, behind the fence. LANL cell phones have rules associated with them and a LANL cell phone user must know and follow these rules.

_ **People:** Clearance, Access, Need-To-Know, Escort, Behavior
_ Before the briefing starts and the classified matter is discussed, ensure the audience has both clearance and need to know for the topics to be discussed.
_ Escorting guests through your work area requires your undivided attention. It is NOT appropriate to excuse yourself from the guest for a few minutes and leave the uncleared guest alone in your office to have a short conference in your boss's office. It's not polite either!

Procedures and Policy: Know, Understand, Follow, Uphold, Improve

_ You can't work as quickly with some new policies and procedures, but to ignore them and proceed in the old mode may create a vulnerability for you and the Laboratory.
_ If you have an idea that might help to meet the intent of a security rule and would save time, and money, present it to management. But under no circumstance should you ignore the rule.
_ When on travel don't leave lap-top-computers, pagers and cell phones unattended or unlocked.
_ As you leave your office put valuables in the proper storage place and lock doors.
_ Tempted to take that worn and "already replaced" item home rather than turning it in to your property representative? Bad Choice.

Facilities: Access, Protection, Usage, Badges, Visitors, Securing

_ As a group of "strangers" walk unescorted through your workplace, engage or challenge them to determine: their need to be there and how you might help them find their destination.

_ If you are only "pretty sure" you locked the building as the last one out, it will be worth your time and peace of mind to go back and check. You may need a better "lock up system".

_ When at the bank, store, or Dentist's office, your badge should NOT be hanging around your neck. The badge is for Lab business on Lab property. Otherwise stow it, don't show it!

Information: Classification, Document, Vu-Graf, Speech, Media, Passwords

_ Review the documents on your desk before you leave. Different documentation and information require different protection. If you are not sure, find out, before you risk compromise.

_ Use your Authorized Derivative Classifier (ADC) on a regular basis. Develop rapport. Build in the review time. Use S-7 for emergencies or to resolve classification issues.

_ Determine "what" you are working with, who is the audience, and "where" you are going with the project before you choose the media and release the product. Sensitive? Classified?

Communication: Telephone, Cell phone, FAX, E-Mail, Mail, Voice, STU-III

_ If you receive a communication, which looks as though it may be classified, but is not marked as such, report the situation and determine the appropriate actions.

_ Private cell phones for private, non-LANL matters should not come to work, behind the fence. LANL cell phones have rules associated with them and a LANL cell phone user must know and follow these rules.

People: Clearance, Access, Need-To-Know, Escort, Behavior

_ Before the briefing starts and the classified matter is discussed, ensure the audience has both clearance and need to know for the topics to be discussed.

_ Escorting guests through your work area requires your undivided attention. It is NOT appropriate to excuse yourself from the guest for a few minutes and leave the uncleared guest alone in your office to have a short conference in your boss's office. It's not polite either!

Procedures and Policy: Know, Understand, Follow, Uphold, Improve

_ You can't work as quickly with some new policies and procedures, but to ignore them and proceed in the old mode may create a vulnerability for you and the Laboratory.

_ If you have an idea that might help to meet the intent of a security rule and would save time, and money, present it to management. But under no circumstance should you ignore the rule.

Use the back button (◀◀) from the main menu bar at the top of the page to get back to your previous page.

Resources

Who to Call

Badge Office	7-6901
Classification	7-5011
Clearance Processing Team	7-7253
Counterintelligence	5-6090
Electronic Communications	5-1795
Emergency Management and Response	7-6211
Foreign Visitors and Assignments	5-1572
ISEC (Internal Security)	5-6090
Nuclear Materials	7-5886
PSAP (Personnel Security Assurance Program)	7-0869
PTLA (Protective Force)	7-4531
Security Help Desk	5-2002
(Ensure issues which are classified are communicated securely!)	
Security Plans	7-0558
Security Training	5-7844
(including questions about credit for security training)	

Useful Web Sites

ISSM Website	http://int.lanl.gov/orgs/s/issm/
Security and Safeguards Division	http://int.lanl.gov/orgs/s/
Classified Matter Protection and Control	http://int.lanl.gov/orgs/s/cmpc/
LANL Password Policy	http://network.lanl.gov/passwords/policy.shtml
Publishing at Los Alamos	http://int.lanl.gov/publishing/
S-5 Computer Security Handbook	http://int.lanl.gov/orgs/s/s5/handbook.shtml
Virtual Training Center	http://www.lanl.gov/labview/training/training.html

DOE Official Policies

DOE Security Regulations and Directives
http://www.cta.doe.gov/ssb2000/fsheets/fs17.html

Polygraphs
http://www.doe.gov/news/fedreg.htm

Reporting Close and Continuing Contact with Sensitive Country Foreign Nationals
http://www.cta.doe.gov/ssb2000/fsheets/fs29.html

Security Reporting Requirements
http://www.cta.doe.gov/ssb2000/fsheets/fs24.html

Sensitive Unclassified Information
http://www.cta.doe.gov/ssb2000/fsheets/fs04.html

“Zero Tolerance”—Secretarial Policy Statement
http://www.cta.doe.gov/ssb2000/fsheets/fs11.html

Security and Safeguards Division

S-1 Security Plans and Programs	7-0558
- Vulnerability Analysis	5-0471
- Nuclear Materials Upgrade Program	5-0473
- Strategic Planning	7-0558
S-2 Program Integration	7-7565
- Security Requirements and Guidance	
- Security Assessments	
- Physical Security	
- Organizational Security Support	
- Protective Force Oversight	
S-3 Security Systems	7-4801
- Access Control	
S-4 Material Control and Accountability	7-5886
S-5 Computer and Technical Security	5-1795
- Computer Security	5-1795
- Technical Surveillance Countermeasures	5-8799 or 5-8867
- Secure Faxes, MASS (Material Accountability and Safeguards System)	7-1607
- Cellular Phones, PTS (Protected Transmission System)	5-5599
S-6 Information and Personnel Security	5-6565
- Classified Matter Protection and Control	5-7467
- Security Awareness, Briefings	7-0077
- Badge Office	7-6901
- Clearance Processing Team	7-7253
- PSAP	7-0869 or 5-8500
S-7 Classification	
- Classification/Declassification Services	7-5011
- Publication Release	7-5013
S-8 Emergency Management and Response	7-6211
S-SPO Special Projects Office	5-3505
- Harassing phone calls/letters	
- Illegal substances on Lab property	
- Property protection	
- Threats/harassment	
- Vandalism	
- Protests/demonstrations	

Resource People in Your Organization

ADC Authorized Derivative Classifier
CDC Classified Document Custodian
OCSR Organizational Computer Security Representative
OSSO Organizational Safeguards and Security Officer

Your Contacts

ADC _____
CDC _____
OCSR _____
OSSO _____

Integrated Safeguards & Security Management

Questions, Concerns, Suggestions Collection & Reporting

General: The worker's voice in ISSM is critical to its success. The data we wish to capture during the initial ISSM rollout and beyond is that which our LANL workers offer to identify questions, concerns or suggestions they have on how to improve security at the Laboratroy. This might include current challenges, best practices, suggestions, and relevant input to the ISSM steering committee for the ISSM path forward. Harvesting the ideas and knowledge of our workforce will only help us to enhance our security performance.

Data Collection Opportunities: Worker ideas and experience will be discussed and collected at:

_ Laboratory All Hands Meeting
_ Division Directors Planning Sessions linking management efforts to Group Workshops.
_ Group or Team level Workshops
_ Individual efforts for those wishing to offer issues or concerns privately or anonymously

Data Collection Methods:

_ Laboratory Director's Open Meeting:
- Facilitators will capture worker comments and issues and forward to Security HELP Desk for analysis / action.
- Security HELP desk access will be encouraged (secure@lanl.gov or 5-2002 Anonymous at Mail Stop K-560)

_ Division Director's meetings linking Director's meeting to Group Workshops.
- Division staff will arrange for capture of ideas and summarize using Division Workshop Report Guide.
- Divisions are encouraged to forward the report after roll up with group reports to the Security HELP Desk for analysis / action. Division should also analyze and address any issue they can at the Division level.

_ Group or Team level Workshops
- Group staff will arrange for capture of ideas and summarize using Group Workshop Report Guide: The report guide covers the types of issues to be included. This report will be forwarded to division for roll-up into division report for division and Security HELP desk analysis / action.
- Individual concerns during these workshops or after the workshops for those wishing to offer issues privately or anonymously.
- Security HELP desk access is encouraged.(secure@lanl.gov or 5-2002, Mail Stop K-560 (Anonymously). NOTE: Ensure that questions that are classified are communicated securely.

Integrated Safeguards & Security Management

Enhancing our Security Performance - - ISSM
Division-level Management Report Guide

Complete this report after all groups in your Division have completed their workshops

Date: _____

Division: _____

Division Leader _____

1. To date, what percentage of workers in your division have completed this training?

2. When do you expect to be at 100% completion?

3. What were the most common questions and concerns raised during the group-level workshops?

4. Which questions, concerns or suggestions for improving security performance are you addressing at the Division level?

5. What are you doing to follow-up on questions, concerns or suggestions that were referred to you?

6. How do you plan to respond to the groups who referred questions, concerns or suggestions to the Division Office?

7. Which issues are you referring for further assistance (to your ALD or DLD)?

8. Which issues are being forwarded to the Security HELP Desk?

Send copies of this report to the ALD or DLD to which you report *and* to the Security HELP Desk (MS K560) by September 15, 2000.

Use the back button (◀◀) from the main menu bar at the top of the page to get back to your previous page.

Integrated Safeguards & Security Management

Questions, Concerns, Suggestions Collection & Reporting

General: The worker's voice in ISSM is critical to its success. The data we wish to capture during the initial ISSM rollout and beyond is that which our LANL workers offer to identify questions, concerns or suggestions they have on how to improve security at the Laboratroy. This might include current challenges, best practices, suggestions, and relevant input to the ISSM steering committee for the ISSM path forward. Harvesting the ideas and knowledge of our workforce will only help us to enhance our security performance.

Data Collection Opportunities: Worker ideas and experience will be discussed and collected at:

_ Laboratory All Hands Meeting
_ Division Directors Planning Sessions linking management efforts to Group Workshops.
_ Group or Team level Workshops
_ Individual efforts for those wishing to offer issues or concerns privately or anonymously

Data Collection Methods:

_ Laboratory Director's Open Meeting:
- Facilitators will capture worker comments and issues and forward to Security HELP Desk for analysis / action.
- Security HELP desk access will be encouraged (secure@lanl.gov or 5-2002 Anonymous at Mail Stop K-560)

_ Division Director's meetings linking Director's meeting to Group Workshops.
- Division staff will arrange for capture of ideas and summarize using Division Workshop Report Guide.
- Divisions are encouraged to forward the report after roll up with group reports to the Security HELP Desk for analysis / action. Division should also analyze and address any issue they can at the Division level.

_ Group or Team level Workshops
- Group staff will arrange for capture of ideas and summarize using Group Workshop Report Guide: The report guide covers the types of issues to be included. This report will be forwarded to division for roll-up into division report for division and Security HELP desk analysis / action.
- Individual concerns during these workshops or after the workshops for those wishing to offer issues privately or anonymously.
- Security HELP desk access is encouraged.(secure@lanl.gov or 5-2002, Mail Stop K-560 (Anonymously). NOTE: Ensure that questions that are classified are communicated securely.

Integrated Safeguards & Security Management

Enhancing our Security Performance - - ISSM
Group-level Management Report Guide

Complete this report when at least 80% of the group members you expected to attend the group-level workshops have completed the workshops or have been briefed individually.

Date: _____

Division: _____

Group: _____

Group Leader: _____

1. How many people in your group were expected to complete this workshop?

2. To date, how many of those have completed the workshop?

3. What are you doing to follow-up with those who have not yet completed the workshop?

4. What questions or concerns did your staff raise during the workshop?

5. What suggestions for improving security practices were made during the workshop?
   - Start with any that you have been able to implement within your group.
   - Include suggestions that could help other groups in your Division or Lab-wide.

6. What questions or concerns did you defer (could not be answered or addressed during the workshop)?

7. What will you do to follow-up on any questions, concerns or suggestions raised during the meeting that could not be resolved at that time?
   - Include how you plan to keep the group informed on how their questions, concerns or suggestions are addressed.

8. What suggestions for improving security do you need assistance with or additional resources to implement?

9. What further information about your group workshop would you like to share?

Send to your Division Office by August 31, 2000.

Use the back button (◀◀) from the main menu bar at the top of the page to get back to your previous page.

Integrated Safeguards & Security Management

ISSM Individual Performance Objectives Worksheet

Directions: Use the **ISSM Five Step Process to identify** roles, responsibilities, and performance objectives you might use in the future in your performance plan.

Based on workshop discussion, what security insights have you gained as applied to your work?

_____
_____
_____
_____
_____

How will you incorporate these insights into your daily work?

_____
_____
_____
_____
_____

What are your duties involving security? (Some concepts to help with the inventory: Badge? Property? Keys? Passwords? Security Container? Physical Security – Your Office, Building? Cell Phone? Sensitive Data? Classified Information? Visitors?)

_____
_____
_____
_____
_____

How would you best accomplish these duties and what are the performance objectives associated with these duties /tasks?

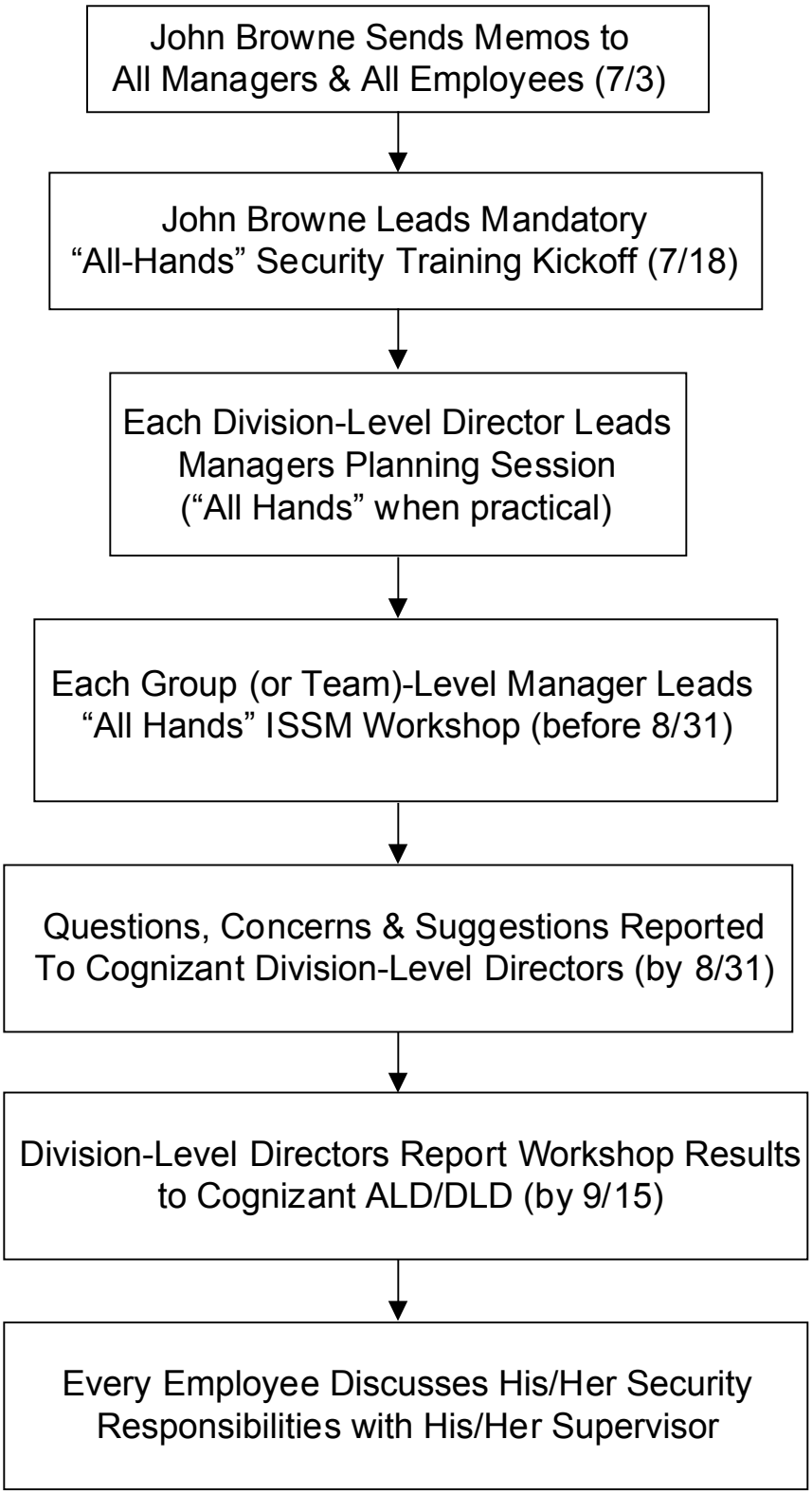
_____
_____
_____
_____
_____

By Applying the 5-Step Process, you will be able to answer the following questions:

1. Are your work and workplace secure?
2. How do you know?
   - Do you know the security requirements governing your work/workplace and how they are being met?
   - Do you know the security vulnerabilities in your work/workplace and whether controls are sufficient to mitigate them?

Enhancing Our Security
Awareness, Commitment & Performance

ISSM Rollout



Draft: 7/2000

ISSM Workshop Guidance for Group-Level Managers

Guidance for Group-Level Managers

ACTION	RESOURCES
Identify target audience for workshop attendance	See Logistics on ISSM Workshop Web site
Schedule and conduct group workshop	Guidance for Group-Level Managers, including slides, hand-outs, and case studies
Collect questions, concerns & suggestions for improving security performance	Questions, Concerns & Suggestions Collection & Report Guidance
Prepare summary report to division-level director on questions, concerns & suggestions regarding security performance in your group	Questions, Concerns & Suggestions Collection & Report Guidance

Guidance for Group-Level Managers (cont.)

ACTION	RESOURCES
Respond to questions, concerns & suggestions and refer unresolved concerns to division level	Questions, Concerns, & Suggestions Collection & Report Guidance
Ensure workshop completion has been documented.	See Logistics, attendance collection on ISSM Workshop Web site
Meet individually with all group staff to review security responsibilities. Agree on Security Performance Objectives for 2000/2001.	See Performance and Salary Management System Web site for guidance on Performance Planning ISSM Individual Performance Objectives Worksheet.

Group-Level Workshops
Facilitation Guide for Group-Level Managers

Purpose:

To provide an opportunity for those closest to the actual work of the group to review the importance of security to the mission of the Laboratory and to their work. To identify ways security performance could be improved within the group and personally by learning and applying the ISSM 5-step process.

Objectives:

1. Clarify the expectations of senior management in regards to good security practice and its importance to the mission of the Laboratory.
2. Introduce ISSM with tools to help staff apply the 5-step process to their work.
3. Provide an opportunity for all workers to discuss how to improve security practice individually, within the group and ultimately across the entire Laboratory. Group-level managers will commit to addressing questions, concerns & suggestions that are identified.

Group-Level Workshops (cont.)
Facilitation Guide for Group-Level Managers

Pre-Workshop Preparation:

1. If you did not have the opportunity to attend the mandatory all-hands meeting with John Browne, watch the video. (This will be aired daily on LabNet and will also be available on the Web. Visit the ISSM workshops Web site).
2. Attend the division managers meeting.
3. Visit the ISSM workshops Web site and click on "Logistics." Follow the directions to identify all group staff that should attend the group-level workshops. Print off a roster.
   - NOTE: Attendance at the group-level workshops is mandatory for all workers, including UC and contractors. Only those workers who are no longer in your group or who work only occasionally and are not currently physically present (e.g., staff on change of station or visiting professors) are exempt.

Group-Level workshops (cont.)
Facilitation Guide for Group-Level Managers

Pre-Workshop Preparation: (cont.)

4. Schedule an all-hands group workshop in a room large enough to accommodate the whole group. A session no less than 3-hours is recommended.
   - If your group is large, consider team or project-level workshops. The group-level manager should plan to attend all of these workshops.
   - If your group routinely handles classified assets and includes uncleared personnel, conduct separate workshops for cleared and uncleared staff if/when discussing potential security vulnerabilities.
5. Invite all group staff to the workshop. Communicate that the workshop is mandatory. Confirm date, time and location. If missed earlier, remind them to watch the video of John Browne's mandatory all-hands meeting, which provides important background information for the group-level workshop.
6. Also invite division management and security resources (e.g., OSSOs, OCSRs, CDCs) to your group workshop. They will be very helpful in answering questions and addressing concerns.

Group-Level Workshops (cont.)
Facilitation Guide for Group-Level Managers

Pre-Workshop Preparation: (cont.)

7. Preview the recommended slides and all the support materials provided. Tailor the presentation as necessary to address the specific security-related issues in your group. If you need assistance or have any questions about the materials or how to proceed with the workshop, contact the Security Help Desk at 5-2002 or send an e-mail message to secure@lanl.gov.
8. If you would like a trained facilitator to assist you with the workshop, contact the Ombuds Program Mediation Center at 7-9367 or marybeth@lanl.gov. If you don't use a facilitator from outside the group, be sure to enlist someone to help you record questions, concerns and suggestions during the workshop.
9. Review the recommended process and tools (included here under "Questions, Concerns, and Suggestions Collection and Reporting") for capturing questions, concerns & suggestions and reporting them to the division office.

Group-Level Workshops (cont.)
Facilitation Guide for Group-Level Managers

Workshop:

Opening and Introductions:

- IMPORTANT NOTE: Ensure all in attendance have the appropriate clearance for the expected discussion.
- Introduce any guests who may be attending: division office staff, security support staff or others.
- Remind participants to be sure to sign the roster!
- Using the slides provided, review the workshop agenda and objectives. Describe your personal commitment to ISSM. Explain why this is a critical topic and practice for the Laboratory at this time.

Setting the Context:

- Using the slides provided as well as any additional points you want to make, provide a broader context for the need to review our security responsibilities at this time. Use the slides to describe ISSM and how it parallels ISM. Present the ISSM 5-step process.
- Use the slides to highlight John Browne's commitment to and expectations in regards to safeguards and security. Emphasize the "zero safeguards and security incidents" goal.
- Explain the relevance of ISSM for your group. (Anticipate and answer the question that may be on some of their minds: "Why should I care about this? We didn't/don't have a problem with this.")

Group-Level Workshops (cont.)
Facilitation Guide for Group-Level Managers

Workshop: (cont.)

Sharing Your Expectations:

- ISSM, similar to ISM, describes the way we do work at the Laboratory. Security is everyone's responsibility.
- Everyone should be familiar with and use the 5-step process routinely to assess their work.
- Use the resources available to you. (Use "Resources" slide.) This includes the reference information on the handouts provided to you. Point out that resources include managers and the security support resources available in your group/ Division (refer to OSSOs, OCSRs, CDCs, et al. by name). If you don't know or aren't sure, always ask.
- Review the process that will be used to report the questions, concerns and suggestions that will be raised during the workshop to the division office. Division-level directors have been asked to respond within 30 days.

Group-Level Workshops (cont.)
Facilitation Guide for Group-Level Managers

Workshop: (cont.)

Sharing Your Expectations: (cont.)

- At the conclusion of this workshop, everyone will be asked to think about ways each of us can support the Laboratory's commitment to zero safeguards and security incidents. Tell them you will discuss this with each worker when you meet to develop individual performance objectives for 2000-2001.
- Let group members know that some of them will be contacted soon to participate in a random-sample survey to find out what they thought about this workshop. If they're contacted, encourage them to participate and to be candid.

Group-Level Workshops (cont.)
Facilitation Guide for Group-Level Managers

Workshop: (cont.)

Discussion:

- Start the discussion by using the handout "Sample Applications of the 5-Step Process". Work through one of the examples that is most relevant to the work in your group. Use the example to demonstrate how the 5-step process can be used to identify and mitigate vulnerabilities before they become incidents. Next, use the handout "Case Studies: Scenarios Based on Actual Incidents". Select one or two incidents to work through together (again, that are relevant to the group). Coach participants in applying the 5-step process to the case. How could they use the 5-step process to mitigate the potential vulnerability in each case?
- If the group is large, consider breaking into smaller groups with each one addressing one of the case studies provided and sharing their conclusions and recommendations with the larger group.
- Be sure to capture any questions, concerns or suggestions that are raised during this exercise and the subsequent discussion. (Appoint a recorder to do this).

Group-Level Workshops (cont.)
Facilitation Guide for Group-Level Managers

Workshop: (cont.)

Discussion: (cont.)

- Continue the exercise by encouraging the group to describe some security-related situations that are specific to the group. Again, coach the group in using the 5-step process to assess the situation. As questions or concerns are raised, model the use of expert resources, such as the OSSOs, OCSRs, and CDCs attending the workshop or refering questions to the Security Help Desk.
- When questions or concerns are raised, address any you can directly and definitively. (Still capture the question or concern. These will provide ideas for subsequent ISSM FAQs). Any questions and/or concerns that come up that can't be addressed definitively should be captured and referred to a division security representative or to the new Security Help Desk. Commit to sharing responses to these questions and/or concerns with all staff through email or at a subsequent group meeting, taking great care to avoid unauthorized disclosure of classified information.

Group-Level Workshops (cont.)
Facilitation Guide for Group-Level Managers

Workshop: (cont.)

- Ask: What questions, concerns or suggestions do you have regarding safeguards and security practice within the group?
  - Capture. Address as many as you can directly and immediately. Commit to following through on any that must be referred. Report on the status of follow-through at subsequent group meetings.
- Remind participants that they can also submit questions, concerns or suggestions anonymously, either by sending them to the mailstop listed on the resources page or by calling the Security Help Desk at 5-2002.
- Provide copies of the handouts to all participants. These will include the following:
  - A quick reference list that includes division security representatives.
  - Guidance for applying the 5-step process to their work.
  - The "Enhancing Our Security Awareness: Behaviors Can Lead to Incidents".
  - An ISSM Individual Performance Objectives Worksheet.

Group-Level Workshops (cont.)
Facilitation Guide for Group-Level Managers

Workshop: (cont.)

- Ask participants to turn to the handout labeled "Enhancing Our Security Awareness: Behaviors Can Lead to Incidents". Review some of the behaviors that are most applicable to the group. Note how heightened awareness of the importance of maintaining good security practice and using the 5-step process can help to mitigate the vulnerabilities inherent in each of these behaviors.
- Ask participants to turn to the Individual Performance Objective Worksheet. Everyone should complete this worksheet before subsequent one-on-one discussions to develop individual performance objectives for 2000-2001.

Group-Level Workshops (cont.)
Facilitation Guide for Group-Level Managers

Workshop: (cont.)

Wrap-Up:

- Thank participants for attending, participating, and committing to ISSM.
- Again, remind everyone to sign the roster if they haven't already and to submit for credit electronically on the Web!
- If they haven't yet watched the playback of John Browne's July 18 mandatory all-hands meeting, remind them of the expectation that they do so ASAP.
- Inform participants that some will be contacted via email as part of a random sample on the impact of this workshop. Encourage participants to respond candidly.
- Remind everyone that we are all responsible for security and for using the 5-step process routinely.
- Again encourage everyone to use the resources reviewed today for any subsequent questions, concerns or suggestions.

Group-Level Workshops (cont.)
Facilitation Guide for Group-Level Managers

Workshop: (cont.)

After the workshop:

- Review the roster. Follow up (either individually or with a make-up session) with any group members who were not able to participate in the workshop.
- Ensure attendance has been reported electronically on the Web. Refer to the ISSM workshop Web page under "Logistics." Update attendance following subsequent group workshops or one-on-one discussions.
- Prepare a report to the division office. Guidance and an example are also available on the ISSM workshops Web site. (This report just summarizes the questions, concerns and suggestions raised during the group workshop.) This report should be submitted within 5 working days of the group workshop. (No later than August 31.) Report on the number of people who attended the workshop and the number of people who still need to attend. See suggested EDS reports under "Logistics."

Case Studies

Case Studies:
Scenarios Based on Actual Incidents

Directions

Select case studies that are relevant to the work in your group, and continue the discussion on application of the ISSM 5-step process.

Lab-Wide Security Issues

- Vu-Graph Classification
- Badges
- Suspicious Packages
- Passwords
- Faxing
- Foreign Visits
- Theft
- Sensitive Unclassified
- “Unclassified” Processing
- “Unclassified” Presentation
- TSCM

Area Access

- SNM Material Access Area (MAA)
- Foreign Visits & Assignments

Case Studies:
Scenarios Based on Actual Incidents (cont.)

Classified Information

- Accountable Classified
- Misplaced Classified
- Copying Classified Information
- Classified Data Transfer
- Classification
- Shredding Materials
- E-mail
- Excess Material
- Classified Faxing
- Security Containers

Case Studies:
Scenarios Based on Actual Incidents (cont.)

Lab-Wide Security Issues

Vu-Graph Classification:

Scenario: Derivative Classifer Review

Circumstances: You create a view graph and have your derivative classifier review the content. It is not classified. Several days later you make a few modifications and ask your uncleared administrator to put the content into Power Point with a lead and closure slide as well. Someone sees the presentation and declares that it is classified. Your derivative classifier agrees. The changes you made were enough to change the classification.

Badges:

Scenario: Wearing Badge in Public Places

Circumstances: You see a fellow LANL employee in a bank in town with her badge clipped to her collar. She has the yellow PSAP appliance / clip showing as well.

Case Studies:
Scenarios Based on Actual Incidents (cont.)

Lab-Wide Security Issues (cont.)

Suspicious Packages:
Scenario: Suspect Briefcase or Package Unattended in Your Office
Circumstances: You see a package in the hallway just outside your office door. There is no tag or identification on the package.

Passwords:
Scenario: Shared Password.
Circumstances: Fred is on vacation, and he has been working on a document from which you need some information for the boss. You mention your frustration to a coworker and she says "I can get that for you. I know Fred's password."

Faxing:
Scenario: Fax Error
Circumstances: You have just faxed a six-page document on an unclassified Fax machine and the completion report indicates there were seven pages. As you look through the document you find a page in the middle marked Secret.

Case Studies:
Scenarios Based on Actual Incidents (cont.)

Lab-Wide Security Issues (cont.)

Foreign Visits:
Scenario: Foreign Visit Rules
Circumstances: You are the host for a foreign visitor who will arrive tomorrow. You receive a priority letter and an e-mail stating that the original visitor, Bill, will not be coming, and James will now be coming in his place.

Theft:
Scenario: Possible Theft of Government Property
Circumstances: You are a team leader, and one of your employees advises you that a fellow team member has been leaving work each evening with briefcase in one hand and a box in the other arm.

Sensitive Unclassified:
Scenario: Protection of Sensitive / Unclassified Information
Circumstances: During closure and lock-up of your building, you discover a list of employees in the recycle bin. The list includes Z numbers and other numbers in a column marked “performance rating.”

Case Studies:
Scenarios Based on Actual Incidents (cont.)

Lab-Wide Security Issues (cont.)

Sensitive Unclassified # 2:

Scenario: Protection of Sensitive / Unclassified Information

Circumstances: As you are making copies, you see the division budget and a list of mission impact statements in the trash can beside the copier. Some of these impacts involve reduction in the number of employees and inability to properly secure materials.

Unclassified Processing

Scenario: Processing Classified on Unclassified Computer

Circumstances: You are processing data on your unclassified computer. After saving your work, you notice that you typed classified information on your unclassified system.

Case Studies:
Scenarios Based on Actual Incidents (cont.)

Lab-Wide Security Issues (cont.)

Unclassified Presentation

Scenario: Presentation Turns Classified

Circumstances: You are attending a presentation and the slides being presented are unclassified. However, during the presentation the presenter verbally presents material you know is classified.

TSCM

Scenario: Cell Phones in Security Areas

Circumstances: After entering a security area, you notice that you have your personal cell phone with you.

Case Studies:
Scenarios Based on Actual Incidents (cont.)

Area Access

SNM Material Access Area (MAA):
Scenario: Improper Access
Circumstances: You and a coworker enter an area which requires a minimum of two people entering the area together for access to that area. You discover a worker working alone in the area.

Foreign Visits:
Scenario: Foreign Visit Escort
Circumstances: You are the host for a group of seven foreign visitors. You are giving a tour in a security area, and you and another escort discover one of the guests has wandered away from the tour.

Foreign Visits & Assignments:
Scenario: Foreign Visit Escort
Circumstances: You are working in a security area and you encounter a visitor with a red badge who should be under escort. You know this, as it was just announced on the loudspeaker. The visitor is walking around without an escort.

Case Studies:
Scenarios Based on Actual Incidents (cont.)

Classified Information

Accountable Classified:

Scenario: Control of Accountable Classified Material

Circumstances: Alice passes an accountable classified document which is stored in her safe to Bill, and after using it, Bill stores the document in his safe. Later the classified document custodian (CDC) performs an inventory, and the document is not found in Alice's safe.

Misplaced Classified:

Scenario: Control and Location of Classified Material

Circumstances: You open your safe to look for a document you created. You can't find it. You remember that you think you may have given it to Joe to critique for you. Or was it Larry? Joe says, "I remember it. I made comments on it, but gave it back to you last month." Larry is on vacation.

Case Studies:
Scenarios Based on Actual Incidents (cont.)

Classified Information (cont.)

White-Board Copier:

Scenario: Copier, White Board.

Circumstances: You have a classified drawing of a security component for a new building design and you are presenting the drawing to a group of workers and are using a white board in a limited-area conference room. As you draw the design on the white-board (which is capable of making copies) and make a copy for each participant, you recall that you have done this before and have seen others do the same. You realize the white-board copier has not been certified for classified copying.

Xeroxing Classified Documents

Scenario: Classified Document Found on Copier.

Circumstances: A classified document is found on the copying machine. What responsibility does the person have if 1) he knows who owns the document and returns it to the person, 2) he knows the group that owns the document and returns it to the group office, or 3) he does not know the owner of the document?

Case Studies:
Scenarios Based on Actual Incidents (cont.)

Classified Information (cont.)

Xeroxing Classified Documents:

Scenario: Classified Document Lost in Jammed Copier.

Circumstances: You are copying classified material on an approved copier in a secure area. The copier jams. You remove what you think is the jam, but the copier still will not function. What should you do? Subsequently, another individual finds material that is marked classified jammed in the copier.

Classified Data Transfer:

Scenario: Data Transfer between Different Forms of Media

Circumstances: You are working late and are just about to leave for an appointment. You are in fact a bit late. Coworker Bill, the only other employee in the building, asks you to observe as he transfers classified data from his hard drive to his A:/ drive. You explain you can't but will help first thing in the morning. When you come in the next day you offer to help but Bill says "It's O.K. I did it last night."

Case Studies:
Scenarios Based on Actual Incidents (cont.)

Derivative Classifier

Classification:

Scenario: Classification of a Document

Circumstances: You have just completed a memo for your counterpart at DOE, and you are not sure if the document is classified. You think it might be. Your group has two authorized derivative classifiers (ADCs) but one is on vacation and the other is on travel.

Shredding Materials:

Scenario: Destruction of Sensitive or Classified Materials by Shredding

Circumstances: You are a team leader, and the building custodian comes to you with a bag of shredded paper he was taking to the dumpster. You can see that he has discovered a partially shredded document with complete classified paragraphs still legible.

Case Studies:
Scenarios Based on Actual Incidents (cont.)

Derivative Classifier (cont.)

E-Mail:
Scenario: E-Mail Error
Circumstances: You have just received an e-mail from a co-worker who is on travel in Washington, DC . As you read the e-mail, you discover that it contains classified material.

E-Mail:
Scenario: E-Mail Error
Circumstances: A staff member is collaborating with a colleague from the United Kingdom Atomic Weapons Establishment. The colleague sends e-mail that he/she believes is unclassified, but you know it to be classified by DOE standards. What do you do?

Excess Material:
Scenario: Excess Classified Material
Circumstances: You are assigned to a position of a coworker who has retired, and you inherit her office and safe. You discover "volumes" of marked and unmarked documents, all of which you believe to be classified. Much of the material is 12-14 years old.

Case Studies:
Scenarios Based on Actual Incidents (cont.)

Derivative Classifier (cont.)

Classified Faxing:

Scenario: Fax Error

Circumstances: You have just received a Fax document on an unclassified Fax machine. As you read the document, you know that it contains classified material.

Security Containers:

Scenario: Security Container Left Open.

Circumstances: As you are working late one evening, you see a two-drawer safe in an open office down the hall from your office. It is in a limited area, and it is 6:30 p.m. The safe has a "LOCKED" sign on it, but the lower drawer is open about 3 inches.

Case Studies:
Scenarios Based on Actual Incidents (cont.)

Derivative Classifier (cont.)

Security Containers:

Scenario: Security Container Check.

Circumstances: A safe checker spins the dial on a “locked” safe but fails to pull the drawers. Subsequently, a security guard pulls on the drawer, and it opens. It is discovered that the safe has had a mechanical failure. Can the owner of the safe get a security infraction? Can the safe checker receive a security infraction? What if there is no written procedure for safe checking?

Workshop Handouts and Worksheets

- ISSM 5-Step Process
- Sample Applications of the 5-Step Process
- Enhancing Our Security Awareness: Behaviors Can Lead to Incidents
- Resources Quick Reference List
- Report Guidance for Division-Level Directors
- Report Guidance for Group-Level Managers
- ISSM Individual Performance Objectives Worksheet

Printable PDF of This Document

Opening the Printable PDF

If you would like to print this document in compact format, just click on the button below. Once you have that file open, you can print it for a hard copy.

OPEN THE PRINTABLE PDF DOCUMENT

The 5-Step Process

The 5-Steps	Questions to ask yourself at the start of each day…
1. Define Scope of Work ➢ Translate mission into work ➢ Set expectations (e.g., goals and objectives) ➢ Identify and prioritize tasks ➢ Allocate resources	What outcome is expected of me today? Who is helping me? Do others need to know what I'm doing? Do I have the appropriate equipment? Am I authorized to do the work? Am I comfortable proceeding? Should I stop work?
2. Analyze Security Vulnerabilities ➢ Identify and analyze the security vulnerabilities associated with performing specific work	What are the vulnerabilities? Have they changed? Are they adequately controlled? How can my work be compromised? What can go wrong? What has gone wrong before? Should I stop work?
3 Develop and Implement Security Controls ➢ Identify appropriate standards and requirements ➢ Develop/implement cost-effective security controls to prevent or mitigate the work-associated vulnerabilities	What are the governing requirements? Is there an "activity security plan"? Are special approvals needed? Is special training/authorization required? Is special equipment required? Prohibited? Do I understand the controls? Am I comfortable with them? Are the controls realistic? Will they get implemented? Should I stop work?
4 Perform the Work Work within Controls ➢ Confirm readiness ➢ Perform work securely within established security controls	Is everything the same today as it was yesterday? Is all equipment working/authorized? Do I know enough to perform the work securely? Am I feeling rushed or pressured to do this job? Do I need help? Should I stop work?
5 Ensure Performance ➢ Collect feedback information on the adequacy of security controls ➢ Identify and implement opportunities for improving the definition, planning, and execution of work ➢ Conduct line and independent assessments ➢ Reinforce expected behaviors	Did the experiment "work?" Did we identify problems and correct them? Are process changes needed? Are secure/better methods possible? Were responsibilities clear? Do I ever want to do this again? What will I do differently next time?

Sample Applications of the ISSM 5-Step Process

Shown below are two applications of the ISSM 5-step process to two entirely different work activities within the Laboratory. The first work activity is performed by every employee – i.e., engaging in performance evaluation with one's supervisor. This activity involves unclassified, but sensitive information. The second work activity is performed by a large percentage of employees at the Laboratory – i.e., establishing a stand-alone classified computing system. This activity involves classified information. In all cases, the ISSM 5-step process begins with defining the scope of work, and then identifying and analyzing the associated security vulnerabilities, developing and implementing security controls, performing the work, and finally evaluating and improving performance. A given control may not fully mitigate an analyzed vulnerability, but combination with others may. Though these two sample applications may not be exhaustive in terms of identifying and controlling vulnerabilities, they nevertheless illustrate how each of the 5 steps should be viewed and executed to help ensure that all Laboratory work is performed securely.

Application #1: Employee Performance Evaluation

1. Define Scope of Work: engage in performance evaluation with supervisor

<u>translate into work activities</u>
1) employee prepares accomplishments/results for supervisor
2) employee meets with supervisor
3) supervisor writes performance summary, ORC score
4) employee reviews online performance summary

<u>set expectations</u>
1) this material is treated as sensitive, unclassified material
2) the new on-line web-based system is used

<u>prioritize tasks</u>
1) various deadlines apply to the process

2. Identify and Analyze Vulnerabilities

<u>identify vulnerabilities</u>
1) inadvertent inclusion/disclosure of classified information
2) inadvertent disclosure of sensitive, unclassified information
3) loss of information from system malfunctions

<u>analyze vulnerabilities</u>
1) disclosure caused by multiple users of processing computer
2) transmission of sensitive, unclassified information over non-sensitive networks (e.g., working from home)
3) persons with classified assignments mistakenly include classified information in their accomplishments/results summaries
4) computer files or hardcopy left laying uncontrolled
5) various computer malfunctions cause data loss

3. Develop and Implement Controls

identify standards and requirements
1) consult HR guidance on handling of performance appraisals
2) consult LANL computer security requirements for processing of sensitive, unclassified information

develop controls to prevent or mitigate vulnerabilities
1) employees prepare write-ups in private, at work, on computer prepared for handling sensitive, unclassified information (1,2)
2) use individual's personal computers with access control, or common computers with separate account access controls, or use separate media and individual backups (1,5)
3) employees save information on removable media or hardcopy which are reasonably secured against unauthorized access (1,4,5)
4) employees conducting classified work review sections of write-up with an ADC (3)
5) use of encryption on files (1,2) [may not be a practical control at this time]
6) use of smart card required for system access (1)
7) use of online access control protocols to limit read access to employee's direct line supervisors (1)
8) mark hardcopy and removable media appropriately (1,4)
9) identify resources and experts capable of providing useful information about or help during the process (all)

*Note: parenthetical notes refer to the analyzed vulnerabilities addressed in 2. above

4. Perform Work

1) use the selected/required controls while performing the work
2) confirm readiness to engage in the work (e.g., controls are operative, time is available, needed resources/tools are available)

5. Ensure Performance

collect feedback/identify improvement opportunities/make changes
1) gather and act on suggestions and lessons learned for improving the process

oversight & enforcement/reinforcement & accountability
1) engage your OCSR on issues or concerns about sensitive, unclassified computing
2) managers engage in self assessments (walkarounds) of the process in action
3) compare process with any applicable security plans

Application #2: Classified Computing System

1. Define Scope of Work: establish a stand-alone classified computing system

translate into work activities
1) determine level and category of information to be processed
2) determine needed system parameters (speed, memory capacity, peripherals and their connectivity, external communications needs, ...)
3) determine location for system
4) determine how data will be transferred in/out of system
5) procure hardware
6) procure software
7) prepare appropriate documentation for accreditation
8) obtain required reviews

set expectations
1) system will conform with requirements of LANL Master AIS Security Plan for Single-User Systems Processing Classified Data

prioritize tasks
1) review Master AIS Security Plan
2) establish hardware/software in selected work area
3) review with S-5 for accreditation approval process
4) introduce classified materials into system

2. Identify and Analyze Vulnerabilities

identify vulnerabilities
1) loss of control or compromise of classified information
2) loss of classified information to system failure

analyze vulnerabilities
1) unauthorized access to information or work area
2) tempest-based disclosure of information
3) insider threat
4) inadvertent access to information or work area
5) failure of various system components

3. Develop and Implement Controls

identify standards and requirements
1) consult LANL Master AIS Security Plan for Single-User Systems Processing Classified Data http://int.lanl.gov/orgs/s/s5/docs/entire_SUC_master_plan.pdf
2) consult LANL Computer Security Handbook http://int.lanl.gov/orgs/s/s5/handbook.shtml
3) consult with TSCM experts
4) consult LANL vault/vault type room and secured repository (safe) requirements

develop controls to prevent or mitigate vulnerabilities
1) incorporate LANL-approved physical barriers to work area (including tempest restrictions), with restrictive access controls (1,3,4)
2) position monitor display so as not to be visible from doors, windows, or other openings into work area (1,2,4)
3) employ encryption technology (1,2,3,4)
4) fix position of cable runs to eliminate significant cross talk (2)
5) work with OCSR to ensure correct installation (1,2,4,5)
6) limit access to personnel with a need-to-know and who have proper clearances (1,3,4)
7) develop SOP for classified system operation (all)
8) review setup with S-5 (1,2,4)

*Note: parenthetical notes refer to the analyzed vulnerabilities addressed in 2. above

4. Perform Work

1) use the selected/required controls while performing the work
2) confirm readiness to engage in the work (e.g., controls are operative, time is available, needed resources/tools are available)

5. Ensure Performance

collect feedback/identify improvement opportunities/make changes
1) gather and act on suggestions and lessons learned for improving the work area, system, or security plan

oversight & enforcement/reinforcement & accountability
1) engage your OCSR on issues or concerns about classified computing
2) managers engage in self assessments (walkarounds) of the work area with owner, users and security personnel
3) owner, users and security personnel compare work are and system with the security plan

Use the back button (◀◀) from the main menu bar at the top of the page to get back to your previous page.

Integrated Safeguards & Security Management

"Behaviors Can Lead To Incidents"

Property: Theft, Protection, Usage, Disposal, Loss, Fraud, Accountability

_ When on travel don't leave lap-top-computers, pagers and cell phones unattended or unlocked.
_ As you leave your office put valuables in the proper storage place and lock doors.
_ Tempted to take that worn and "already replaced" item home rather than turning it in to your property representative? Bad Choice.

Facilities: Access, Protection, Usage, Badges, Visitors, Securing

_ As a group of "strangers" walk unescorted through your workplace, engage or challenge them to determine: their need to be there and how you might help them find their destination.
_ If you are only "pretty sure" you locked the building as the last one out, it will be worth your time and peace of mind to go back and check. You may need a better "lock up system".
_ When at the bank, store, or Dentist's office, your badge should NOT be hanging around your neck. The badge is for Lab business on Lab property. Otherwise stow it, don't show it!

Information: Classification, Document, Vu-Graf, Speech, Media, Passwords

_ Review the documents on your desk before you leave. Different documentation and information require different protection. If you are not sure, find out, before you risk compromise.
_ Use your Authorized Derivative Classifier (ADC) on a regular basis. Develop rapport. Build in the review time. Use S-7 for emergencies or to resolve classification issues.
_ Determine "what" you are working with, who is the audience, and "where" you are going with the project before you choose the media and release the product. Sensitive? Classified?

_ **Communication:** Telephone, Cell phone, FAX, E-Mail, Mail, Voice, STU-III
_ If you receive a communication, which looks as though it may be classified, but is not marked as such, report the situation and determine the appropriate actions.
_ Private cell phones for private, non-LANL matters should not come to work, behind the fence. LANL cell phones have rules associated with them and a LANL cell phone user must know and follow these rules.

_ **People:** Clearance, Access, Need-To-Know, Escort, Behavior
_ Before the briefing starts and the classified matter is discussed, ensure the audience has both clearance and need to know for the topics to be discussed.
_ Escorting guests through your work area requires your undivided attention. It is NOT appropriate to excuse yourself from the guest for a few minutes and leave the uncleared guest alone in your office to have a short conference in your boss's office. It's not polite either!

Procedures and Policy: Know, Understand, Follow, Uphold, Improve

_ You can't work as quickly with some new policies and procedures, but to ignore them and proceed in the old mode may create a vulnerability for you and the Laboratory.
_ If you have an idea that might help to meet the intent of a security rule and would save time, and money, present it to management. But under no circumstance should you ignore the rule.
_ When on travel don't leave lap-top-computers, pagers and cell phones unattended or unlocked.
_ As you leave your office put valuables in the proper storage place and lock doors.
_ Tempted to take that worn and "already replaced" item home rather than turning it in to your property representative? Bad Choice.

Facilities: Access, Protection, Usage, Badges, Visitors, Securing

_ As a group of "strangers" walk unescorted through your workplace, engage or challenge them to determine: their need to be there and how you might help them find their destination.

_ If you are only "pretty sure" you locked the building as the last one out, it will be worth your time and peace of mind to go back and check. You may need a better "lock up system".

_ When at the bank, store, or Dentist's office, your badge should NOT be hanging around your neck. The badge is for Lab business on Lab property. Otherwise stow it, don't show it!

Information: Classification, Document, Vu-Graf, Speech, Media, Passwords

_ Review the documents on your desk before you leave. Different documentation and information require different protection. If you are not sure, find out, before you risk compromise.

_ Use your Authorized Derivative Classifier (ADC) on a regular basis. Develop rapport. Build in the review time. Use S-7 for emergencies or to resolve classification issues.

_ Determine "what" you are working with, who is the audience, and "where" you are going with the project before you choose the media and release the product. Sensitive? Classified?

Communication: Telephone, Cell phone, FAX, E-Mail, Mail, Voice, STU-III

_ If you receive a communication, which looks as though it may be classified, but is not marked as such, report the situation and determine the appropriate actions.

_ Private cell phones for private, non-LANL matters should not come to work, behind the fence. LANL cell phones have rules associated with them and a LANL cell phone user must know and follow these rules.

People: Clearance, Access, Need-To-Know, Escort, Behavior

_ Before the briefing starts and the classified matter is discussed, ensure the audience has both clearance and need to know for the topics to be discussed.

_ Escorting guests through your work area requires your undivided attention. It is NOT appropriate to excuse yourself from the guest for a few minutes and leave the uncleared guest alone in your office to have a short conference in your boss's office. It's not polite either!

Procedures and Policy: Know, Understand, Follow, Uphold, Improve

_ You can't work as quickly with some new policies and procedures, but to ignore them and proceed in the old mode may create a vulnerability for you and the Laboratory.

_ If you have an idea that might help to meet the intent of a security rule and would save time, and money, present it to management. But under no circumstance should you ignore the rule.

Use the back button (◀◀) from the main menu bar at the top of the page to get back to your previous page.

Resources

Who to Call

Badge Office	7-6901
Classification	7-5011
Clearance Processing Team	7-7253
Counterintelligence	5-6090
Electronic Communications	5-1795
Emergency Management and Response	7-6211
Foreign Visitors and Assignments	5-1572
ISEC (Internal Security)	5-6090
Nuclear Materials	7-5886
PSAP (Personnel Security Assurance Program)	7-0869
PTLA (Protective Force)	7-4531
Security Help Desk	5-2002
(Ensure issues which are classified are communicated securely!)	
Security Plans	7-0558
Security Training	5-7844
(including questions about credit for security training)	

Useful Web Sites

ISSM Website	http://int.lanl.gov/orgs/s/issm/
Security and Safeguards Division	http://int.lanl.gov/orgs/s/
Classified Matter Protection and Control	http://int.lanl.gov/orgs/s/cmpc/
LANL Password Policy	http://network.lanl.gov/passwords/policy.shtml
Publishing at Los Alamos	http://int.lanl.gov/publishing/
S-5 Computer Security Handbook	http://int.lanl.gov/orgs/s/s5/handbook.shtml
Virtual Training Center	http://www.lanl.gov/labview/training/training.html

DOE Official Policies

DOE Security Regulations and Directives
http://www.cta.doe.gov/ssb2000/fsheets/fs17.html

Polygraphs
http://www.doe.gov/news/fedreg.htm

Reporting Close and Continuing Contact with Sensitive Country Foreign Nationals
http://www.cta.doe.gov/ssb2000/fsheets/fs29.html

Security Reporting Requirements
http://www.cta.doe.gov/ssb2000/fsheets/fs24.html

Sensitive Unclassified Information
http://www.cta.doe.gov/ssb2000/fsheets/fs04.html

“Zero Tolerance”—Secretarial Policy Statement
http://www.cta.doe.gov/ssb2000/fsheets/fs11.html

Security and Safeguards Division

S-1 Security Plans and Programs	7-0558
- Vulnerability Analysis	5-0471
- Nuclear Materials Upgrade Program	5-0473
- Strategic Planning	7-0558
S-2 Program Integration	7-7565
- Security Requirements and Guidance	
- Security Assessments	
- Physical Security	
- Organizational Security Support	
- Protective Force Oversight	
S-3 Security Systems	7-4801
- Access Control	
S-4 Material Control and Accountability	7-5886
S-5 Computer and Technical Security	5-1795
- Computer Security	5-1795
- Technical Surveillance Countermeasures	5-8799 or 5-8867
- Secure Faxes, MASS (Material Accountability and Safeguards System)	7-1607
- Cellular Phones, PTS (Protected Transmission System)	5-5599
S-6 Information and Personnel Security	5-6565
- Classified Matter Protection and Control	5-7467
- Security Awareness, Briefings	7-0077
- Badge Office	7-6901
- Clearance Processing Team	7-7253
- PSAP	7-0869 or 5-8500
S-7 Classification	
- Classification/Declassification Services	7-5011
- Publication Release	7-5013
S-8 Emergency Management and Response	7-6211
S-SPO Special Projects Office	5-3505
- Harassing phone calls/letters	
- Illegal substances on Lab property	
- Property protection	
- Threats/harassment	
- Vandalism	
- Protests/demonstrations	

Resource People in Your Organization

ADC Authorized Derivative Classifier
CDC Classified Document Custodian
OCSR Organizational Computer Security Representative
OSSO Organizational Safeguards and Security Officer

Your Contacts

ADC _____
CDC _____
OCSR _____
OSSO _____

Integrated Safeguards & Security Management

Questions, Concerns, Suggestions Collection & Reporting

General: The worker's voice in ISSM is critical to its success. The data we wish to capture during the initial ISSM rollout and beyond is that which our LANL workers offer to identify questions, concerns or suggestions they have on how to improve security at the Laboratroy. This might include current challenges, best practices, suggestions, and relevant input to the ISSM steering committee for the ISSM path forward. Harvesting the ideas and knowledge of our workforce will only help us to enhance our security performance.

Data Collection Opportunities: Worker ideas and experience will be discussed and collected at:

_ Laboratory All Hands Meeting
_ Division Directors Planning Sessions linking management efforts to Group Workshops.
_ Group or Team level Workshops
_ Individual efforts for those wishing to offer issues or concerns privately or anonymously

Data Collection Methods:

_ Laboratory Director's Open Meeting:
- Facilitators will capture worker comments and issues and forward to Security HELP Desk for analysis / action.
- Security HELP desk access will be encouraged (secure@lanl.gov or 5-2002 Anonymous at Mail Stop K-560)

_ Division Director's meetings linking Director's meeting to Group Workshops.
- Division staff will arrange for capture of ideas and summarize using Division Workshop Report Guide.
- Divisions are encouraged to forward the report after roll up with group reports to the Security HELP Desk for analysis / action. Division should also analyze and address any issue they can at the Division level.

_ Group or Team level Workshops
- Group staff will arrange for capture of ideas and summarize using Group Workshop Report Guide: The report guide covers the types of issues to be included. This report will be forwarded to division for roll-up into division report for division and Security HELP desk analysis / action.
- Individual concerns during these workshops or after the workshops for those wishing to offer issues privately or anonymously.
- Security HELP desk access is encouraged.(secure@lanl.gov or 5-2002, Mail Stop K-560 (Anonymously). NOTE: Ensure that questions that are classified are communicated securely.

Integrated Safeguards & Security Management

Enhancing our Security Performance - - ISSM
Division-level Management Report Guide

Complete this report after all groups in your Division have completed their workshops

Date: _____

Division: _____

Division Leader _____

1. To date, what percentage of workers in your division have completed this training?
2. When do you expect to be at 100% completion?
3. What were the most common questions and concerns raised during the group-level workshops?
4. Which questions, concerns or suggestions for improving security performance are you addressing at the Division level?
5. What are you doing to follow-up on questions, concerns or suggestions that were referred to you?
6. How do you plan to respond to the groups who referred questions, concerns or suggestions to the Division Office?
7. Which issues are you referring for further assistance (to your ALD or DLD)?
8. Which issues are being forwarded to the Security HELP Desk?

Send copies of this report to the ALD or DLD to which you report *and* to the Security HELP Desk (MS K560) by September 15, 2000.

Use the back button (◀◀) from the main menu bar at the top of the page to get back to your previous page.

Integrated Safeguards & Security Management

Questions, Concerns, Suggestions Collection & Reporting

General: The worker's voice in ISSM is critical to its success. The data we wish to capture during the initial ISSM rollout and beyond is that which our LANL workers offer to identify questions, concerns or suggestions they have on how to improve security at the Laboratroy. This might include current challenges, best practices, suggestions, and relevant input to the ISSM steering committee for the ISSM path forward. Harvesting the ideas and knowledge of our workforce will only help us to enhance our security performance.

Data Collection Opportunities: Worker ideas and experience will be discussed and collected at:

_ Laboratory All Hands Meeting
_ Division Directors Planning Sessions linking management efforts to Group Workshops.
_ Group or Team level Workshops
_ Individual efforts for those wishing to offer issues or concerns privately or anonymously

Data Collection Methods:

_ Laboratory Director's Open Meeting:
- Facilitators will capture worker comments and issues and forward to Security HELP Desk for analysis / action.
- Security HELP desk access will be encouraged (secure@lanl.gov or 5-2002 Anonymous at Mail Stop K-560)

_ Division Director's meetings linking Director's meeting to Group Workshops.
- Division staff will arrange for capture of ideas and summarize using Division Workshop Report Guide.
- Divisions are encouraged to forward the report after roll up with group reports to the Security HELP Desk for analysis / action. Division should also analyze and address any issue they can at the Division level.

_ Group or Team level Workshops
- Group staff will arrange for capture of ideas and summarize using Group Workshop Report Guide: The report guide covers the types of issues to be included. This report will be forwarded to division for roll-up into division report for division and Security HELP desk analysis / action.
- Individual concerns during these workshops or after the workshops for those wishing to offer issues privately or anonymously.
- Security HELP desk access is encouraged.(secure@lanl.gov or 5-2002, Mail Stop K-560 (Anonymously). NOTE: Ensure that questions that are classified are communicated securely.

Integrated Safeguards & Security Management

Enhancing our Security Performance - - ISSM
Group-level Management Report Guide

Complete this report when at least 80% of the group members you expected to attend the group-level workshops have completed the workshops or have been briefed individually.

Date: _____

Division: _____

Group: _____

Group Leader: _____

1. How many people in your group were expected to complete this workshop?

2. To date, how many of those have completed the workshop?

3. What are you doing to follow-up with those who have not yet completed the workshop?

4. What questions or concerns did your staff raise during the workshop?

5. What suggestions for improving security practices were made during the workshop?
   - Start with any that you have been able to implement within your group.
   - Include suggestions that could help other groups in your Division or Lab-wide.

6. What questions or concerns did you defer (could not be answered or addressed during the workshop)?

7. What will you do to follow-up on any questions, concerns or suggestions raised during the meeting that could not be resolved at that time?
   - Include how you plan to keep the group informed on how their questions, concerns or suggestions are addressed.

8. What suggestions for improving security do you need assistance with or additional resources to implement?

9. What further information about your group workshop would you like to share?

Send to your Division Office by August 31, 2000.

Use the back button (◀◀) from the main menu bar at the top of the page to get back to your previous page.

Integrated Safeguards & Security Management

ISSM Individual Performance Objectives Worksheet

Directions: Use the **ISSM Five Step Process to identify** roles, responsibilities, and performance objectives you might use in the future in your performance plan.

Based on workshop discussion, what security insights have you gained as applied to your work?

_____
_____
_____
_____
_____

How will you incorporate these insights into your daily work?

_____
_____
_____
_____
_____

What are your duties involving security? (Some concepts to help with the inventory: Badge? Property? Keys? Passwords? Security Container? Physical Security – Your Office, Building? Cell Phone? Sensitive Data? Classified Information? Visitors?)

_____
_____
_____
_____
_____

How would you best accomplish these duties and what are the performance objectives associated with these duties /tasks?

_____
_____
_____
_____
_____

By Applying the 5-Step Process, you will be able to answer the following questions:

1. Are your work and workplace secure?
2. How do you know?
   - Do you know the security requirements governing your work/workplace and how they are being met?
   - Do you know the security vulnerabilities in your work/workplace and whether controls are sufficient to mitigate them?

The 5-Step Process

The 5-Steps	Questions to ask yourself at the start of each day…
1. Define Scope of Work ➢ Translate mission into work ➢ Set expectations (e.g., goals and objectives) ➢ Identify and prioritize tasks ➢ Allocate resources	What outcome is expected of me today? Who is helping me? Do others need to know what I'm doing? Do I have the appropriate equipment? Am I authorized to do the work? Am I comfortable proceeding? Should I stop work?
2. Analyze Security Vulnerabilities ➢ Identify and analyze the security vulnerabilities associated with performing specific work	What are the vulnerabilities? Have they changed? Are they adequately controlled? How can my work be compromised? What can go wrong? What has gone wrong before? Should I stop work?
3 Develop and Implement Security Controls ➢ Identify appropriate standards and requirements ➢ Develop/implement cost-effective security controls to prevent or mitigate the work-associated vulnerabilities	What are the governing requirements? Is there an "activity security plan"? Are special approvals needed? Is special training/authorization required? Is special equipment required? Prohibited? Do I understand the controls? Am I comfortable with them? Are the controls realistic? Will they get implemented? Should I stop work?
4 Perform the Work Work within Controls ➢ Confirm readiness ➢ Perform work securely within established security controls	Is everything the same today as it was yesterday? Is all equipment working/authorized? Do I know enough to perform the work securely? Am I feeling rushed or pressured to do this job? Do I need help? Should I stop work?
5 Ensure Performance ➢ Collect feedback information on the adequacy of security controls ➢ Identify and implement opportunities for improving the definition, planning, and execution of work ➢ Conduct line and independent assessments ➢ Reinforce expected behaviors	Did the experiment "work?" Did we identify problems and correct them? Are process changes needed? Are secure/better methods possible? Were responsibilities clear? Do I ever want to do this again? What will I do differently next time?

Sample Applications of the ISSM 5-Step Process

Shown below are two applications of the ISSM 5-step process to two entirely different work activities within the Laboratory. The first work activity is performed by every employee – i.e., engaging in performance evaluation with one's supervisor. This activity involves unclassified, but sensitive information. The second work activity is performed by a large percentage of employees at the Laboratory – i.e., establishing a stand-alone classified computing system. This activity involves classified information. In all cases, the ISSM 5-step process begins with defining the scope of work, and then identifying and analyzing the associated security vulnerabilities, developing and implementing security controls, performing the work, and finally evaluating and improving performance. A given control may not fully mitigate an analyzed vulnerability, but combination with others may. Though these two sample applications may not be exhaustive in terms of identifying and controlling vulnerabilities, they nevertheless illustrate how each of the 5 steps should be viewed and executed to help ensure that all Laboratory work is performed securely.

Application #1: Employee Performance Evaluation

1. Define Scope of Work: engage in performance evaluation with supervisor

<u>translate into work activities</u>
1) employee prepares accomplishments/results for supervisor
2) employee meets with supervisor
3) supervisor writes performance summary, ORC score
4) employee reviews online performance summary

<u>set expectations</u>
1) this material is treated as sensitive, unclassified material
2) the new on-line web-based system is used

<u>prioritize tasks</u>
1) various deadlines apply to the process

2. Identify and Analyze Vulnerabilities

<u>identify vulnerabilities</u>
1) inadvertent inclusion/disclosure of classified information
2) inadvertent disclosure of sensitive, unclassified information
3) loss of information from system malfunctions

<u>analyze vulnerabilities</u>
1) disclosure caused by multiple users of processing computer
2) transmission of sensitive, unclassified information over non-sensitive networks (e.g., working from home)
3) persons with classified assignments mistakenly include classified information in their accomplishments/results summaries
4) computer files or hardcopy left laying uncontrolled
5) various computer malfunctions cause data loss

3. Develop and Implement Controls

identify standards and requirements
1) consult HR guidance on handling of performance appraisals
2) consult LANL computer security requirements for processing of sensitive, unclassified information

develop controls to prevent or mitigate vulnerabilities
1) employees prepare write-ups in private, at work, on computer prepared for handling sensitive, unclassified information (1,2)
2) use individual's personal computers with access control, or common computers with separate account access controls, or use separate media and individual backups (1,5)
3) employees save information on removable media or hardcopy which are reasonably secured against unauthorized access (1,4,5)
4) employees conducting classified work review sections of write-up with an ADC (3)
5) use of encryption on files (1,2) [may not be a practical control at this time]
6) use of smart card required for system access (1)
7) use of online access control protocols to limit read access to employee's direct line supervisors (1)
8) mark hardcopy and removable media appropriately (1,4)
9) identify resources and experts capable of providing useful information about or help during the process (all)

*Note: parenthetical notes refer to the analyzed vulnerabilities addressed in 2. above

4. Perform Work

1) use the selected/required controls while performing the work
2) confirm readiness to engage in the work (e.g., controls are operative, time is available, needed resources/tools are available)

5. Ensure Performance

collect feedback/identify improvement opportunities/make changes
1) gather and act on suggestions and lessons learned for improving the process

oversight & enforcement/reinforcement & accountability
1) engage your OCSR on issues or concerns about sensitive, unclassified computing
2) managers engage in self assessments (walkarounds) of the process in action
3) compare process with any applicable security plans

Application #2: Classified Computing System

1. Define Scope of Work: establish a stand-alone classified computing system

translate into work activities
1) determine level and category of information to be processed
2) determine needed system parameters (speed, memory capacity, peripherals and their connectivity, external communications needs, ...)
3) determine location for system
4) determine how data will be transferred in/out of system
5) procure hardware
6) procure software
7) prepare appropriate documentation for accreditation
8) obtain required reviews

set expectations
1) system will conform with requirements of LANL Master AIS Security Plan for Single-User Systems Processing Classified Data

prioritize tasks
1) review Master AIS Security Plan
2) establish hardware/software in selected work area
3) review with S-5 for accreditation approval process
4) introduce classified materials into system

2. Identify and Analyze Vulnerabilities

identify vulnerabilities
1) loss of control or compromise of classified information
2) loss of classified information to system failure

analyze vulnerabilities
1) unauthorized access to information or work area
2) tempest-based disclosure of information
3) insider threat
4) inadvertent access to information or work area
5) failure of various system components

3. Develop and Implement Controls

identify standards and requirements
1) consult LANL Master AIS Security Plan for Single-User Systems Processing Classified Data http://int.lanl.gov/orgs/s/s5/docs/entire_SUC_master_plan.pdf
2) consult LANL Computer Security Handbook http://int.lanl.gov/orgs/s/s5/handbook.shtml
3) consult with TSCM experts
4) consult LANL vault/vault type room and secured repository (safe) requirements

develop controls to prevent or mitigate vulnerabilities
1) incorporate LANL-approved physical barriers to work area (including tempest restrictions), with restrictive access controls (1,3,4)
2) position monitor display so as not to be visible from doors, windows, or other openings into work area (1,2,4)
3) employ encryption technology (1,2,3,4)
4) fix position of cable runs to eliminate significant cross talk (2)
5) work with OCSR to ensure correct installation (1,2,4,5)
6) limit access to personnel with a need-to-know and who have proper clearances (1,3,4)
7) develop SOP for classified system operation (all)
8) review setup with S-5 (1,2,4)

*Note: parenthetical notes refer to the analyzed vulnerabilities addressed in 2. above

4. Perform Work

1) use the selected/required controls while performing the work
2) confirm readiness to engage in the work (e.g., controls are operative, time is available, needed resources/tools are available)

5. Ensure Performance

collect feedback/identify improvement opportunities/make changes
1) gather and act on suggestions and lessons learned for improving the work area, system, or security plan

oversight & enforcement/reinforcement & accountability
1) engage your OCSR on issues or concerns about classified computing
2) managers engage in self assessments (walkarounds) of the work area with owner, users and security personnel
3) owner, users and security personnel compare work are and system with the security plan

Use the back button (◀◀) from the main menu bar at the top of the page to get back to your previous page.

Integrated Safeguards & Security Management

"Behaviors Can Lead To Incidents"

Property: Theft, Protection, Usage, Disposal, Loss, Fraud, Accountability

_ When on travel don't leave lap-top-computers, pagers and cell phones unattended or unlocked.
_ As you leave your office put valuables in the proper storage place and lock doors.
_ Tempted to take that worn and "already replaced" item home rather than turning it in to your property representative? Bad Choice.

Facilities: Access, Protection, Usage, Badges, Visitors, Securing

_ As a group of "strangers" walk unescorted through your workplace, engage or challenge them to determine: their need to be there and how you might help them find their destination.
_ If you are only "pretty sure" you locked the building as the last one out, it will be worth your time and peace of mind to go back and check. You may need a better "lock up system".
_ When at the bank, store, or Dentist's office, your badge should NOT be hanging around your neck. The badge is for Lab business on Lab property. Otherwise stow it, don't show it!

Information: Classification, Document, Vu-Graf, Speech, Media, Passwords

_ Review the documents on your desk before you leave. Different documentation and information require different protection. If you are not sure, find out, before you risk compromise.
_ Use your Authorized Derivative Classifier (ADC) on a regular basis. Develop rapport. Build in the review time. Use S-7 for emergencies or to resolve classification issues.
_ Determine "what" you are working with, who is the audience, and "where" you are going with the project before you choose the media and release the product. Sensitive? Classified?

_ **Communication:** Telephone, Cell phone, FAX, E-Mail, Mail, Voice, STU-III
_ If you receive a communication, which looks as though it may be classified, but is not marked as such, report the situation and determine the appropriate actions.
_ Private cell phones for private, non-LANL matters should not come to work, behind the fence. LANL cell phones have rules associated with them and a LANL cell phone user must know and follow these rules.

_ **People:** Clearance, Access, Need-To-Know, Escort, Behavior
_ Before the briefing starts and the classified matter is discussed, ensure the audience has both clearance and need to know for the topics to be discussed.
_ Escorting guests through your work area requires your undivided attention. It is NOT appropriate to excuse yourself from the guest for a few minutes and leave the uncleared guest alone in your office to have a short conference in your boss's office. It's not polite either!

Procedures and Policy: Know, Understand, Follow, Uphold, Improve

_ You can't work as quickly with some new policies and procedures, but to ignore them and proceed in the old mode may create a vulnerability for you and the Laboratory.
_ If you have an idea that might help to meet the intent of a security rule and would save time, and money, present it to management. But under no circumstance should you ignore the rule.
_ When on travel don't leave lap-top-computers, pagers and cell phones unattended or unlocked.
_ As you leave your office put valuables in the proper storage place and lock doors.
_ Tempted to take that worn and "already replaced" item home rather than turning it in to your property representative? Bad Choice.

Resources

Who to Call

Security Help Desk _____ (505) 665-2002

Security and Safeguards Division

S-1 Security Plans _____ **(505) 667-0558**
- Vulnerability Analysis _____ (505) 665-0471
- Nuclear Materials Safeguards & Security Upgrade Program _____ (505) 665-0473
- Strategic Planning _____ (505) 667-0558

S-2 Security Integration _____ **(505) 667-7565**
- Security Requirements and Guidance
- Security Assessments
- Organizational Security Support
- Protective Force Oversight
- Security Training _____ (505) 665-7844

S-3 Security Systems _____ **(505) 667-4801**
- Access Control

S-4 Material Control and Accountability _____ **(505) 667-5886**

S-5 Security Support _____ **(505) 665-6565**
- Technical Surveillance Countermeasures _____ (505) 665-2437 or (505) 665-8867
- Secure Faxes, MASS _____ (505) 665-8756
- Cellular Phones _____ (505) 665-8756
- Classified Matter Protection and Control _____ (505) 665-7467
- Physical Security _____ (505) 665-7281
- Vault/Vault-type room Certification _____ (505) 665-2437

S-6 Personnel Security _____ **(505) 665-6565**
- Badge Office _____ (505) 667-6901
  - Classified Visits
    - Incoming _____ (505) 667-5587
    - Outgoing _____ (505) 667-7959
- Clearance Processing Team _____ (505) 667-7253
- PSAP _____ (505) 667-0869 or (505) 665-8500

S-7 Classification _____ **(505) 667-5011**
- Classification/Declassification services _____ (505) 667-0511
- Publication Release _____ (505) 667-5013

S-8 Emergency Management and Response _____ **(505) 667-6211**

S-DO Security and Safeguards Division Office _____ **(505) 667-5911**

S-OSI Office of Security Inquiries _____ **(505) 665-3505**
- Security Incidents
- Harassing phone calls/letters
- Illegal substances on Lab property
- Property protection
- Threats/harassment
- Vandalism
- Protests/demonstrations

Chief Information Officer _____ (505) 665-1795
- Cyber Security Team _____ (505) 665-1795
- Protected Transmission System (PTS) _____ (505) 665-5599

Internal Security (ISEC) _____ (505) 665-6090
- Counterintelligence _____ (505) 665-6090
- Foreign Visits and Assignments _____ (505) 665-1572
- Operational Security (OPSEC) _____ (505) 665-3372

Protective Force (PTLA) _____ (505) 667-4531

Security Help Desk

The Security and Safeguards HELP desk **(505) 665-2002** provides one-stop information for all Laboratory organizations that need assistance in meeting their safeguards and security responsibilities. The Security and Safeguards HELP desk operation interacts closely with the division and group security representatives, providing assistance to divisions requesting OSSO support, and assisting with the implementation of the Integrated Safeguards and Security Management program. By maintaining a list of frequently asked questions and answers, the HELP desk team opens up lines of communication between the OSSOs, CDCs, OCSRs, ADCs, and key/core custodians.

Security Resources in your Organization

ADC	Authorized Derivative Classifier
CDC	Classified Document Custodian
OCSR	Organizational Computer Security Representative
OSSO	Organizational Safeguards and Security Officer
ISSO	Information Safeguards & Security Officer
CMC	Classified Media Custodian
CPC	Classified Parts Custodian
NMC	Nuclear Material Custodians
TID Custodians	Tamper Indicating Device Custodians
AAC	Access Alarms Custodian

Useful Web Sites

Security and Safeguards Division
http://int.lanl.gov/orgs/s/

Classified Matter Protection & Control
http://int.lanl.gov/orgs/s/cmpc/

Publishing at Los Alamos
http://int.lanl.gov/publishing/

LANL Password Policy
http://network.lanl.gov/passwords/policy.shtml

CIO Computer Security Handbook
http://int.lanl.gov/cio/htmls/handbook.shtml

Virtual Training Center
http://www.lanl.gov/labview/training/training.html

Badges and Access

Color of Badge	Clearance Level	Access Privileges
Gray	Uncleared (U.S. Citizen)	Access to open areas only - access to unclassified information only.
Yellow	L-Cleared	Access to security areas where work will be done - highest level of information you can access is Secret Formerly Restricted Data.
Blue	Q-Cleared	Access to security areas where work will be done - highest level of information you can access is Top Secret Restricted Data.
Red	Uncleared (Foreign National)	Access to approved open areas only - access to unclassified information only.

Facilities: Access, Protection, Usage, Badges, Visitors, Securing

_ As a group of "strangers" walk unescorted through your workplace, engage or challenge them to determine: their need to be there and how you might help them find their destination.

_ If you are only "pretty sure" you locked the building as the last one out, it will be worth your time and peace of mind to go back and check. You may need a better "lock up system".

_ When at the bank, store, or Dentist's office, your badge should NOT be hanging around your neck. The badge is for Lab business on Lab property. Otherwise stow it, don't show it!

Information: Classification, Document, Vu-Graf, Speech, Media, Passwords

_ Review the documents on your desk before you leave. Different documentation and information require different protection. If you are not sure, find out, before you risk compromise.

_ Use your Authorized Derivative Classifier (ADC) on a regular basis. Develop rapport. Build in the review time. Use S-7 for emergencies or to resolve classification issues.

_ Determine "what" you are working with, who is the audience, and "where" you are going with the project before you choose the media and release the product. Sensitive? Classified?

Communication: Telephone, Cell phone, FAX, E-Mail, Mail, Voice, STU-III

_ If you receive a communication, which looks as though it may be classified, but is not marked as such, report the situation and determine the appropriate actions.

_ Private cell phones for private, non-LANL matters should not come to work, behind the fence. LANL cell phones have rules associated with them and a LANL cell phone user must know and follow these rules.

People: Clearance, Access, Need-To-Know, Escort, Behavior

_ Before the briefing starts and the classified matter is discussed, ensure the audience has both clearance and need to know for the topics to be discussed.

_ Escorting guests through your work area requires your undivided attention. It is NOT appropriate to excuse yourself from the guest for a few minutes and leave the uncleared guest alone in your office to have a short conference in your boss's office. It's not polite either!

Procedures and Policy: Know, Understand, Follow, Uphold, Improve

_ You can't work as quickly with some new policies and procedures, but to ignore them and proceed in the old mode may create a vulnerability for you and the Laboratory.

_ If you have an idea that might help to meet the intent of a security rule and would save time, and money, present it to management. But under no circumstance should you ignore the rule.

Use the back button (◀◀) from the main menu bar at the top of the page to get back to your previous page.

Integrated Safeguards & Security Management

Questions, Concerns, Suggestions Collection & Reporting

General: The worker's voice in ISSM is critical to its success. The data we wish to capture during the initial ISSM rollout and beyond is that which our LANL workers offer to identify questions, concerns or suggestions they have on how to improve security at the Laboratroy. This might include current challenges, best practices, suggestions, and relevant input to the ISSM steering committee for the ISSM path forward. Harvesting the ideas and knowledge of our workforce will only help us to enhance our security performance.

Data Collection Opportunities: Worker ideas and experience will be discussed and collected at:

_ Laboratory All Hands Meeting
_ Division Directors Planning Sessions linking management efforts to Group Workshops.
_ Group or Team level Workshops
_ Individual efforts for those wishing to offer issues or concerns privately or anonymously

Data Collection Methods:

_ Laboratory Director's Open Meeting:
- Facilitators will capture worker comments and issues and forward to Security HELP Desk for analysis / action.
- Security HELP desk access will be encouraged (secure@lanl.gov or 5-2002 Anonymous at Mail Stop K-560)

_ Division Director's meetings linking Director's meeting to Group Workshops.
- Division staff will arrange for capture of ideas and summarize using Division Workshop Report Guide.
- Divisions are encouraged to forward the report after roll up with group reports to the Security HELP Desk for analysis / action. Division should also analyze and address any issue they can at the Division level.

_ Group or Team level Workshops
- Group staff will arrange for capture of ideas and summarize using Group Workshop Report Guide: The report guide covers the types of issues to be included. This report will be forwarded to division for roll-up into division report for division and Security HELP desk analysis / action.
- Individual concerns during these workshops or after the workshops for those wishing to offer issues privately or anonymously.
- Security HELP desk access is encouraged.(secure@lanl.gov or 5-2002, Mail Stop K-560 (Anonymously). NOTE: Ensure that questions that are classified are communicated securely.

Integrated Safeguards & Security Management

Enhancing our Security Performance - - ISSM
Division-level Management Report Guide

Complete this report after all groups in your Division have completed their workshops

Date: _____

Division: _____

Division Leader _____

1. To date, what percentage of workers in your division have completed this training?
2. When do you expect to be at 100% completion?
3. What were the most common questions and concerns raised during the group-level workshops?
4. Which questions, concerns or suggestions for improving security performance are you addressing at the Division level?
5. What are you doing to follow-up on questions, concerns or suggestions that were referred to you?
6. How do you plan to respond to the groups who referred questions, concerns or suggestions to the Division Office?
7. Which issues are you referring for further assistance (to your ALD or DLD)?
8. Which issues are being forwarded to the Security HELP Desk?

Send copies of this report to the ALD or DLD to which you report *and* to the Security HELP Desk (MS K560) by September 15, 2000.

Use the back button (◀◀) from the main menu bar at the top of the page to get back to your previous page.

Integrated Safeguards & Security Management

Questions, Concerns, Suggestions Collection & Reporting

General: The worker's voice in ISSM is critical to its success. The data we wish to capture during the initial ISSM rollout and beyond is that which our LANL workers offer to identify questions, concerns or suggestions they have on how to improve security at the Laboratroy. This might include current challenges, best practices, suggestions, and relevant input to the ISSM steering committee for the ISSM path forward. Harvesting the ideas and knowledge of our workforce will only help us to enhance our security performance.

Data Collection Opportunities: Worker ideas and experience will be discussed and collected at:

_ Laboratory All Hands Meeting
_ Division Directors Planning Sessions linking management efforts to Group Workshops.
_ Group or Team level Workshops
_ Individual efforts for those wishing to offer issues or concerns privately or anonymously

Data Collection Methods:

_ Laboratory Director's Open Meeting:
- Facilitators will capture worker comments and issues and forward to Security HELP Desk for analysis / action.
- Security HELP desk access will be encouraged (secure@lanl.gov or 5-2002 Anonymous at Mail Stop K-560)

_ Division Director's meetings linking Director's meeting to Group Workshops.
- Division staff will arrange for capture of ideas and summarize using Division Workshop Report Guide.
- Divisions are encouraged to forward the report after roll up with group reports to the Security HELP Desk for analysis / action. Division should also analyze and address any issue they can at the Division level.

_ Group or Team level Workshops
- Group staff will arrange for capture of ideas and summarize using Group Workshop Report Guide: The report guide covers the types of issues to be included. This report will be forwarded to division for roll-up into division report for division and Security HELP desk analysis / action.
- Individual concerns during these workshops or after the workshops for those wishing to offer issues privately or anonymously.
- Security HELP desk access is encouraged.(secure@lanl.gov or 5-2002, Mail Stop K-560 (Anonymously). NOTE: Ensure that questions that are classified are communicated securely.

Integrated Safeguards & Security Management

Enhancing our Security Performance - - ISSM
Group-level Management Report Guide

Complete this report when at least 80% of the group members you expected to attend the group-level workshops have completed the workshops or have been briefed individually.

Date: _____

Division: _____

Group: _____

Group Leader: _____

1. How many people in your group were expected to complete this workshop?

2. To date, how many of those have completed the workshop?

3. What are you doing to follow-up with those who have not yet completed the workshop?

4. What questions or concerns did your staff raise during the workshop?

5. What suggestions for improving security practices were made during the workshop?
   - Start with any that you have been able to implement within your group.
   - Include suggestions that could help other groups in your Division or Lab-wide.

6. What questions or concerns did you defer (could not be answered or addressed during the workshop)?

7. What will you do to follow-up on any questions, concerns or suggestions raised during the meeting that could not be resolved at that time?
   - Include how you plan to keep the group informed on how their questions, concerns or suggestions are addressed.

8. What suggestions for improving security do you need assistance with or additional resources to implement?

9. What further information about your group workshop would you like to share?

Send to your Division Office by August 31, 2000.

Use the back button (◀◀) from the main menu bar at the top of the page to get back to your previous page.

Integrated Safeguards & Security Management

ISSM Individual Performance Objectives Worksheet

Directions: Use the **ISSM Five Step Process to identify** roles, responsibilities, and performance objectives you might use in the future in your performance plan.

Based on workshop discussion, what security insights have you gained as applied to your work?

_____
_____
_____
_____
_____

How will you incorporate these insights into your daily work?

_____
_____
_____
_____
_____

What are your duties involving security? (Some concepts to help with the inventory: Badge? Property? Keys? Passwords? Security Container? Physical Security – Your Office, Building? Cell Phone? Sensitive Data? Classified Information? Visitors?)

_____
_____
_____
_____
_____

How would you best accomplish these duties and what are the performance objectives associated with these duties /tasks?

_____
_____
_____
_____
_____

By Applying the 5-Step Process, you will be able to answer the following questions:

1. Are your work and workplace secure?
2. How do you know?
   - Do you know the security requirements governing your work/workplace and how they are being met?
   - Do you know the security vulnerabilities in your work/workplace and whether controls are sufficient to mitigate them?

Case Studies

Case Studies:
Scenarios Based on Actual Incidents

Directions

Select case studies that are relevant to the work in your group, and continue the discussion on application of the ISSM 5-step process.

Lab-Wide Security Issues

- Vu-Graph Classification
- Badges
- Suspicious Packages
- Passwords
- Faxing
- Foreign Visits
- Theft
- Sensitive Unclassified
- “Unclassified” Processing
- “Unclassified” Presentation
- TSCM

Area Access

- SNM Material Access Area (MAA)
- Foreign Visits & Assignments

Case Studies:
Scenarios Based on Actual Incidents (cont.)

Classified Information

- Accountable Classified
- Misplaced Classified
- Copying Classified Information
- Classified Data Transfer
- Classification
- Shredding Materials
- E-mail
- Excess Material
- Classified Faxing
- Security Containers

Case Studies:
Scenarios Based on Actual Incidents (cont.)

Lab-Wide Security Issues

Vu-Graph Classification:

Scenario: Derivative Classifer Review

Circumstances: You create a view graph and have your derivative classifier review the content. It is not classified. Several days later you make a few modifications and ask your uncleared administrator to put the content into Power Point with a lead and closure slide as well. Someone sees the presentation and declares that it is classified. Your derivative classifier agrees. The changes you made were enough to change the classification.

Badges:

Scenario: Wearing Badge in Public Places

Circumstances: You see a fellow LANL employee in a bank in town with her badge clipped to her collar. She has the yellow PSAP appliance / clip showing as well.

Case Studies:
Scenarios Based on Actual Incidents (cont.)

Lab-Wide Security Issues (cont.)

Suspicious Packages:
Scenario: Suspect Briefcase or Package Unattended in Your Office
Circumstances: You see a package in the hallway just outside your office door. There is no tag or identification on the package.

Passwords:
Scenario: Shared Password.
Circumstances: Fred is on vacation, and he has been working on a document from which you need some information for the boss. You mention your frustration to a coworker and she says "I can get that for you. I know Fred's password."

Faxing:
Scenario: Fax Error
Circumstances: You have just faxed a six-page document on an unclassified Fax machine and the completion report indicates there were seven pages. As you look through the document you find a page in the middle marked Secret.

Case Studies:
Scenarios Based on Actual Incidents (cont.)

Lab-Wide Security Issues (cont.)

Foreign Visits:
Scenario: Foreign Visit Rules
Circumstances: You are the host for a foreign visitor who will arrive tomorrow. You receive a priority letter and an e-mail stating that the original visitor, Bill, will not be coming, and James will now be coming in his place.

Theft:
Scenario: Possible Theft of Government Property
Circumstances: You are a team leader, and one of your employees advises you that a fellow team member has been leaving work each evening with briefcase in one hand and a box in the other arm.

Sensitive Unclassified:
Scenario: Protection of Sensitive / Unclassified Information
Circumstances: During closure and lock-up of your building, you discover a list of employees in the recycle bin. The list includes Z numbers and other numbers in a column marked “performance rating.”

Case Studies:
Scenarios Based on Actual Incidents (cont.)

Lab-Wide Security Issues (cont.)

Sensitive Unclassified # 2:

Scenario: Protection of Sensitive / Unclassified Information

Circumstances: As you are making copies, you see the division budget and a list of mission impact statements in the trash can beside the copier. Some of these impacts involve reduction in the number of employees and inability to properly secure materials.

Unclassified Processing

Scenario: Processing Classified on Unclassified Computer

Circumstances: You are processing data on your unclassified computer. After saving your work, you notice that you typed classified information on your unclassified system.

Case Studies:
Scenarios Based on Actual Incidents (cont.)

Lab-Wide Security Issues (cont.)

Unclassified Presentation

Scenario: Presentation Turns Classified

Circumstances: You are attending a presentation and the slides being presented are unclassified. However, during the presentation the presenter verbally presents material you know is classified.

TSCM

Scenario: Cell Phones in Security Areas

Circumstances: After entering a security area, you notice that you have your personal cell phone with you.

Case Studies:
Scenarios Based on Actual Incidents (cont.)

Area Access

SNM Material Access Area (MAA):
Scenario: Improper Access
Circumstances: You and a coworker enter an area which requires a minimum of two people entering the area together for access to that area. You discover a worker working alone in the area.

Foreign Visits:
Scenario: Foreign Visit Escort
Circumstances: You are the host for a group of seven foreign visitors. You are giving a tour in a security area, and you and another escort discover one of the guests has wandered away from the tour.

Foreign Visits & Assignments:
Scenario: Foreign Visit Escort
Circumstances: You are working in a security area and you encounter a visitor with a red badge who should be under escort. You know this, as it was just announced on the loudspeaker. The visitor is walking around without an escort.

Case Studies:
Scenarios Based on Actual Incidents (cont.)

Classified Information

Accountable Classified:

Scenario: Control of Accountable Classified Material

Circumstances: Alice passes an accountable classified document which is stored in her safe to Bill, and after using it, Bill stores the document in his safe. Later the classified document custodian (CDC) performs an inventory, and the document is not found in Alice's safe.

Misplaced Classified:

Scenario: Control and Location of Classified Material

Circumstances: You open your safe to look for a document you created. You can't find it. You remember that you think you may have given it to Joe to critique for you. Or was it Larry? Joe says, "I remember it. I made comments on it, but gave it back to you last month." Larry is on vacation.

Case Studies:
Scenarios Based on Actual Incidents (cont.)

Classified Information (cont.)

White-Board Copier:

Scenario: Copier, White Board.

Circumstances: You have a classified drawing of a security component for a new building design and you are presenting the drawing to a group of workers and are using a white board in a limited-area conference room. As you draw the design on the white-board (which is capable of making copies) and make a copy for each participant, you recall that you have done this before and have seen others do the same. You realize the white-board copier has not been certified for classified copying.

Xeroxing Classified Documents

Scenario: Classified Document Found on Copier.

Circumstances: A classified document is found on the copying machine. What responsibility does the person have if 1) he knows who owns the document and returns it to the person, 2) he knows the group that owns the document and returns it to the group office, or 3) he does not know the owner of the document?

Case Studies:
Scenarios Based on Actual Incidents (cont.)

Classified Information (cont.)

Xeroxing Classified Documents:

Scenario: Classified Document Lost in Jammed Copier.

Circumstances: You are copying classified material on an approved copier in a secure area. The copier jams. You remove what you think is the jam, but the copier still will not function. What should you do? Subsequently, another individual finds material that is marked classified jammed in the copier.

Classified Data Transfer:

Scenario: Data Transfer between Different Forms of Media

Circumstances: You are working late and are just about to leave for an appointment. You are in fact a bit late. Coworker Bill, the only other employee in the building, asks you to observe as he transfers classified data from his hard drive to his A:/ drive. You explain you can't but will help first thing in the morning. When you come in the next day you offer to help but Bill says "It's O.K. I did it last night."

Case Studies:
Scenarios Based on Actual Incidents (cont.)

Derivative Classifier

Classification:

Scenario: Classification of a Document

Circumstances: You have just completed a memo for your counterpart at DOE, and you are not sure if the document is classified. You think it might be. Your group has two authorized derivative classifiers (ADCs) but one is on vacation and the other is on travel.

Shredding Materials:

Scenario: Destruction of Sensitive or Classified Materials by Shredding

Circumstances: You are a team leader, and the building custodian comes to you with a bag of shredded paper he was taking to the dumpster. You can see that he has discovered a partially shredded document with complete classified paragraphs still legible.

Case Studies:
Scenarios Based on Actual Incidents (cont.)

Derivative Classifier (cont.)

E-Mail:
Scenario: E-Mail Error
Circumstances: You have just received an e-mail from a co-worker who is on travel in Washington, DC . As you read the e-mail, you discover that it contains classified material.

E-Mail:
Scenario: E-Mail Error
Circumstances: A staff member is collaborating with a colleague from the United Kingdom Atomic Weapons Establishment. The colleague sends e-mail that he/she believes is unclassified, but you know it to be classified by DOE standards. What do you do?

Excess Material:
Scenario: Excess Classified Material
Circumstances: You are assigned to a position of a coworker who has retired, and you inherit her office and safe. You discover "volumes" of marked and unmarked documents, all of which you believe to be classified. Much of the material is 12-14 years old.

Case Studies:
Scenarios Based on Actual Incidents (cont.)

Derivative Classifier (cont.)

Classified Faxing:

Scenario: Fax Error

Circumstances: You have just received a Fax document on an unclassified Fax machine. As you read the document, you know that it contains classified material.

Security Containers:

Scenario: Security Container Left Open.

Circumstances: As you are working late one evening, you see a two-drawer safe in an open office down the hall from your office. It is in a limited area, and it is 6:30 p.m. The safe has a "LOCKED" sign on it, but the lower drawer is open about 3 inches.

Case Studies:
Scenarios Based on Actual Incidents (cont.)

Derivative Classifier (cont.)

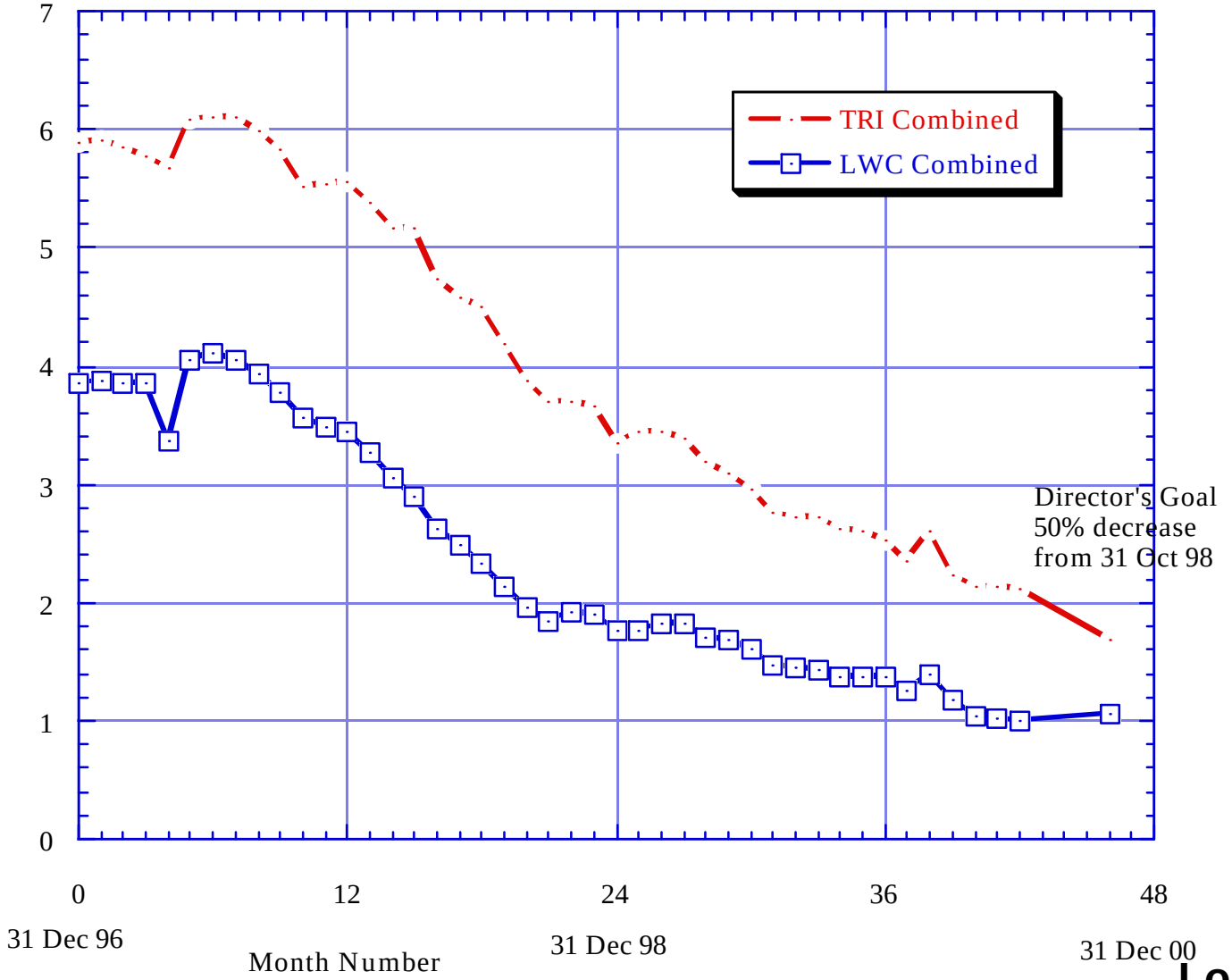
Security Containers:

Scenario: Security Container Check.

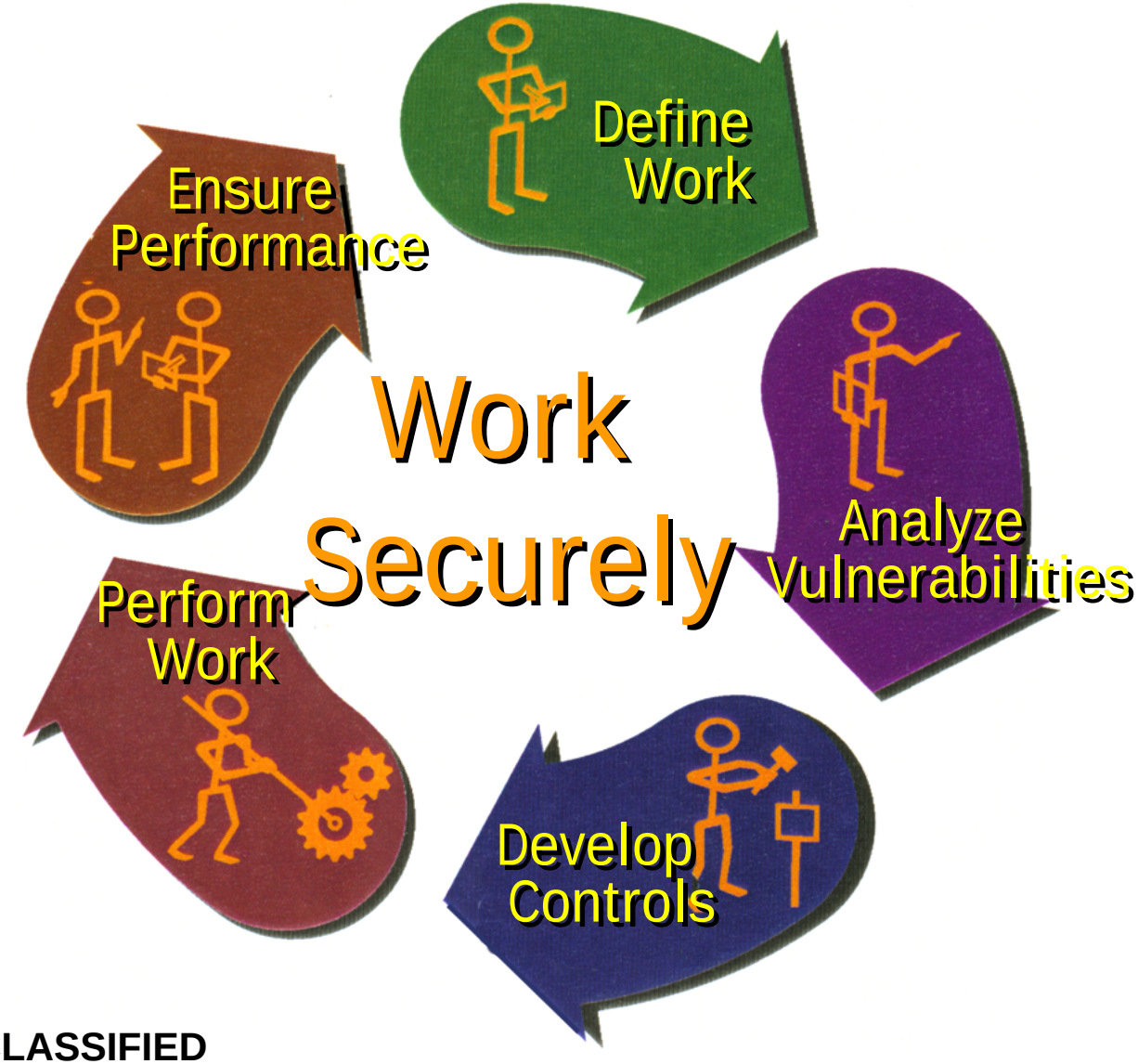
Circumstances: A safe checker spins the dial on a “locked” safe but fails to pull the drawers. Subsequently, a security guard pulls on the drawer, and it opens. It is discovered that the safe has had a mechanical failure. Can the owner of the safe get a security infraction? Can the safe checker receive a security infraction? What if there is no written procedure for safe checking?

Safety and Security are everyone's job

ISM has led to significant improvement



Integrated Safeguards and Security Management



Director's "All Hands" Meeting

Enhancing Our Security Awareness, Commitment and Performance

- *Integrated Safeguards and Security Management* (ISSM) Workshops -

Jon Weisheit

July 18, 2000

Director's Expectations

ISSM Objective:

Systematically integrate security into all work practices at all levels so that the Laboratory mission is accomplished cost effectively and safely, *while protecting security interests and striving for "ZERO safeguards and security incidents"*

Director's Expectations

- The Laboratory will stay the course with ISSM
- Security must be incorporated into the way we do business if we are to succeed
- Everyone must take security seriously and do whatever they can to ensure their workplace is incident free
- Everyone must actively participate in the ISSM workshops

Tailored ISSM Workshops

Post-Kickoff Events:

- Division-level management planning sessions
- Group-level “all hands” ISSM workshops
- Group results reported to division-level director
- Division results reported to cognizant ALD/DLD
- All employees (including managers) review their security responsibilities with their supervisors

Tailored ISSM Workshops

Division-level management planning sessions:

Each division-level director convenes their management team to review John Browne's expectations and tailor their workshop approach to their organization's scope of work (tasks, security assets, issues, and concerns) to maximize the benefit to each worker and to their overall organization.

Where practical, division-level directors are also encouraged to help launch the subsequent group-level ISSM workshops by first calling an "all hands" meeting and/or by kicking off each group-level workshop.

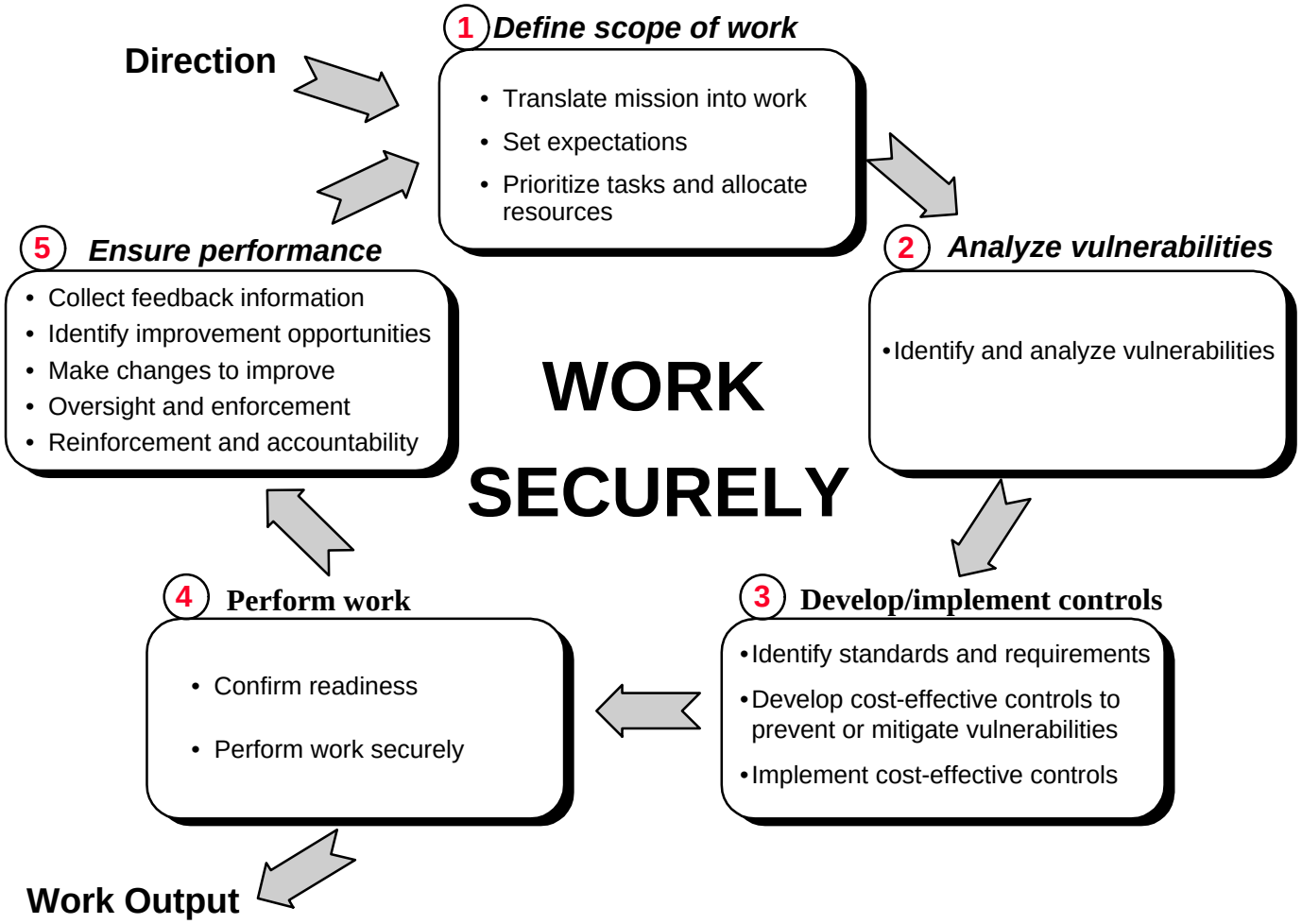
Tailored ISSM Workshops

Group-level "all hands" ISSM workshops:

Each group-level manager leads a highly-interactive ISSM workshop in the next few weeks to review John Browne's expectations and conduct tailored exercises aimed at learning and applying the ISSM five-step process for improving security. Questions, concerns, and suggestions will be collected for follow-up action.

Attendance will be tracked/reported. Trained facilitators will be available. (Note: Large groups may conduct their workshops at the team level, then rollup their results.)

ISSM Process



Tailored ISSM Workshops

Group results reported to division-level director:

Group-level managers will summarize/document by August 31, 2000, for their division-level directors all security questions, concerns, and suggestions raised during their workshops, including their planned follow-up actions.

Managers are accountable for responding to all questions, concerns, and suggestions, seeking help as needed from their security representatives (OSSOs, OCSRs, CDCs, etc.) and the new Security Help Desk (5-2002, secure@lanl.gov).

Tailored ISSM Workshops

Division results reported to cognizant ALD/DLD:

Division-level directors will summarize/document by September 15, 2000, for their supervisor all security questions, concerns, and suggestions raised during all their workshops, including their planned follow-up actions. They will copy their report to the new Security Help Desk.

Managers are accountable for responding to all questions, concerns, and suggestions, seeking help as needed from their security representatives (OSSOs, OCSRs, CDCs, etc.) and the new Security Help Desk (5-2002, secure@lanl.gov).

Workshop Resources

- For help, contact the new Security Help Desk at 5-2002 or secure@lanl.gov
- Get support from your designated security representatives (OSSOs, OCSRs, CDCs, etc.)
- Go to the new “ISSM” web site under “Security” on the Lab homepage for ISSM info and click on “ISSM Workshops” for specific guidance/tools

ISSM Website

ISSM Workshop Website

Tailored ISSM Workshops

All employees (including managers) review their security responsibilities with their supervisors:

After the workshops, all employees will meet one-on-one with their supervisors to review their security responsibilities. This should be reflected in the development of individual performance objectives for 2000-2001.

Managers should promote, recognize, and reward valuable security improvement insights and suggestions.

The Bottom Line

- ***Everyone working at the Laboratory is responsible for security!***

- ***We must never compromise safety or security for operational needs!!***

ISSM Update

June 27, 2000

Laboratory Information Meeting

Carl Ostenak, LANL DIR/S-DO ISSM Leader

- Central Message -

Progress Is Well Underway BUT

Accelerating ISSM Would Be Beneficial!

- <u>Top Priority</u> -

Senior Management Committed to Extend the ISM Model to Safeguards & Security

(J. Browne, R. Atkinson, R. Glass, G. Podonsky, Gen. Habiger)

Topics

- Background
- Current Status
- Path Forward

Background -- Why ISSM?

Strong Security Performance Requires a Strong Security Culture:

- **ISM Strengthened Our ES&H Culture**
  - Total recordable injuries down by factor of three
  - Pushing “best in class”
- **Extending ISM Model to Security Offers Similar Benefits**
  - Stronger security culture
  - Stronger performance (“ZERO Violations”)
  - Greater public confidence/trust
  - Common management model for cost-effective operational excellence (ES&H and S&S)

Background -- Why ISSM?

Two Imperatives for ISSM:

- ***Moral Imperative*** - We must not compromise the "safety of our nation."

- ***Business Imperative*** - We must cost-effectively meet our contractual security requirements.

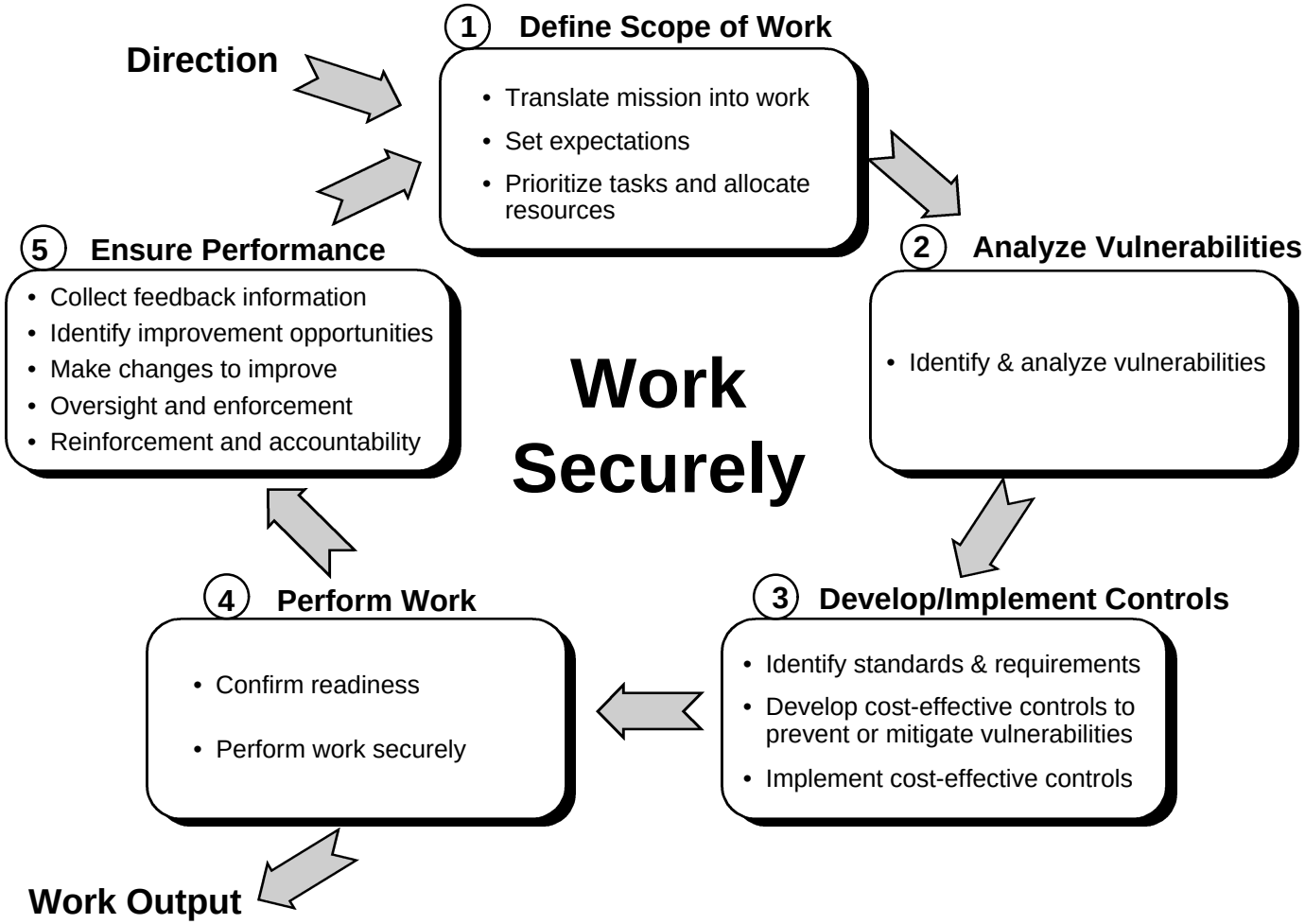
Background -- What Is ISSM?

ISM Basic Tenets Are Fundamental to ES&H <u>and</u> Security:

- ***<u>Eight Guiding Principles</u>*** **- Management commitment, workforce involvement, line "ownership," clearly defined roles/responsibilities, work/worker authorization, etc.**

- ***<u>Five-Step Process</u>*** **- Define scope of work, etc.**

Background -- What Is ISSM?



Background -- What Is ISSM?

1 Institutional

UC-DOE Contractual Security Requirements

↓

Lab Performance Requirement (1 Total)
(LPR/"What")

↓

Lab Implementing Requirements (3 Total)
(LIR/"How")

↓

2 Facility

Facility-Level Security Requirements
(Facility Security Plans/SSSP)

↓

3 Activity

Activity-Level Security Requirements
(Activity Security Plans)

Current Status -- Accomplishments

Completed ISSM Actions:

- Dick Burick/DLDOPS Appointed ISSM Champion
- Carl Ostenak/S-DO Appointed ISSM Leader
- UC Launched Tri-Lab (LANL, LLNL, LBNL) ISSM Initiative
- Established X-Cutting (Line/Program/Support) Joint LANL-DOE ISSM Steering Team/Charter
- Developed ISSM Concept, Gained SET & OWG Approval, Briefed LIM & All Managers (3-13-00)

Current Status -- Accomplishments

Completed ISSM Actions (Cont'd):

- Developed Draft ISSM Description Document
- Developed Draft ISSM LPR
- Developed Streamlined/Simplified LIR Approach (3 Total)
- Launched 2 of 3 Line/Program/Support LIR Focus Teams
- Recently Developed Proposal for DIR-Launched ISSM Security Awareness/Commitment Workshops
- Recommended Additional Actions for Accelerating ISSM

Current Status -- Steering Team

Joint LANL-DOE ISSM Steering Team:

- Dennis Brandt, NMT-4
- Bob Day, DX-DO
- Sharon Eklund, S-1
- Richard Kendall, CIC-DO
- Kevin Leifheit, S-2
- Lee McAtee, ESH-DO
- Evelyn Mullen, NIS-DO
- Carl Ostenak, DIR ISSM Leader, Chair
- Susan Seestrom, P-DO/LANSCE
- Phil Thullen, DIR ISM Leader
- Frank Ward, DOE/LAAO
- Joel Williams, NW-M&M

Current Status -- ISSM Charter

Joint LANL-DOE ISSM Steering Team Charter:

- **Develop/Rollout "Straw" ISSM Concept to the SET, OWG, and at LIM and All Managers' Meetings**
- **Develop/Implement a Lab-Wide ISSM Communications and Workforce Involvement Strategy**
- **Create/Publish/Track an ISSM Description Document and Cost-Effective Implementation Plan (Issue CY00)**
- **Develop a Truly Integrated Operations Management (IOM) Model (IOM=ISM+ISSM+?) for Achieving Cost-Effective Operational Excellence (Target CY01)**

Path Forward -- Recommendations

Additional Actions for Accelerating ISSM:

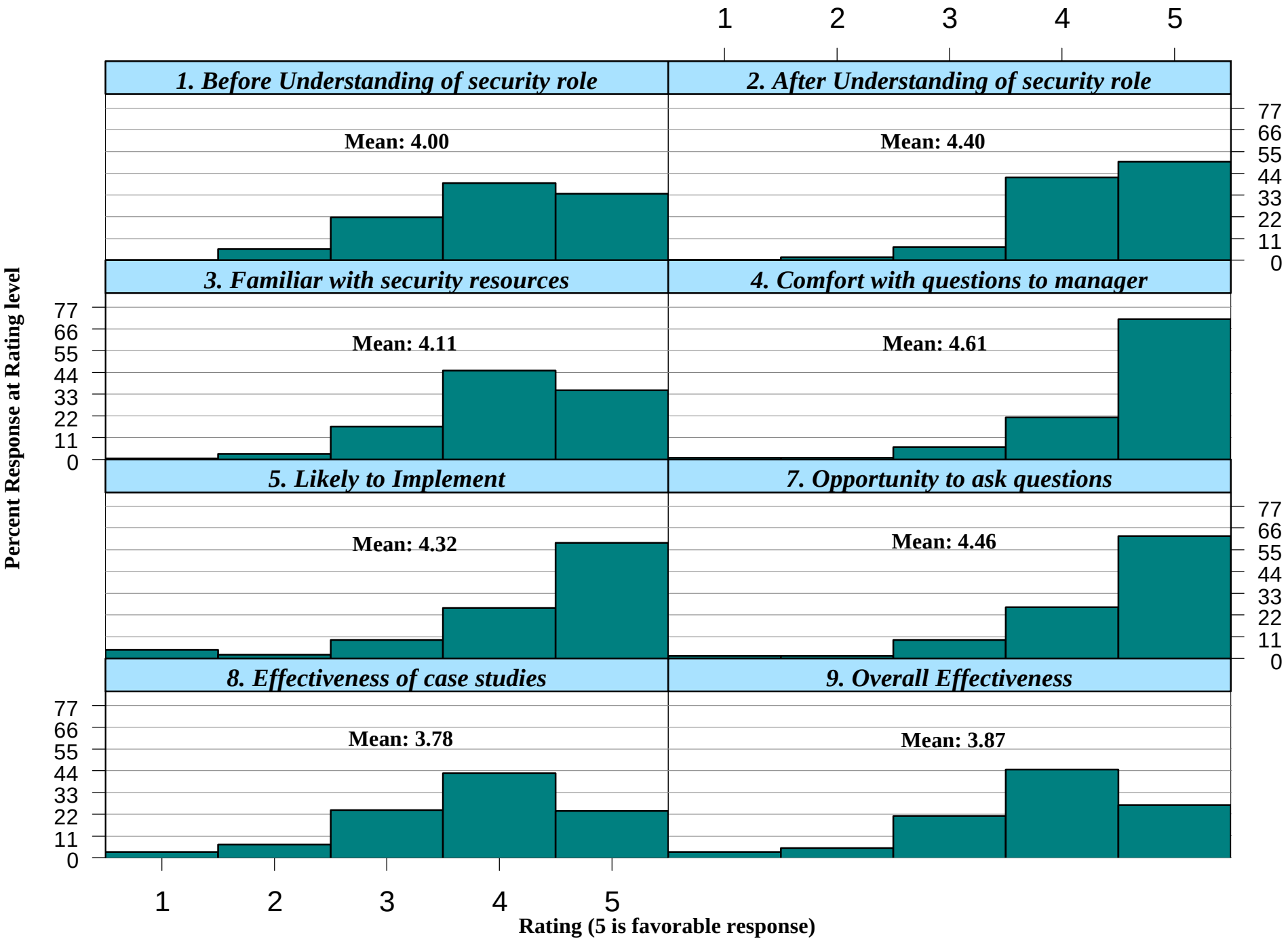
- Begin All LANL Meetings with "Safety <u>and</u> Security First!"
- Approve/Publish New "Safety and Security Policy."
- Approve/Publish New ISSM LPR
- Expedite Completion of the ISSM Description Document
- Expedite Completion of the three ISSM LIRs
- Use New "ISSM Help Desk" and secure@lanl.gov.
- Use Management Walk-Around Program for Security
- Invite Preeminent Security Experts for DIR Colloquia
- Include Security Job Factor in 2000-2001 Performance Plans
- Require Security Infractors to Brief Lab Director/SET

- Bottom Line -

Strong Security Performance Requires a Strong Security Culture!

Your Active Support and Involvement Are Vital for Success!

ISSM Group-level Workshops Evaluation



(507 respondents from random sample of 1000 workshop participants)

Laboratory ISSM Rollout "Progress Chart"

Organization	Jul 18 '00 Division Attended (or subsequently made up) Director John Browne's July 18 "All Hands" ISSM Meeting	Division-level Director Led "All Managers" ISSM Workshop Planning Session for Their Division	Division-level Director Led "All Hands" ISSM Meeting for Their Division (optional)	Group-level Managers Identified "Target Audience" for Their ISSM Workshops	By Aug 31 Group-level Managers Led Their ISSM Workshops	By Aug 31 Documented/Reported Attendance for Group-level ISSM Workshops	By Aug 31 Submitted Group-level Summary Reports to Cognizant Division-level Director, Including Unresolved Questions, Concerns, Suggestions	By Sept 15 Submitted Division–level Summary Reports to Cognizant ALD or DLD, Including Unresolved Questions, Concerns, Suggestions	By Oct 15 Division Management Team Informed Their Workforce of Actions Taken and/or Underway on Submitted Questions, Concerns, Suggestions	By Nov 30 Completed 1-on-1 Employee/Supervisor Meetings to Establish a 2000-2001 Individual Performance Objective (IPO) for ISSM/Security Responsibilities
AA										
B										
BUS										
C										
CCN										
CCS										
CER										
DIR										
DVO										
DX										
E										
EES										
ESA										
ESH										
ESS										
FWO										
HR										
IBD										
IM										
ISEC										
JCNNM										
LANSCE										
LC										
MST										
NIS										
NMT										
NW										
OEO										
OMBUDS										
P										
PM										
PTLA										
QIO										
S										
SNS										
SSR										
STB										
T										
TR										
TSA										
X										

Integrated Safeguards & Security Management
UPDATE

Security Help Desk 5-2002

January 18, 2001 VOL. 1, NO. 2

The ISSM Update Bulletin purpose is to share security guidance & clarification to LANL users.

NEWS:

This is the second set of Q&A's that were primarily generated from individual ISSM Rollout Workshops. These questions and the respective answers were reviewed by Security professionals and will be available in a searchable format on the web in the near future. This printable document is one of the methods we will use to notify you of our progress answering peoples' questions, concerns and suggestions. If you have any questions, please contact the Security Help Desk at 5-2002.

Contents:

S&S Policy and Funding	1
S&S cultural change, accountability, and lessons learned	2
S&S Management Walkarounds	2
Safety & Security First	3
ISM/ISSM Integration	3
CIC	4
OUO	4
MC&A	4
Training	5-7

S&S Policy and Funding

Q: Eight organizations had concerns about what's being done to ensure practical, value-adding, and adequately funded safeguards and security requirements?

A: The success of Integrated Safeguards and Security Management (ISSM) is heavily dependent on creating Lab-wide buy-in through active workforce involvement in streamlining and integrating internal safeguards and security requirements, tailoring safeguards and security controls, and establishing clear line (vs. support) safeguards and security ownership. Moreover, when external safeguards and security requirements are identified that appear to add little or no value, the Lab must work closely with DOE's new National Nuclear Security Administration (NNSA), which now "owns" the Lab, to seek relief so we can jointly achieve safeguards and security objectives in a defensible, efficient and cost-effective manner.

To this end, the Lab has had some real success working with DOE, and now NNSA, through joint committees such as the Site Safeguards and Security Plan Change Control Board and the Materials Control & Accountability Senior Steering Group. These efforts promote practical, value-adding, and adequately funded direct funding of safeguards and security are intended to eliminate traditional unfounded mandates and promote more prioritization and integration of safeguards and security requirements and resources throughout DOE, including NNSA. Additionally, the NNSA is now designated as the single (vs. DOE's traditional multiple) source of external safeguards and security requirements that flow into the Lab and has committed to solicit "feedback" from the Lab in developing policy.

S&S cultural change, accountability, and lessons learned

Q: Thirty-two different organizations had concerns about what's being done to make the Lab-wide cultural change necessary for effective safeguards and security, including fair and effective personal accountability and sharing of lessons learned?

A: Integrated Safeguards and Security Management (ISSM) is well underway thanks to outstanding Labwide participation in highly interactive and tailored ISSM workshops conducted last summer. Workforce feedback has been very favorable. Participants learned to apply the ISSM 5-step process and openly shared their security questions, concerns, and suggestions. Among the common concerns, much of the workforce is asking for more effective institutional processes to:

- Promote continuous security awareness
- Reinforce and reward positive security behaviors
- Promote trust in self-reporting near misses/incidents
- Ensure root-cause analysis and capture and communicate lessons
- Ensure real, visible fairness in assigning and adjudicating infractions
- Track trends and report meaningful performance metrics.

As a result, a large, cross directorate ISSM Positive Security Behaviors Team was established by Carl Ostenak, ISSM Program Manager, to critically examine each of these related concerns and recommend specific process improvements aimed at addressing them. The team is chaired by Ed Heighway, Physics Division Office, and includes workers and managers from technical divisions across the lab, the Diversity and Ombuds Offices, and the Employee Advisory Council. Although the team represents all major security interests at the lab (classified processing, special nuclear materials, special access programs, etc.), Lab-wide input is welcome. Employees are encouraged to send their input to the Security Help Desk (mailto:security@lanl.gov) ATTN: ISSM Positive Security Behaviors Team. "Your voice is critical to the success of ISSM," said Ostenak.

S&S Management Walkarounds

Q: How does management plan to make their commitment to safeguards and security more visible to workers?

A: Several actions are already underway, beginning with last summer's Integrated Safeguards and Security Management (ISSM) workshops. The workshops involved the active participation of all workers (both non-managers and managers), and continues with managers actively encouraging workers to help develop ISSM. Several employees are now working on highly integrated and streamlined sets of three safeguards and security LIRs to replace currently documented Lab security requirements found in numerous master management memos, manuals, etc., because they are viewed as fragmented, often conflicting, and otherwise user-unfriendly. Additionally, all managers will soon be routinely performing security management walkarounds (MWAs) under ISSM just as they do for safety under ISM. These MWAs will be highly visible to workers because they are aimed at directly interacting with workers in the workplace, including observing security behaviors and conditions and promoting continuous security awareness and improvement.

Safety and Security First

Q: Shouldn't both safety and security be first at all group and higher level meetings at the Lab?

A: Since last summer, an increasing number of groups, divisions, and directorates are beginning their meetings with "Safety and Security First" (vs. only Safety First). Senior management has expressed and modeled this expectation by now beginning all Laboratory Information Meetings (or LIMs, which are weekly senior management meetings) as well as "All Managers" and "All Employees" meetings with "Safety and Security First". As with safety, this simple action can pay huge dividends in terms of enhancing security awareness and promoting positive security behaviors. Moreover, in the final analysis, safety and security have a common objective—protecting people and the environment. Indeed, the loss of classified information and/or special nuclear material can put our national security (i.e. national safety) at risk. This is why U. S. National Security Council policy begins with, "To ensure the safety of our nation, the U.S. will continue its integrated approach to addressing the numerous threats to our interests and preserve a full range of foreign policy tools..."

ISM/ISSM Integration

Q: Does the ISSM acronym have two translations?

A: Yes—perhaps the best known (but not first) translation of DOE's ISSM acronym is "Integrated Safeguards & Security Management", which is routinely used even at the highest levels in DOE. Indeed, General Gordon, who leads DOE's new National Nuclear Security Administration and therefore "owns" the three nuclear weapons Labs (LANL, LLNL, and SNLA), uses and is fully committed to this meaning for ISSM as are the directors of the three weapons labs and the UC President Richard Atkinson. However, DOE also uses the ISSM acronym to mean "Information Systems Security Site Manager". Although not ideal, this certainly isn't the only acronym in the DOE Complex having two or more translations. The important thing is to minimize confusion by defining the specific use of an acronym whenever it's presented.

Q: Five different organizations had questions about whether ISM and ISSM eventually will be integrated into a single model for managing work.

A: Both Integrated Safety Management (ISM) and Integrated Safeguards and Security Management (ISSM) are ways of doing business, and the focus of the business is work. Integration means that safety and security must be an integral part of all work planning, performance, assessment, and improvement. This common objective will ultimately drive the establishment of a single management model for managing work. To this end, the Lab's more mature and highly successful ISM model is being extended to safeguards and security (or "security", more generally). Director John Browne launched this new initiative in early CY00 because ISM's basic tenets—management commitment, worker involvement, line "ownership", clearly defined roles, responsibilities, authorities, and accountability, work and worker authorization, self-assessment, continuous improvement etc.—are vital to the success of both safety and security at Los Alamos. Pursuing this new ISSM initiative offers not only a stronger Lab-wide security culture and enhanced security performance, but a path forward for establishing a single management model for achieving cost-effective operational excellence (safety and security).

CIC

Q: Smart Card orientation needs to be reviewed and possibly revamped to better educate the holders of their responsibilities.

A: This suggestion has been addressed with IM-5, who will be re-evaluating the Smart Card orientation.

OUO

Q: Social Security Numbers are not to be used for identification purposes, however some (medical) testing equipment requires the use of SSNs to perform the test. Also, some vendors require SSNs for tracking purposes.

A: Please refer to the UC Business & Finance Bulletin, RMP-8, LEGAL REQUIREMENTS ON PRIVACY OF AND ACCESS TO INFORMATION, Section III, Federal Privacy Act of 1974, located at the following web site: http://www.ucop.edu/ucophome/policies/bfb/rmp8.html

In particular, Section III states,
III. FEDERAL PRIVACY ACT OF 1974
The Federal Privacy Act is primarily directed to Federal agencies for the purpose of protecting the privacy of individuals identified in information systems maintained by such Federal agencies. Except with respect to social security numbers, the Act applies to the University only in the few instances when a contract (not a grant) is entered into obligating the University to operate a system of records on behalf of a Federal agency in order to accomplish a Federal agency function. "System of records" includes any group of records from which information is retrievable by name of an individual or some identifying number, symbol, or other identifying particular assigned to the individual.
Regarding use of social security number, the Federal Privacy Act does pertain to the University. Section 7(b) of the Act is applicable to any Federal, State, or local governmental agency. In accordance with Section 7 (b), if the University requests an individual to disclose his or her social security number, it must inform that individual whether such disclosure is mandatory or voluntary, by what statutory or other authority the number is solicited, and what uses will be made of it. Furthermore, the University may not deny any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his or her social security number unless, (a) the disclosure is required by Federal statute, or (b) the disclosure is required in relation to a system of records maintained by the University in existence and operating before January 1, 1975, and if such disclosure was required by statute or regulation adopted prior to that date to verify the identity of an individual (Sample Federal Privacy Notices are attached as Exhibit A.). For further information contact Judy Rose Archuleta, IM-5, at 667-4515.

MC&A

Q: Does a Category III area require a PSAP clearance?

A: At LANL a majority of the Category III nuclear Materials Balance Areas (MBAs) lay outside of the protected areas. In cases involving these MBAs an individual with an L or Q clearance is all that is required. However, in circumstances involving Category III MBAs located within a nuclear Material Access Area (MAA) (i.e. PF-4) where only properly cleared and authorized personnel are permitted unescorted access to Category I special nuclear material a Q clearance and PSAP is required.

Training

Q: What happened to standardized cyber-security training for System Administrators and why is Cyber security information not disseminated in an organized fashion at LANL by CIC?

A: Several courses were offered to system administrators at the Laboratory in 1999 and early 2000. The courses were sponsored by DOE and presented by an off-site vendor in response to the Laboratory's 1999 Nine Point Computer Restart Plan. CCN Division is analyzing the needs of system administrators throughout the Laboratory in order to design an on-going, comprehensive certification program. Your Organizational Computer Security Representative (OCSR) is your primary contact for getting the latest computer security information. However, computer security information is disseminated to Laboratory workers in a variety of ways, including formal training and through Organizational Safeguards and Security Officers (OSSOs).

Q: Two Organizations had concerns about S&S Training, and what was in them as far as what employees should do, vs. what employees should NOT do.

A: Roles and responsibilities are included in all safeguards and security training courses as are regulatory drivers for the programs. These drivers are a reference for workers to have a better idea why they are being required to take the training. As we design on-line courses, we are coming up with more menu/learner driven designs to allow you, as a worker, to steer your own learning path through the course. Some material must be presented without the option to skip over it; however, with the new designs you should have more options as to how and when you access the information. Although there are several courses designed for the entire Laboratory or a large majority thereof, some security training programs are designed for very specific audiences. As such, we work at tailoring the information to best meet the needs of our diverse audience characteristics while also preserving the intent and requirements set by DOE.

Q: Four different organizations brought up issues concerning initial security briefings when a person receives their clearance.

A: A Comprehensive Briefing for workers is offered when a Q or L clearance is granted or a clearance has been reinstated after 11 months or more. The course (#8480) is a live briefing offered twice weekly and covers the protection and control of classified and sensitive unclassified information; security access authorization and access control; targeting and recruitment methods for intelligence services; and classification procedures. An annual refresher is required thereafter and is offered as an on-line training. For additional information on attending the comprehensive briefing or where refresher training is located on the web contact the S-Division Training Team at 7-7565.

Q: LANL employees need more training concerning security issues, especially handling of classified documents and escort procedures.

A: Training is offered for both Handling of Classified Documents http://www.hr.lanl.gov/SCOURSES/LANL/CLASSIFIEDMATTER/PAGE01.asp. as well as for Escort Responsibilities http://www.hr.lanl.gov/sources/lanl/EscortDuty-US/page01.asp. S-Division has established a web site which lists all security courses offered at the Laboratory and how to get them. http://int.lanl.gov/orgs/s/training/required-training.shtml

Training (Continued)

Q: How can we determine if everyone has completed escort training? When the Group Leader signs the 1812, how can they know that the escort has been trained appropriately?

A: Each individual that properly completes a course is credited. Organizations can then run reports through datawarehouse or IB showing which of their employees have completed the course. If you are unfamiliar with those systems, your organization's Designated Training Generalist (DTG) should be able to assist you.

Q: I have been surprised over the last few years at how little security training has been required, even with a Q-clearance. The on-line courses are an excellent delivery method. It would be better if the requirement were some topic once every three months rather than a marathon once a year (which is admittedly easier to manage). Perhaps a requirement (with automatic e-mail reminder) that allows the cleared individual to select the most relevant of the available training once per quarter would keep security fresh in our minds.

A: There are over 20 different security courses available to employees at the Laboratory with additional courses that are available from the DOE at no cost, at the Nonproliferation and National Security Institute in Albuquerque. What S-Division has trouble with is assignment of personnel to training when an employee is newly assigned a security responsibility. There are some job assignments where the employee must be formally identified and recognized by S-Division groups and they automatically get enrolled into a training plan, receive the training and get EDS reminders when it's time to requalify. Unfortunately we don't have a good system for identifying all employees who have incidental or casual need for training such as "handling classified" without management or cognizant training specialists letting us know. We are working to close this loophole.

Regarding your idea about changing the topic of security training, we are limited by DOE as to what is presented for our Annual Security Refresher. The content is standard issue from DOE with some site specific information inserted by our office. The content is changed annually and we are not allowed to change the theme for this required training. This does not preclude us from having additional security briefings quarterly on different topics as you recommend. Unfortunately we could not grant Annual Security Refresher credit for this attendance. The recommendation is a good one and will be brought to the Security Education Coordinator and the OPSEC Office.

Q: The problem with web training is that you can just scroll through without reading any of it and still get credit.

A: What we have done as a first step to stop the "clickers" for the 2000 Annual Security Refresher is to place a time limit feature which will not allow you to click to the end. This feature works by delaying the next button for a few seconds before the student can move on. For the most part, this works, but it's not the best methodology to get people to read the information. The 2001 program will incorporate more adult learning theory into the initial design. We also are working to build in special flags that will identify the clickers based on time spent in the program. If someone clicks through a 40 minute program in 4.5 minutes, they will be flagged.

Training (Continued)

Q: Will the security training requirements be addressed in the 3 security LIR's being written? Isn't there some way to standardize who needs what kind of training?

A: A security training matrix has been developed and will be included into the General Security LIR. The matrix will help identify the training by job assignment. If you have this security responsibility (handling classified materials) training is required. It will reference the DOE driver, the format of the course, number, title, and relevant comments.
In addition, the Training Integration Office (TIO) of HR-6 has an on-line training requirements questionnaire that an employee can run through and answer questions on various job assignments. When the employee indicates that they do a specific job assignment, they are automatically identified into the correct EDS training plan. The employees supervisor must approve (electronically) the training plan before the employee actually is enrolled. The questionnaire is located at the Laboratory Virtual Training Center—http://www.lanl.gov/labview/training/training.html, bottom left corner.

Q: The S-Division on-line training does not reflect current rules. It still states we have a 2 hour rule and we don't.

A: The training content was revised shortly after the 2 hour rule was revoked by DOE in 2 of our courses.
During the past two years of security crises, many rules and procedures have changed. Each course is revised annually and all changes will be caught and updated.

Q: Conduct real training for security, personnel, document, and computer. On-line training does not work.

A: A few years ago, Security received sufficient comments from the field asking that we conduct more web-based training and less classroom instruction. The reason for this was time spent in class. Due to the unusually higher educational levels and computer literacy we have at the Laboratory, many customers would rather do their training requirements on-line rather than go to a live class. A majority of them on-line. This does not necessarily work for everyone and every course. For example, we never place any first time training or "orientation" type training on the web. It's instructor based and will remain that way. We are working to have "prerequisite" web-based training prior to going to a live course to ensure that all students arrive with a certain level of knowledge.
Realizing that we need to have options, we will begin to have more live instruction beginning in January 2001. Our Annual Security Refresher will be offered as a live course on a weekly basis.

Q: Are contractors required to take the same training regarding security? Training should be required.

A: At the Laboratory, security training is based on job assignment regardless of who you work for. Anyone having a Q/L clearance must take the appropriate training (i.e. Initial Security Briefing, Annual Security Refresher). If you use a computer, you must take Initial Computer Security and consequently Annual Computer Security Refresher. If you escort others into a security area, you must complete Security Escort Training. The training is based on job assignment.

Integrated Safeguards & Security Management
UPDATE

Security Help Desk 5-2002

December 12, 2000 VOL. 1, NO. 1

The ISSM Update Bulletin purpose is to share security guidance & clarification to LANL users.

NEWS:

These Q&A's, and more to come, were primarily generated from individual ISSM Rollout Workshops. These questions and the respective answers were reviewed by Security professionals and will be available in a searchable format on the web in the near future. This printable document is one of the methods we will use to notify you of our progress answering peoples questions, concerns, and suggestions. If you have any questions, please contact the Security Help Desk at 5-2002.

Contents:

Email	1	Special Projects Office	15
Definitions	1	Assessments	16
PSAP	2	Training	16
Physical Security	2	Procedures	16
EM&R	2-3	Visitors	17
CMPC	3-4	MC&A	17
OUO	4-7	Contacts	18-20
Clearances	7-8	Badges	21-24
Classification	8-15	Miscellaneous	24-26

Email

Q: What should employees do about "chain letters" they receive or send electronically or hardcopy?

A: Chain letters are illegal and should be forwarded to the Special Projects Office (S-SPO), who will conduct an inquiry.

Q: Issues were brought up by four organizations which shared concerns of using secure@lanl.gov as the lab wide email address for security issues, concerns, and questions.

A: Initially, the word "secure" was used instead of "security", stating that LANL wanted to be in a "secure" state. After several people expressed concerns that somebody might send a classified email based on the address, it was changed to security@lanl.gov.

Definitions

Q: Two different organizations wanted definitions of Safeguards, Security, and Safeguards and Security.

A: Safeguards: An integrated system of physical protection, material accounting, and material control measures designed to deter, prevent, detect, and respond to unauthorized possession, use, or sabotage of nuclear materials.

Security: An integrated system of activities, systems, programs, facilities, and policies for the protection of classified information and/or classified matter, sensitive information, nuclear materials, nuclear weapons, and nuclear weapon components, and/or the Department's and the Department's contractors, facilities, property, and equipment.

A Safeguards and Security Activity is any work performed under contract, subcontract, or other agreement which involves access to classified information, nuclear material, or DOE property of significant monetary value by DOE, a DOE contractor, or any other activity under DOE jurisdiction. Also included is the verification of the capabilities of approved Federal locations.

PSAP

Q: Two organizations have issues with the yellow PSAP strip. What purpose does it serve?

A: The function of the yellow PSAP unique identifier is to provide additional check and balance for those personnel who enter PSAP work areas and MAAs unescorted. It serves as a visual identifier for the protective force and co-workers that the individual is, in fact, an approved PSAP participant.

Q: Why do some employees who have access to SNM (at CMR) not have to be PSAPed, when other employees doing the same work do?

A: The requirement to be in PSAP centers around unescorted access to SNM. Anyone who has unescorted access to Category 1 levels of SNM or Category 2 (where there is critical rollup to Cat 1) must be in PSAP. Additionally, persons with knowledge of where Cat 1 is located at any given time must also be in PSAP. Access to lower levels of SNM (Categories 2,3,4) does not have to comply with the human reliability requirements of PSAP.

Q: If you tell someone you're enrolled in PSAP is that a problem?

A: It depends on the context. Work related questions about enrollment in the program present no problem. Non-work related questioning in a social environment should be considered logically and if the questioning seems unusual or of an over interested nature, it would be best not to elaborate on your participation in a human reliability program.

Q: Two different organizations have asked if they can use a LANL badge with the PSAP appliance on it as an ID.

A: The use of the standard badge for official business is no different even if a PSAP unique identifier is attached. Examples would include using the standard badge as identification at the stationary store or providing it as verification of government identification when requesting government rates.

Physical Security

Q: What is the Lab's policy for access to areas that are controlled by Palm Readers? There is some confusion over how many people may enter after one (1) person has had their palm scanned. This situation is when there are several individuals entering at the same time and together. A new policy on palm reader access was promised a year ago. Where is it? If it does exist, employees need to be notified. Badge access and palm reader access is inconsistent across the laboratory sites.

A: Piggybacking is allowed trough doors and gates where the access is controlled by palm reader only, and you recognize and work with the individual(s). Another scenario would be: if they are visiting and have identified the individual they are visiting, and have the proper clearance level for your building you are allowed to piggyback. If you feel uncomfortable and/or uncertain, you can ask them to please run their badge through the badge reader. The thing to remember: When you allow piggybacking you are in essence performing the same function of the palm reader; therefore, assuming that responsibility. The latest guidance on piggybacking can be found in DOE N 473.5-6, dated 6/5/00.

EM&R

Q: Five different organizations expressed concerns and issues about policies for tagging bags.

A: All bags, briefcases, lunchboxes, purses, etc. on Laboratory property should be tagged. Any bag, purse, package, etc. left unattended, will be treated as a suspicious package. In the process of determining whether the package is an actual hazardous device, the object could be destroyed. Identification tags may prevent the destruction of your package, thus protecting your belongings or government property assigned to you. For those on travel, if you don't wish to travel with the tags on your bags, remove them and replace them upon your return.

EM&R (Continued)

Q: Issues were mentioned by 6 organizations concerning suspicious packages/briefcases, and the process for reporting such an incident.

A: Upon discovery of a package that you deem "suspicious", you should warn people in the immediate surrounding area to leave the area and then you should call "911" to report it. Calling "911" will alert all the necessary response personnel needed to handle the situation. Try to keep people from re-entering the area until response personnel arrive. Based on the potential threat, the response personnel will determine the danger area to be evacuated. The evacuation must be controlled to ensure that employees are not placed in harm's way during the evacuation. For that reason, the fire alarm should not be used to initiate the evacuation. Employees should be told to evacuate and the safest path to follow, i.e. away from the package. This can be accomplished by word of mouth, an intercom system, or any other means available. The purpose of the muster area is to provide a safe place for employees to assemble for accountability purposes. If the "suspicious" package could threaten the muster area, select another area in a safe location and direct employees to go there. Safe muster areas must be selected to protect employees. If the area is deemed not to be safe for any reason, select another safe area as the muster area. Personnel safety is the driver in selecting the appropriate muster area.

CMPC

Q: How would an uncleared individual recognize classified data if they saw it? How do you distinguish if a "TOP SECRET" stamp is valid? Some "junk mail will have a "TOP SECRET" stamped on it!

A: Official DOE classified documents will have the following markings, and not just "TOP SECRET":Level, Category, Subject or Title (Suggested), Authorized Derivative Classifier (ADC) Information, Date, Office of Origination, and Caveats (if applicable). Accountable documents must also have a unique identification number. Classified documents with additional pages must have level and category on the TOP and BOTTOM of subsequent pages, and, BACK of last page. However, category is not needed for NSI documents.

Q: DOE should re-institute tracking classified (secret) documents.

A: Thank you for your comment. DOE has recently changed the requirement to account for electronic media as you know. They would have to study the impact of tracking documents nationally. If LANL approved the proposition, LANL could institute their own tracking of the documents, but operational impact, costs and time versus the benefit would have to be considered prior to implanting such a system. We are on the way with the electronic tracking, but documents would add a substantial load.

CMPC (Continued)

Q: What is the Lab policy for handling classified information in an open area? Non-cleared employees are not trained in the proper methods for handling classified data. Training non-cleared employees in the proper handling of classified information could be helpful, should a situation arise where a non-cleared person comes in possession of classified information by accident or through the mail system.

A: Generally, classified information should not even be in Open Areas (unless somebody authorized is handcarrying it from one secure area to another and goes through an open area to get there) - so, if somebody has classified in an open area, it should be properly covered and marked, in a sealed opaque envelope, with the name, group, and Classified MS of the person transferring the information, as well as the name, group, and classified MS of the person receiving the information. OR, classified information may be in an open area IF it is in a locking briefcase with the owner of the briefcase's name, group, and classified mailstop. It must be covered and protected AT ALL TIMES within an OPEN area. S Division does offer training on Classified Matter Protection, which can be found by going to Training, from the LANL home page, and then click on Safeguards and Security.

OUO

Q: Can addresses be sent over email?

A: Yes; however, the general rule of thumb is that if you don't want anyone but the person you're sending it to see it, don't email it. Email is not a secure communication system.

Q: What about sensitive issues or ADSM backups?

A: It is not secure; therefore, not recommended, but not prohibited.

Q: What are the guidelines for handling unclassified sensitive personnel files?

A: When they are not in your possession, they need to be locked up.

Q: Two organizations have asked how to protect sensitive unclassified?

A: Sensitive unclassified needs to be protected by a single barrier. Examples of a single barrier include, a locked office, drawer, or building. A security area provides a single barrier as well.

Q: Where should industrial partnership data be physically kept?

A: Industrial Partnership data is sensitive unclassified, which requires a single barrier of protection. Examples are a locked drawer or locked office.

Q: Who in Industrial Business Development (IBD) is the LANL POC for Industrial Partnership policies, procedures, and data?

A: Donna Smith, 7-9473

Q: Many employees in several organizations questioned the sensitive nature of names, Z numbers, financial codes and etc. when much of this kind of information is readily available through the Lab's web site or other internal sites.

A: Z numbers and financial codes are not considered sensitive, and that is why they are so readily available.

OUO (Continued)

Q: Two organizations had issues concerning Project Financial Data: Is this "sensitive unclassified"? Salaries are a matter of public record. Does this mean that a project is "sensitive unclassified"? The concern expressed here was that project cost estimates and resources planning tools in common use identify individual staff members with a cost that is a function of their salary. Salary categories, especially for staff, have evolved in the past few years to quite narrow, and it allows easy determination of a person's salary within a fairly narrow margin. However, LANL salaries are a matter of public record and yet all documents that deal with salary are protected. The basic is another one of lack of guidance, and the specific questions relates to whether or not cost estimates and project budget planning documents should be treated as "sensitive unclassified" (FOUO)? because of salary concerns.

A: An employee's salary, in and of itself, is public information as defined in the California Information Practices Act and the California Public Records Act. It is public information because of our association with the University of California, a public institution, because the University of California is subject to these laws, and we are employees of the University of California.

When combined with other non-public information, such as project proposal, salary increase documentation, disciplinary actions, or personal information then the document may be "personal information", "sensitive unclassified", or "in-confidence" depending on the sensitivity of the other information. A person's salary is public information, as is their name. If name and salary are combined with gender and/or ethnicity, it becomes personal information, and must be protected. If the name, salary and gender were included in a disciplinary document, the document would be "sensitive unclassified". Most project cost estimates are based on "salary factors" which only relate to a specific employee because of their Series and level, not their specific base annual salary. For more information, contact HR-1.

Q: If UCNI is left on a copier outside the fence, is it considered a security infraction?

A: Normally, infractions involve classified information; HOWEVER, any violation of procedures listed in DOE Order 470.1 (UCNI is addressed in this order) can result in an infraction.

Q: LANL Policy for Sensitive Information-What is the LANL policy on handling sensitive information? It's not clear what type of information the lab views as sensitive. Is Project Financial data sensitive? On personnel data, what is sensitive and what is not? Can you take sensitive information home to work on it? Can you take personnel information home to work on it? Is there a LANL policy?

A: As far as protecting sensitive unclassified information, there are 2 main types of sensitive unclassified...UCNI, and OUO. Other types of sensitive unclassified include export controlled information, NNPI, Applied Technology, Proprietary, Protected CRADA, etc. LANL organizations sometimes invent their own categories like "In Confidence", "Personal Information", "Privileged", etc. These last 3 have no authority, penalties, etc. for disclosure, and no actual protection should be assumed. It is just a flag. As far as UCNI: Please refer to the following websites for protection requirements:
http://int.lanl.gov/orgs/s/s5/docs/UCNI_protection_requirements.pdf

OUO (Continued)

Q: (Continued): LANL Policy for Sensitive Information-What is the LANL policy on handling sensitive information? It's not clear what type of information the lab views as sensitive. Is Project Financial data sensitive? On personnel data, what is sensitive and what is not?
Can you take sensitive information home to work on it? Can you take personnel information home to work on it? Is there a LANL policy?

A: OUO is a type of unclassified sensitive information that is exempt from release under the Freedom of Information Act on a case by case basis. OUO documents should be marked on the bottom of the first page or cover page with the following marking: Official Use Only. The marking OFFICIAL USE ONLY should be placed on the bottom of each subsequent page or on the pages containing OUO information. OUO information should be stored either in a building that is locked at night or in a locked room, desk, container, or cabinet. When not in storage, OUO should be physically controlled to protect it from unauthorized access by nongovernment personnel. OUO may be transmitted by first class mail or any other more secure means. If a transmittal letter is used, indicate on the letter of transmittal that the transmission contains OUO. OUO may be reproduced without the permission of the originator. OUO may be destroyed by any means that renders it unreadable. Strip shredding is acceptable. As a general rule, we have been telling people to protect all sensitive unclassified as they would OUO. If you'd still like further guidance, please feel free to email or call us at 5-2002.
Most project cost estimates are based on "salary factors" which only relate to a specific employee because of their Series and Level, not their specific base annual salary, so it is not considered sensitive. All personnel data is considered "sensitive". You can take sensitive information home to work on it. There is nothing written that says you can't take sensitive home...General rule of thumb is, if YOU wouldn't want to see it in the newspaper, then consider it sensitive, and protect it.

Q: Project tracking shows person's name and salary, this should be eliminated. There should be a way to lock and close out cells. This was a comment to the effect that LANL on-line reports such as those from Data Warehouse should automatically include proper sensitivity markings. In some cases, they should provide the user with a non-sensitive option for some reports, such as projects budget with names and salary information, to automatically hide information that would make the report sensitive but still provide user information required for tracking and planning.

A: An employee's salary, in and of itself, is public information as defined in the California Information Practices Act and the California Public Records Act. It is public information because of our association with the University of California, a public institution, because the University of California is subject to these laws, and we are employees of the University of California. When combined with other non-public information, such as project proposal, salary increase documentation, disciplinary actions, or personal information then the document may be "Personal Information", "Sensitive Unclassified", of "In Confidence" depending on the sensitivity of the other information, and must be protected. If the name, salary, and gender and/or ethnicity, it becomes personal information, and must be protected. If the name, salary and gender were included in a disciplinary document, the document would be "sensitive unclassified". Most project cost estimates are based on "salary factors" which only relate to a specific employee because of their Series and Level, not their specific base annual salary.

OUO (Continued)

Q: Should social security numbers be sent on unclassified faxes? Should travel itineraries be sent by email for employee travel? Is there a vulnerability to cleared employees?

A: Social security numbers are considered sensitive information, as are travel itineraries. At this time there is nothing written that prohibits a person from sending them on email or faxing that information; however, it is not recommended.

Clearances

Q: 9 different organizations had issues, concerns, and questions concerning L clearances; specifically, why the Lab has L's, why L's and Q's can co-mingle, and why can't the Lab just get ride of L's.

A: The question of whether or not the Laboratory should be an "all Q" Laboratory has been discussed for the past year or more at both the local and federal level. The three Laboratory directors (LANL, LLNL, SNL) have stated before several Congressional committees that their Labs should be Q cleared facilities only. On the one hand, this seems like a reasonable approach, and until 1993, it was a given that anyone working at Los Alamos had to have a Q. However, in order to implement an all Q Laboratory now, the cost would be such that Congress must agree financially to help make the conversion due to the current large number of L cleared and uncleared workers now at Los Alamos. Divisions have taken it upon themselves to change some buildings to "all Q" areas based on the work performed in the building and on available funding for the clearances. If you believe there is a serious security problem with mixing L and Q clearances in your building, this should be discussed with your division or building management.

Q: 4 different organizations have had concerns about Q clearances issues, such as wanting and/or needing more, why they take so long, who pays for them, etc.

A: There is no question about needing more Q clearances. This fiscal year the Laboratory has requested 1100 Q clearances. We expect to be allowed to clear less than half that amount. Funding is a matter of Congressional decision that comes to us as a ceiling on how much money we can spend on clearances. The money to pay for clearances must come from funds already allocated to the Laboratory. Last year Congress raised the ceiling, allowing us to spend more money on clearances, but again, this money had to come from program funding already in place. This has been a kind of borrowing from Peter to pay Paul approach, wherein money must be siphoned from programmatic efforts in order to clear the personnel needed to perform the programmatic work. Part of the funds we "spend" on clearance includes funding for staff support at DOE Albuquerque. DOE/AL has worked hard to lessen the time it takes to grant a Q (in the last few months the average has dropped to around four months from one year), but we have yet to see a long-term trend in this direction. DOE/AL is working under a government-mandated reduction in staffing combined with increased clearance needs from all the sites it oversees. This has resulted in DOE/AL having to do much more with considerably less. Part of the funding we supplied to DOE/AL has been used to increase its contractor staff to alleviate the length of time it takes for a Q clearance to be processed. Security and Safeguards Division management is working closely with NNSA to try to alleviate this problem, but the final fix must come from Congress.

Clearances (Continued)

Q: What do you do about Lab employees who have lost their clearance but are still working at the Lab specifically at TA-46? Should they be issued an uncleared badge? They have no identification.

A: All workers on Laboratory property for 10 working days or longer must have a badge identification. An individual who has lost his/her clearance is always provided with an uncleared badge. If they have no identification their management should be notified. The individual is required to have and wear the appropriate badge while on the worksite.

Q: Shouldn't TA-55 be a Q cleared only facility?

A: This is ultimately a Division decision, although Security needs to be heavily involved.

Q: The problems are the following:
1. Non-DOE cleared: Persons investigating our staff with clearances are not presently cleared through DOE.
2. Unrestricted Access: Investigators have access to both: our backgrounds and our work assignment.
3. Unbadged and Unescorted: They are walking around Lab property without badges and unescorted (in uncleared areas).
Extrapolations of potential threat:
- Espionage Threat: There are few better places for a foreign country to put a controller or spy to evaluate potential "spy recruits."
- Intelligence Threat: Security of Lab property thru "badged access" not enforced and therefore, our investigators are free to roam Lab premises without escorts. The policy of unbadged visitors needs to be tightened up. These are short term visitors, so Lab policy requires an escort for unbadged persons while they are on Lab property-- even in uncleared areas. Without an escort or badge, we cannot determine their authenticity of conducting official business. A hostile entity could take notes of our security schedules, record intel, etc... and will go virtually unchallenged.

A: There are nine L-cleared USIS investigators assigned to Los Alamos. These investigators wear "visitor" badges from DOE/HQ. During the year, many more investigators, mostly uncleared, are assigned to Los Alamos to perform the needed interviews for the approximately 2,000 clearance reinstatements, reinvestigations, and initial clearances required by LANL. Laboratory policy states that if an individual is going to be on-site for a cumulative ten days or longer, they must be badged. If an uncleared investigator is here less than that time, they do not officially need to be badged; however, we have asked USIS to badge anyone who is here for more than 10 days. All investigators must have identification from OPM, Office of Personnel Management, or USIS. All investigators receive a background check before they are hired by USIS. The LANL Clearance Processing Office acts as liaison with USIS for any complaints and should be contacted if an individual is concerned about an interview. Beginning in April, 2001, the FBI will perform the investigations for all individuals in special access programs (SAPs) and in the Human Reliability Program (PSAP and PAP). The only way we could insist that all visitors be badged and escorted is to close the entire Laboratory. This concept has been discussed over the years. It would entail closing Pajarito Road and several other major changes to traffic and access. Studies have been made on the feasibility of doing this but no decision has been made. If they are uncleared and require access into a secure area, the 1812 process must be followed. The form 1812 is located at:
http://enterprise.lanl.gov/forms/1812.pdf

Classification

Q: What about formal collaboration agreements with institutions in foreign countries?

A: A formal collaboration agreement does not supersede the export control regulations. Technical data provided to foreign nationals must be in accordance with Laboratory policies and procedures (see guide at http://bus.lanl.gov/bus6/eximguide/guide.htm) whether or not there is a collaboration agreement.

Classification (Continued)

Q: Other DOE labs and sites want to benchmark against BUS-6 programs. Can we release this information and to what extent?

A: BUS-6 management will need to make the determination whether to benchmark with other DOE labs and sites. Contact BUS-6 for more information.

Q: What are our responsibilities for email going abroad? LANL employee on sabbatical in France:

A: Email senders are responsible for whether there are export control restrictions on technical data mailed to foreign countries or foreign nationals in the US. (see guide at http://bus.lanl.gov/bus6/eximguide/guide.htm). The subject line of the email should include one of the labels "Correspondence" or "TSPA", just as for hard copy. See the Laboratory guidelines on export control of information found in the Requestor's Guide to Exporting/Importing at http://bus.lanl.gov/bus6/eximguide.htm.

Q: What are the rules for technical information exchange with colleagues at LANL?

A: Anyone providing technical data to a foreign national (at the Laboratory or elsewhere) is responsible for determining whether there are export restrictions on the information (see guide at http://bus.lanl.gov/bus6/eximguide/guide.htm).

Q: Basic scientific research is not export controlled. What email is deemed export?

A: Fundamental research not specific to defense articles as specified in the International Traffic in Arms Regulations (ITAR) is outside the scope of the export control regulations, and may be provided to foreign nationals without export control concerns.
An export of technical data is "deemed" to have occurred if technical data which is within the scope of the export control regulations is transferred within the United States to a foreign national who does not hold a permanent resident alien visa. (see guide at http://bus.lanl.gov/bus6/eximguide/guide.htm.)

Q: Some purchase requests are FOIA sensitive. LANL should have foreign codes for ordering materials for sensitive or classified projects.

A: While "FOIA sensitive" is not defined, the Laboratory has in the past devised methods to disguise the purchaser or funding source for certain material where that information would reveal classified information. This is generally handled on a case-by-case basis. If this procedure seems necessary, S-7 may be contacted for assistance.

Q: Three different organizations had questions concerning SUCI vs. Sigma definitions.

A: Sigma definitions are available at http://www.hr.lanl.gov/scourses/lanl/SigmaUpdate/page01.asp. Pending revision of the applicable DOE Order (DOE O 5610.2) these definitions are all that is currently available. Individual Sigma authorities must be assigned by managers to employees using the Signature Authority System on Labwide Systems(see:http://w10.lanl.gov:80/orgs.cic/computingatlanl/training/labwide.html). For visitors from other sites, contact the Badge Office for information on how to request Sigmas. Sensitive Use Control Information (SUCI) is an obsolete designator that referred to information that currently falls under Sigma 14 and 15. For more information, see DOE M 452.4-1.

Classification (Continued)

Q: Two organizations wanted further guidance regarding "DUSA".

A: The Designated Unclassified Subject Area (DUSA) program is described in detail at http://int.lanl.gov/orgs/s/s7/dusa.shtml. The Laboratory no longer exempts documents from classification review based on program code, but only on applicability of an approved DUSA. It is the responsibility of the author to confirm that a DUSA applies and that none of the general or specific exclusions to that DUSA apply, before releasing a document without ADC review.

Q: Three different organizations commented that there were too many levels of classification, and two of those three wanted to know if there was a chart that explains all the levels.

A: The levels and categories of classified information are available in several places in addition to the annual security refresher. One place is the ADC handbook available on the S-7 web pages. Since there is very little Top Secret material involved in most Laboratory activities, most employees only need to worry about two levels of classified information-Secret and Confidential. The rules of marking and handling such information can be found on the S-6 web pages.

Q: Can you give us more information on Export Control Information?

A: Laboratory guidelines on export control of information can be found in the Requestor's Guide to Exporting/Importing at http://bus.lanl.gov/bus6/eximguide/guide.htm.

Q: Do emails to foreign countries need to be marked in the same manner that letters and other hard copy correspondence are marked?

A: Yes. The subject line should included one of the labels "Correspondence" or "TSPA", just as for hard copy.

Q: How do you handle performance evaluations where accomplishments may deal with classified information?

A: Performance appraisals should be reviewed for classification as for any other documents relating to Laboratory activities in potentially classified subject areas. Extra care must be taken to avoid inconsistency in the wording of activities or assignments year-to-year which might reveal classified information when taken together, for example in a personnel file. If neither the employee nor the supervisor is an ADC, S-& may be contacted for assistance if necessary where confidentiality is of concern.

Q: Four organizations raised concerns about the Laboratory not having enough ADCs to handle the workload.

A: It is a management responsibility to ensure that there are sufficient ADCs in organizations to handle the review workload. This number can depend on the amount and type of classified work, geographical distribution of the organization, employee work schedules, etc. Management support for the classification program is a DOE metric upon which the Laboratory is appraised.

Q: Do we have any control over classified information that may be published, or work done while at LANL as a visitor?

A: If the visitor is (or was) cleared, he or she is bound by the same nondisclosure rules as any cleared employee. If the visitor was not cleared, he or she should never have had access to classified information. If an uncleared person publishes classified information in any venue, the only response allowed by the DOE is "no comment."

Classification (Continued)

Q: Two organizations had questions concerning classification review of emails, and who is responsible when an email (classified) is forwarded that hadn't been reviewed.

A: Classification review of emails can be problematic and very inconvenient. One mechanism to consider is for the sender to discuss with an ADC the intended content of the email, and then to be very sure that the content does not exceed the boundaries of information confirmed by the ADC to be unclassified. If there is any uncertainty, the ADC should review the actual text. While this mechanism meets the intent of the DOE requirement, it does not absolutely guarantee there will be no mistakes. Close interaction with your ADC is the key, and it is always wise to avoid any references to subject areas with classified aspects. Mere forwarding of email which subsequently is determined to be classified usually does not result in security infractions, but will require potentially inconvenient and time-consuming "cleanup" of the computer system. Of course, if you know or suspect that the email has classification problems, you should never forward it, but consult your ADC or OCSR immediately.

Q: Two organizations suggested enhancing the training, as well as revising guidance documents.

A: The ADC training program is being updated but this has been delayed somewhat by the Cerro Grande fire and other issues in the past year. We will be able to focus more on specific classification guidance during initial training in the future. Although DOE has discouraged "local" classification guides, S-7 has in fact prepared and obtained approval for such guides where a clear programmatic need exists and current approved guidance is not adequate. For issues that are broader than LANL interests, revision of DOE Headquarters guides may be needed. While there is no specific "extra reward" for ADC service, nomination of an ADC by his or her manager carries the implied commitment to support and recognize that extra responsibility.

Q: There should be clear guidance on UCNI.

A: Since its inception in 1982, UCNI has evolved from a very poorly understood and implemented program to a more definitive, focused program for protecting certain unclassified but sensitive information about our most critical facilities and their security features, as well as certain proliferation-sensitive unclassified technical information. In the past ten years, specific topical UCNI guidelines have been approved and issued by DOE, covering a variety of subject areas. These guidelines, along with current DOE classification guides, are listed on the S-7 web pages at http://int.lanl.gov/orgs/s/s7/doe-classification-guides.shtml. ADCs who are also UCNI Reviewing Officials can use these guidelines for UCNI determinations. Some subject areas, such as facility design information, remain somewhat vague, but S-7 has provided an interpretive guide for these issues, also available on the S-7 web pages.

Q: 4 different organizations suggested that UCNI be eliminated.

A: Many lab employees and others share the frustration with UCNI; however, given that it is based in U.S. law (the Atomic Energy Act of 1954 as amended in 1982) and backed up by Federal regulation (10 CFR 1017) as well as DOE directives, we anticipate that UCNI is here to stay in some form.

Classification (Continued)

Q: Two organizations had issues regarding the LA 4000; specifically, should it be assigned as required reading to everyone to clarify classified territory, as well as what the most current version is, and if distribution is automated.

A: LA-4000 "Guide to the Classification of Technical Information" is the primary LANL local classification guide and is approved by DOE. The guide itself is classified SRD and is distributed by IM-5 to appropriately cleared employees with Sigma 1 and 11 access. The latest revision is Rev. 7, dated 9/93. A new revision is in the process of review and approval by DOE Headquarters and will be distributed when approved. LA-4000 is primarily for use by ADCs in making classification decisions but is available for other employees (appropriately cleared and with a need to know) who wish to learn more about the classified aspects of their jobs. Of course, employees should always consult an ADC about classification issues, since only ADCs have the authority to classify documents and other material. Another role of ADC is to help ensure that employees in their organizations are cognizant of classification issues with their work, through briefings, discussions, etc. with coworkers.

Q: How can something be "sensitive" but not classified?

A: Sensitive but unclassified information refers to information that would NOT damage national security if given unauthorized disclosure (this is the criteria used for defining classified information), but either 1) must be protected because of legal or regulatory requirements, or 2) may be exempt from public release under the provisions of the federal Freedom of Information Act. Examples of the former are: Unclassified Controlled Nuclear Information (UCNI), which is withheld under the Atomic Energy Act for reasons related to preventing nuclear weapon proliferation or theft or sabotage of nuclear material or nuclear facilities; export controlled information, which is withheld based on US law and regulations intended to preserve US economic competitiveness and military superiority; and personal/privacy information, withheld under the federal Privacy Act and other laws and regulations to protect individual privacy rights. Examples of the latter are government predecisional information, government agency internal procedures and policies (usually designated as Official Use Only) and commercial proprietary information.

Classification (Continued)

Q: Thirteen organizations raised issues, concerns, and questions dealing with ADCs; specifically, what happens when ADCs disagree with each other over the classification of something, the risks involved over making an error, training issues, roles and responsibilities, and gray areas associated with classification.

A: Classification guidance cannot cover in detail all possible situations or ways of describing particular concepts or activities. Hence, guidance is complex and applying it requires knowledge of the subject area and the guidance. Given that, most classification decisions are relatively easy. However, in some cases, ADCs using their best judgment will differ in interpretation of classification guide topics when applied to specific situations. In those cases, the Laboratory Classification Officer (S-7 Group Leader) is authorized by DOE, and has authorized his staff, to resolve these conflicts. If the issue cannot be satisfactorily resolved locally, DOE/AL or DOE/HQ may be asked for a ruling. A formal process exists for this if necessary. If guidance is determined to be inadequate, changes and/or additions may be formally requested. ADCs should always consult S-7 for resolution of guidance conflicts or ambiguities. According to DOE M 475.1-1 "Identifying Classified Information," there is no intent to issue security infractions in cases where ADCs disagree for legitimate reasons, that is, where there is no negligence interpretation when any such disagreements arise.

Q: We do not get classification guidance for Sub Crits until it is almost too late. This should somehow come out sooner.

A: It is S-7's responsibility to draft, obtain DOE approval for, and issue, classification guides for individual Subcritical Experiments (SCEs) carried out at the Nevada Test Site. While we try to get these guides in place as early as possible, our processes are always capable of being improved. There are issues that prevent development of these guides very many months in advance of the experiments. We work with technical and program representatives to ensure that the experiment design is determined to a degree adequate to be addressed effectively in the guidance before finalizing the draft guide. On one occasion, the design changed significantly after the guide was submitted for approval, resulting in some confusion and additional delay in obtaining correct guidance. As experiment designs and diagnostics become more complex, this close cooperation is even more important.

For information, here are the dates on which recent SCE guides have been submitted for DOE approval, approved, and issues, along with the experiment date.

	Guide submitted to DOE for approval	Approval received from DOE	Guide issued	Date of experiment
REBOUND	1/17/96	2/21/96	3/12/96	7/2/97
STAGECOACH	11/7/97	1/12/98	1/13/98	3/25/98
CIMARRON	8/15/96	9/17/96	9/30/96	12/11/98
THOROUGHBRED	2/8/99	12/8/99	12/8/99	3/22/00
STALLION	4/17/00	11/14/00	11/20/00	TBD

Classification (Continued)

Q: UCNI and need to know - can it be made available to vendors or possible CRADA partners?

A: According to DOE O 471.1 (the DOE UCNI directive currently appearing in Appendix G of the UC Contract), UCNI may be made available to any contractors or subcontractors to the government, consistent with need-to-know for the government work. It appears that if a vendor contract is in place, then the only remaining requirement is that all recipients be made aware of the requirements for handling and protecting UCNI.

Q: 2 different organizations had issues dealing with divisions having ADCs trained on specific topics.

A: Authorized Derivative Classifiers (ADCs) are authorized to make classification decisions in subject areas where they are technically competent, and where they are familiar with the applicable classification guidance. If they are also designated as UCNI Reviewing Officials, this applies to UCNI subject areas and UCNI guidelines as well. ADCs should never attempt to make classification decisions where they are not familiar with both the subject matter and the guidance , but should defer to another ADC or to
S-7. If classification guidance or UCNI guidelines appear too vague or ambiguous to allow a decision, another ADC or S-7 should be consulted for clarification. Under the DOE directives, there are procedures for resolving issues of interpretation if they cannot be resolved locally. ADCs who are uncertain of their roles and responsibilities in their organizations should discuss with their management in what subject areas they are expected to make classification decisions, and whether this is appropriate given their expertise and experience. In some cases, this discussion may point out the need for additional ADCs in an organization. S-7 will certify as many ADCs as needed in an organization.

Q: Two organizations raised concerns about roll up issues, combining unclassified information, and it then becomes classified.

A: In most if not all cases, the issue of "rollup" or compilation of information is not one of unclassified information "becoming" classified, but one of sufficient information being included to at some point cross the threshold of violating a specific classification guide topic. This usually means that a document has had significant additions without receiving subsequent classification review to ensure that it remains unclassified. Often, authors choose to avoid classification of a document by withholding certain specific material, and this is not uncommon or forbidden. However, if the information (which standing alone may be unclassified) is then added inadvertently the document will then be classified. Similarly, if two authors writing about the same subject choose to withhold different material to avoid classification, and subsequently the two documents are combined or closely associated (as in a file or on a web page) the same problem occurs. These scenarios point out the need for ADC involvement at all stages of production or publication of information in potentially classified subject areas.

Classification (Continued)

Q: Three different organizations wanted to know more about SUTI, and also information on the Sensitive Subjects List.

A: In early 1999, DOE directed that the laboratories identify which technologies at their sites should be considered "sensitive". This request resulted in the generation of various lists of "sensitive Unclassified Technical Information", or SUTI. At the time, there was considerable confusion and misinterpretation about the intent of these lists. Some misunderstanding still exists. These lists have since been incorporated into the Department's "sensitive Subjects List (SSL). According to a recent memo from the Office of Counterintelligence and the Acting Deputy Administrator for Defense Nuclear Nonproliferation, the SSL is an "illustrative, not comprehensive" list of subjects related to development of weapons of mass destruction and other subjects significant to national security, and the subjects are to be considered pointers to specific detailed entries in the U.S. export control regulations.

As such, the SSL is to be used for determining the possible need for export licensing considerations and certain counterintelligence-related checks in connection with unclassified foreign visits and assignments to U.S. laboratories, and also in connection with foreign travel by U.S. citizen employees. No other use for the SSL is intended by DOE, and these broad subject categories do NOT constitute information requiring specific protections, like Unclassified Controlled Nuclear Information (UCNI). This, "SUTI" is not a DOE-recognized category of information.
For information on the specific kinds of unclassified sensitive information at the Laboratory, employees can refer to the "Sensitive Unclassified Information Identification and Protection Manual" which was created in 1997 and is available from the S-7 web pages at http://int.lanl.gov/orgs/s/s7/pubs.shtml. This manual is currently being updated.

Special Projects Office (SPO)

Q: What are the rules for driving POV's on government business with a parking pass into areas marked as "Government Vehicles Only", or "No privately owned vehicles beyond this point"?

A: The parking permits are issues to allow privately owned vehicles (POV's) to park in spots marked for government vehicles. POV's with a parking permit may park in a spot marked "Government Vehicles Only", unless the spot is reserved for a specific (identified by a license number on the sign) government vehicle. The parking permit does not allow for a POV to enter areas marked "No Privately Owned Vehicles Beyond This Point". If you are issues a parking permit, please read all of the regulations governing their use on the reverse side of the permit.

Q: How does one get help in the case of angry or potentially violent employee/visitor?

A: If a person believes they are in grave danger, dial 911 immediately, otherwise call the Special Projects Office of S Division (S-SPO). S-SPO will take whatever action necessary to ensure your safety.

Assessments

Q: Previously, NMT-4 conducted a periodic internal audit of classified documents (program conducted by Richard Naranjo) that would help identify potential issues or problems that could be addressed by the parent group prior to any formal audit or review. Should this process or program be reinstutited?

A: An OSSO focus group has been established, and is in the process of developing Checklists that will be used to conduct periodic reviews of all S&S related functions.

Training

Q: Is it permissible to 1) use the "back" key function to review material, and 2) print information before taking the online test, for the purposes of review?

A: It is permissible to print security training information for purposes of review and reference; it is also permissible to use the "back" key function to review material.

Q: We have problems with Laboratory-wide Security Training Materials.

A: The above comment "we have problems with laboratory-wide security training materials" is not specific enough to address in this forum; however, we do encourage anyone who is experiencing problems to contact the members of the S Division Training Team at 7-5911 for assistance. This could be an opportunity for us to improve our materials.

Q: We often don't know the security rules. We do lots of work outside the fence. To keep the pace, we use "gray areas" in the rules.

A: Please contact either your Division's OSSO, or the LANL Security Help Desk, at 5-2002, if you have questions concerning the security rules.

Q: Is there an emergency email address for security?

A: There is not an emergency email address for security. The quickest way is to call 5-2002, with your security concern. After hours, if you have a security concern, you can call PTLA, at 7-4437. Of course, if it is truly an emergency, call 911.

Procedures

Q: The following list of guidance checklists could be posted on the Web.
1. Arrangements for all visitors
2. How to initiate classified computing
3. Handling reprint requests from sensitive countries
4. Guidance on communications with foreign nationals.

A: The Web does have information/guidance on various security related procedures. The S-6 Badge Office home page (http://badge.lanl.gov/) has a "Site Index", with subjects listed in alphabetical order to assist in finding procedures. ISEC also has a home page (http://s6server.lanl.gov/isec/is.html) with pertinent information. We do encourage anyone who has security problems or questions to contact their OCSR or the related Security & Safeguards Group Office for assistance if they cannot find a procedure on the Web.

Q: Does the group have the flexibility to establish internal group policies on security related issues?

A: Internal group policies (as long as they meet LANL policy) can be established, but make sure you keep your OSSO involved in all the policy changes.

Visitors

Q: What is the policy regarding minors on Laboratory property?

A: The policy regarding minors on Laboratory property can be found in the Laboratory's Administrative Manual, under AM616, section .0-.15, entitled "Visitors under 18 years old". To access this site, go to http://admin-manual.lanl.gov/. From there click on Administration, then General Administration Policies. Scroll down, and you'll see AM 616, Visitors.

Q: Who is allowed at TA-53 without a DOE Badge? How do unbadged vendors get on site? How far in advance do we need to notify the guard at the guard station of unbadged visitors allowed to enter TA-53, and who notifies the guard station?

A: As per the latest PTLA Post orders: For access into TA-53 via post 416-DOE/LANL who have been issued a badge, but have forgotten it must go to the badge office for a "T" badge. Others who do not have a badge are cleared into the area by personnel listed on the TA-53 Authorization List by telephone or in writing. This list is maintained at Post 416. Photo ID is required.
Unbadged persons who arrive at the post who have not been cleared into the area prior to their arrival will be instructed to park in the parking area just to the south of the post. They may use the courtesy phone to attempt to gain clearance into the area. There is a phone number posted on the inside cover of the phone they call for assistance. The site person contacted will contact the post to authorize the visitor into the area.
Foreign Nationals "must" have a valid Foreign National Visitor Badge. They cannot be "cleared in" any other way.
Family Member access- Unbadged family members may access TA-53provided they are in possession of a TA-53 Family Pass, issued by TA-53.
Carpool Member Pass- Unbadged carpool members may access TA-53 provided they are in possession of a valid TA-53 Carpool Pass, issued by TA-53.
Personal deliveries-Deliveries of products of a personal nature such as pizza, flowers, etc. will not be permitted. The delivery person will be instructed to contact the recipient and the recipient must report to the Post to accept delivery. They can use the courtesy phone as well.

MC&A

Q: 2-Person rule scenario-what is the appropriate response if this type of incident is encountered:

A: 1. The observer calls attention to the perpetrator, the fact that he/she is "out of compliance" with the 2-person rule. At that point the "perpetrator" will either:
Come into compliance
Cease the operation
Keep on working alone

Notification: The observer should notify his manager and custodian, and must call the S-4 Control Team leader as soon as possible to report the event.
NOTE: If the perpetrator kept on working alone (c), prompt notification of local management must be made first.

S&S Contacts

Q: Why is the contact list for Safeguards and Security so complicated? The list needs to be simplified.

A: This list has been simplified for the ISSM rollout presentations. The simplified list can be found at: http://int.lanl.gov/orgs/s/issm/docs/resource.pdf

Q: The security resources that are located in the ISSM should be posted in everyone's work area.

A: This is a great suggestion, and will be brought up at the next Labwide OSSO monthly meeting.

Q: What are the responsibilities of the BUS OSSO, OCSR, and OPSEC and how do we determine who to contact concerning different security issues?

A: The Organizational Safeguards & Security Officer (OSSO) appointed below will serve as the organizational point of contact for Safeguards and Security (S&S). This includes coordinating, assisting, and ensuring development of S&S implementation and the duties and responsibilities listed below. These duties and responsibilities require a commitment of 500 hours to 2080 per year, depending on the size and activities of the organization and should be reflected in the OSSO's annual performance appraisal.

- Attend OSSO training and working group meetings on a regular basis; participate in S&S Focus Groups as needed.
- Serve as organizational focal point in incident reporting, tracking and response.
- Coordinate S&S communications by:
  - Briefing management on S&S concerns or incidents and keep them informed on program items that need special security considerations.
  - Working with program/division management to develop an understanding of and support for S&S efforts and activities.
  - Writing security plans for construction and other special projects with security requirements.
  - Establishing division specific procedures in support of S&S policies and requirements (i.e. escorting, vault/VTR, etc.).
  - Contacting Technical Surveillance Countermeasures (TSCM) Officer for services.
  - Ensure appropriate actions are taken for changes of clearance or assignment status.

S&S Contacts (Continued)

Q: (Cont.) What are the responsibilities of the BUS OSSO, OCSR, and OPSEC and how do we determine who to contact concerning different security issues?

A: (Cont.)

- Advise management concerning requirements for personnel appointments and ensure the following S&S functional responsibility assignments are made:
  - Information Safeguards and Security Officer (ISSO)
  - Organizational Computer Security Representative (OCSR)
  - Classified Document Custodian (CDC)/Part Custodian
  - Authorized Derivative Classifier (ADC)/UCNI Reviewer
  - Key/Core Custodian
  - Alarmed Access Area Custodian
  - MC&A Coordinator
  - Nuclear Material Custodian
  - TID Custodian
  - ISEC Organizational Representative
  - Physical Security Representative
  - Personnel Security Assurance Program (PSAP)/Personnel Assurance Program (PAP) Coordinator

- Ensure that all Division/Program personnel receive required initial and refresher security training.
- Coordinate and participate in all security related assessments of LANL security programs pertinent to their area of responsibility. This includes:
  - Performing self assessments, and
  - Developing and tracking a corrective action plan for S&S concerns identified during assessments.

OCSR: http://int.lanl.gov/orgs/s/s5/docs/OCSR_form.doc

OPSEC: As the ISEC Organizational Representative (IOR) you will assist in identifying and coordinating Counterintelligence (CI), Operations Security (OPSEC), and Foreign Visits and Assignments (FV&A) issues within your respective organization. You are tasked with the following responsibilities:

- Participate as a member of the OPSEC Working Group (OSWG) representing your organization.
- Attend OSWG Meetings on a regular basis.
- Participate in other meetings, as needed, for the ISEC Program Office.
- Participate in CI, OPSEC, and FV&A training as required.
- Coordinate CI, OPSEC, and FV&A activities within your organization.
- Be cognizant of the presence and location of visiting/assigned foreign nationals to your organization.
- Periodically monitor the workspace of visiting/assigned foreign nationals and report any problems.
- Be cognizant of any after hours work conducted by visiting/assigned foreign nationals.
- Report to the ISEC Program Office all problems/concerns of a CI/OPSEC/FV&A nature.
- Coordinate and assist in the development and updating of the local site-specific threat statement.

S&S Contacts (Continued)

Q: (Cont.) What are the responsibilities of the BUS OSSO, OCSR, and OPSEC and how do we determine who to contact concerning different security issues?

A: (Cont.) OPSEC: As the ISEC Organizational Representative (IOR) you will assist in identifying and coordinating Counterintelligence (CI), Operations Security (OPSEC), and Foreign Visits and Assignments (FV&A) issues within your respective organization. You are tasked with the following responsibilities:

- Develop, review, and update a Critical and Sensitive Information List (CSIL) and the Essential Elements of Friendly Information (EEFI) for items requiring OPSEC consideration in your area(s) of responsibility and LANL in general. These CSILs and EEFIs will be prioritized and disseminated to appropriate management and operating individuals.
- Identify OPSEC consideration for ongoing and new projects or activities, new construction, or significant changes that occur to existing programs or projects based on the LANL threat statement.
- Coordinate and participate in OPSEC reviews/assessments of LANL programs or facilities pertinent to your area of responsibility, and make recommendations of corrective actions on identified concerns or vulnerabilities based on the results of the reviews/assessments.
- Support the counterimagery program at LANL, which is an integral part of the OPSEC program pertaining to imagery-susceptible, sensitive activities.
- Be aware of and ready to assist regarding challenge inspections (i.e., Chemical Warfare, etc.)
- Brief your respective management on CI/OPSEC/FV&A threats and keep them informed on program items that need CI/OPSEC/FV&A considerations at both division and group level.
- Work with division management to develop an understanding of and support for CI/OPSEC/FV&A efforts and activities in your area(s) of responsibility.
- Provide CI/OPSEC/FV&A awareness and educational material to managers and employees within your area(s) of responsibility. This material may be by memo(s) pertinent to a specific operation, emails, oral presentations by ISEC Program Team Members, oral presentations by yourself, briefings on specific ISEC considerations on a particular project/subject, video tapes on pertinent subjects, and/or CI/OPSEC/FV&A news bulletins. This list is not all-inclusive.

Badges

Q: Questions where raised concerning wearing badges. Specifically, safety issues, where and where not to wear your badge, and wearing your badge in the Wellness Center.

A: A memorandum issued by DOE/LAAO on July 31, 1998 and made available to the Laboratory community attempts to clarify the requirements on proper wearing of the badge- where on the body, health and safety considerations, and answers most of the concerns raised. Consult this memorandum at: http://badge.lanl.gov/documents/MM882.pdf.

A Newsbulletin article on appropriate wearing of one's badge was adapted by the Badge Office and can be found on the Badge Office Web site, at http://badge.lanl.gov/faqs/moreinfo_grimler.shtml. While the Laboratory, to date, has not had a formal policy on consequences of wearing one's badge off of Laboratory property, there have been general statements, and Lab workers are encouraged, to alert individuals who are wearing their badge in public places that this is inappropriate. This is within the concept that we are all responsible for security at the lab. A LANL badgeholder is expected to wear his/her badge whenever on Laboratory property, which includes "public" places such as the Otowi cafeteria.

If a badge is contaminated, arrangements should be made through the individual's Laboratory manager to report the situation. As long as the badge can be accounted for and its destruction assured and validated, the Badge Office can reprint the same badge. The Badge Office does require procedures to definitely account for the badge and assure its destruction before reprinting the badge. To date, no badges have ever been reported to the Badge Office as radiologically contaminated, thereby raising an ESH concern about returning it.

Specifically addressing the Wellness Center, on the one hand, it fits within the definition of Laboratory property. On the other hand, there are potential safety issues as recognized by DOE/LAAO in the above-cited memorandum. Once a person has been verified by the Wellness Center to have a valid LANL badge, it should be possible for the Wellness Center to develop reasonable arrangements within the confines of its buildings that do not interfere with the purpose for which badgeholders go there and also which ensure protection of the badges so that it does not fall into unauthorized hands.

Q: What is the proper protection measure for badges once you leave work if you are not going directly home (we are not suppose to wear the badge and we are not suppose to leave it in the car, so what should an employee do with the badge)?

A: Common sense rules on properly protecting one's badge after leaving Lab property. The first point, which cannot be stressed enough, is to remove the badge after leaving lab property and to not display it in public places. If the badge is removed in one's car, it should be kept out of view, i.e., kept in the glove compartment. Generally, once home, keep the badge at home, but in a place where it will be remembered whenever one is going to go to the lab. There is no policy that a badge cannot be left in a car, only that it should not be left in public view in a car while the badgeholder is not in the car.

Badges (Continued)

Q: On official travel are we allowed to wear our badges on other DOE sites or do we have to check in as visitors, for example Sandia?

A: The governing document, the DOE Badge Program, mandates that a DOE Standard badge issued by one site shall be accepted at any other DOE site. There may be additional site requirements, but a LANL-issued DOE Standard badge is required to be accepted by all other sites (e.g., Sandia National Laboratories) and would be worn there. You should always contact the Laboratory Visitors Center before your trip to determine whether or not they have additional requirements.

Q: 12 different organizations raised questions and concerns about Laboratory ID cards, as well as use of the LANL Badge as ID.

A: Complete information on the allowable use of the badge as ID can be found at:
LANL Memorandum on use of the badge as identification.
http://badge.lanl.gov/documents/MM1056.pdf.
FAQ on why the Laboratory no longer issues ID cards provides much background info:
http://badge.lanl.gov/faqs/moreinfo_idcards.shtml.
Note that no other DOE site's Badge Office that LANL benchmarked with issues picture ID cards in addition to the badge-this is not the mission of Badge Offices and represents a duplication of effort.

Q: Encoding Sigma levels and special access info on the badge for the magnetic readers would be helpful.

A: Encoding requirements for the badge (if by that is meant the data encoded onto the badge's magnetic stripe) is set by DOE and LANL is not permitted to develop unique encoding protocols for the DOE standard badge. In order for LANL site-specific badges (e.g. visitor badges) to work in Lab readers, an analogous encoding protocol must be followed-by doing this, even site-specific badges will work in the readers maintained by S-3 and CCN-4, the two groups which, between them, are responsible for most of the badge readers at the lab.
In the kind of integrated data environment represented by the badging system implemented in September 1999, it is, in principle, possible to develop badge reader controls which can identify the individual swiping a badge, and if certain auxiliary conditions are not met (e.g., Sigma authorizations, which are maintained in the Lab's Signature Authority System) deny access to the individual. While no facility has apparently done this yet, it is, in principle, feasible. It is a more robust approach because it could check Sigma authorities in "real time" instead of having them "hard wired" into the badge.

Q: Consistency in badging at DOE Sites

A: Sense of comment is unclear. In order to respond, we need more detail on the specific point involved.

Badges (Continued)

Q: On a side note, but just as important, can you guys find some sort of way we can wear our badges around our necks, and not have them flipped over 50% of the time??? I have tried wider bands, clipping the badge to the sides of bands, wearing keys below to weight the bands, and my badge is still upside down at least half the time. I would like to see a badge clearly displayed on all people that are hanging around my work area, and 50% of the time all I can see is the back of a badge - an electronic strip and small print, no color, no picture. While I have ideas on securing the cyber stuff, I am at a loss as to a way to keep badges upright without having to clip them directly to my clothes!! And since I wear mostly collarless shirts, and I am, well, rather "curvy", clipping them to my clothes is not a good option. Plus, if I began clipping badges to my shirt, it still does not help me identify all the people on the hallway and around the facility that are sporting flipped badges! Believe me, cyber security is VERY dependant on physical security, and badge identification is a large part of physical security. There are ways to bypass a fence, and a person would never be questioned once he is inside because he has a badge "displayed". - See e-mail for rest of Suggestion

A: There are a variety of different badge accessories to attach the badge to, contain the badge, etc., and the specific choice depends on personal preference, functionality, conditions under which the individual does his/her work, etc.
For this reason, the Badge Office set up a JIT (Just in time) mode by which a group office can purchase supplies-it provides for greater choice and products of somewhat superior quality to the basic supplies the Badge Office's budget permits it to distribute to individual badgeholders. In addition, there are fairly sophisticated lanyards that DOE does not support the Lab supplying to its badgeholders, but which may be purchased by the individual (available commercially in the Los Alamos town site) that may meet the need to ensure the badge is always turned face outward, as required. The list of JIT badge supplies and accessories may be found at: http://badge.lanl.gov/jit.shtml.
One suggestion is to place the badge inside a clear pocket which has a clip on it-the clip can then be attached to most types of lanyards (necklaces) in a way that it will not spin around a face backwards.

Q: I have a Q-clearance, but am denied entry by a badge reader--should I go to the Badge Office or can I tailgate in with someone else?

A: Do not tailgate in with someone else. There is usually a legitimate reason why ones badge does not work. You should contact your Group Administrator and have them check the status of your badge through a web query. If the query indicates that your training is current, contact the Badge Office.

Badges (Continued)

Q: White changeover badges still work in badge readers at the CMR. We weren't supposed to turn them in, but we aren't protecting them any longer since the badge changeover. How should employees be handling their white badges?

A: Use of the plain white access card (not a badge) was discontinued Lab-wide approximately 2 years ago. Any badge reader managed by either S-3 or CCN-4 (formerly CIC-4) were reconfigured to work directly from the badge, not from the white access card.
If any facility-specific systems, such as that at the CMR, exist that continue to accept the white card, that facility should make its own arrangements on terminating the acceptability of the white card. Proper disposal of the white card should follow. This is the first time in a long time that the Badge Office has become aware that the white card might still be accepted at any badge reader at LANL.

Q: The Gray Uncleared LANL badge is trouble waiting to happen. I have been told of several cases where it was mistaken for a Blue Badge due to lighting conditions, etc. Perhaps changing the color or attaching the badge with a colored clip (similar to PSAP) would help mitigate this problem.

A: The Department of Energy sets the specification requirements for the badge, including the colors designating Q-cleared (blue), L-cleared (yellow) and uncleared (gray). To date, this is the first comment received since the new badges began being issued in September 1999 about confusing the gray color with blue. Overall, the response has been very positive, with most comments indicating a great improvement in distinguishing clearance through badge color coding. Unfortunately, even if there was a widespread concern about the use of gray (which there has not been, either at LANL or other DOE sites which LANL benchmarks with) no change to the badge could be made unilaterally-it must be authorized by DOE.

Q: Could the personnel badge be used to track personnel, assure need to know, and other attributes?

A: LANL-issued badges provide for several mechanisms to track personnel-the reverse side of the badge shows the bar-code for both the individual's Z number and badge serial number-thus a capability exists to track the badge and the individual for various work-related purposes.
As to "need to know", if by this is meant Sigma approvals for weapon data access, LANL has determined that the badge is not the best mechanism to do this, since one's need-to-know requirements may change as a result of circumstances that the badge cannot track. For this reason, the Laboratory uses the Signature Authority System to track Sigma authorizations of Laboratory workers.

Miscellaneous

Q: Many of BUS employees work out in the "field"-areas that they may not be familiar with-security is your responsibility. Be aware of the areas you are visiting and conform to their rules.

A: Work with the Division's (the Division you're going to be assigned to) to find out more about the security rules for the area. The URL for the OSSO listing can be found at: http://int.lanl.gov/orgs/s/documents/labossolisting.doc.

Q: The Help Desk may improve this situation but they need an excellent list of subject matter experts or points of contact for all the work we do in S. Recommend a periodic review and update.

A: The Help Desk relies on their list of SME's which comes directly from the S Division Group Leaders. Periodic review and updating of the SME listing is done.

Miscellaneous (Continued)

Q: Can you disclose that you work in TA-55 if asked?

A: Yes. If someone asked you if you work at TA-55. it is OK to tell them you do; however, non work related questioning in a social environment should be considered logically, and if the questioning seems unusual or of an over interested nature, it would be best not to elaborate.

Q: What happens to suggestions?

A: All suggestions, comments, concerns, etc. are forwarded to the appropriate Subject Matter Expert for comment.

Q: OSSO's need to be involved in those implementations and then share them with the Division. These are also good things to discuss at labwide OSSO monthly meeting.

A: Start with any improvement that you have been able to implement within your group and share them with your division and the Help Desk...i.e. actively implement the buddy-system.

Q: It was mentioned that it might be helpful to have a 24 hour hotline for security questions.

A: Emergency after hours security issues can be reported to PTLA, at 7-4437. PTLA will then notify the S Division on call Duty Officer.

Q: Who will pay for increased security measures (engineered)?

A: Costs associated with ISSM in line organizations are absorbed by the organization. ISSM activities above the line organization are being assessed and no decision as to costs and cost alignment have been made to date.

Q: Are the security information cards still current? Do we still need them?

A: No. The security information cards are not current, and you don't need them.

Q: What does the lab spend on the patent effort?

A: Legal fees are approximately $1,000,000 per year, but there is a lot more to consider than just that. For more information please contact the Laboratory's legal office.

Q: The Laboratory should require that a Security Manager's name be added to the standard emergency call-out signs on buildings.

A: The standard emergency call-out signs on buildings have an emergency contact number (EM&R, 7-6211), which will ring to PTLA after hours. PTLA will immediately notify the S Division on call Duty Officer for all security related incidents.

Q: The Laboratory should institute a "security-all" email listing to disseminate concise/meaningful security awareness messages that are pertinent to all employees.

A: There is a listing for all Division/Program "OSSO's at the laboratory. Currently all security awareness messages are sent to them, and it is their responsibility to disseminate the information to their organizations.

Q: There should be a lab-wide security ombudsman to objectively evaluate employee's concerns.

A: The Security Help Desk acts as a liaison for all security concerns. Security issues are worked through individual LANL Division Security representatives, as well as representatives from Security Division.

Miscellaneous (Continued)

Q: Does the lab provide legal defense for people accused of willful violations?

A: The University will provide an employee with a legal defense in a civil enforcement proceeding where the employee has acted within the scope of his or her employment and where there is no evidence to suggest that the employee acted with actual fraud, corruption, or malice. Additionally, the University may, in its discretion, pay fines imposed on the employee if it finds that:
the fine is based on an act of the employee acting within the course and scope of his or her employment;
At the time of the act giving rise to the fine, the employee acted or failed to ct, in good faith, without actual malice and in the apparent best interests of the University;
Payment of the claim or judgment would be in the best interests of the University.

Although it is not required to do so, the University may, in its discretion, provide for the defense of a criminal action brought against an employee or former employee if:
The criminal action is brought on account of an act or omission in the scope of his employment as an employee
The University determines that such defense would be in its best interests and that the employee acted, or failed to act, in good faith, without actual malice and in the apparent interests of the University.

Please login to the Management Walk-Around System!

Warning - For security related MWA entries ensure your comments are unclassified - consult with an Authorized Derivative Classifier (ADC) if in doubt.

Enter your Z number and Token Card passcode:

Z number [ ] **Passcode** [ ]

Enter Clear

Guidance Cards | Introduction and Orientation | Frequently Asked Questions
Lessons Learned Resources | LANL Operating Experience Summaries

The **Management Walk-Around System** brought to you by The IM-8 Remedy Team

For information concerning the Management Safety Walk-Around Program contact Jim Loud - AA-2

Copyright 1997 UC 25 - March - 1997

***** NOTICE *****

This is a Federal computer system and is the property of the United States Government. It is for authorized use only. Users (authorized or unauthorized) have no explicit or implicit expectation of privacy. Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized site, Department of Energy, and law enforcement personnel, as well as authorized officials of other agencies, both domestic and foreign. By using this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of authorized site or Department of Energy personnel. Unauthorized or improper use of this system may result in administrative disciplinary action and civil and criminal penalties. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use. LOG OFF immediately if you do not agree to the conditions stated in this warning!

Lessons Learned Resources

Learning from the past to improve the future

LESSONS LEARNED: An operational experience that causes a worker or organization to change a process or activity to improve the safety, efficiency, or effectiveness of the process or activity.

Share Lessons Learned

Lessons Learned Network

Lessons Learned Database

Lessons Learned Programs

Lessons Learned Contacts

Lessons Learned Other Resources