Annual Security Refresher

Self-Study #1425

November 2008

Los Alamos NATIONAL LABORATORY EST. 1943

Operated by Los Alamos National Security, LLC for NNSA

Questions about this course?

Technical Content:
Security Help Desk Team
5-2002
security@lanl.gov

Course Design:
Security & Safeguards Training Team
safeguards-security@lanl.gov

Course Credit:
Security Training Registrar
5-7844 phone
5-7953 fax
ss-registrar@lanl.gov

Course Manager:
Stephen Bonner
Security and Safeguards Training Team

Editor:
Susan Basquin
IRM-CAS

Course Number: 1425
Date: November 2008
Controlled Document Number:
Annual_Security_Refresher_SS_1425,R3

This document was reviewed by an ADC in March 2008 and contains no classified information.

Contents

Introduction

Course Overview

This course, *Annual Security Refresher Self-Study* (#1425), is designed to refresh Los Alamos National Laboratory (LANL) workers with

- the knowledge necessary to perform work securely,
- a review of the basics of Integrated Safeguards and Security Management (ISSM),
- computer security refresher requirements for all computer users,
- Technical Surveillance and Countermeasures (TSCM) refresher requirements for all Laboratory workers, and
- a reminder to reference security requirements documented in implementation support documents (ISDs).

Course Purpose

Although this course is required for all workers at LANL, it satisfies requirements for different groups of workers:

- It provides the *Annual Security Refresher,* which is required for all active clearance holders.
- It provides the *Annual Computer Security Refresher,* which is required for all computer users.
- It provides the *Technical Surveillance and Countermeasures Security Refresher*, which is required for all Laboratory workers.

Each employee is required to complete the ASR every year. Failure to complete the ASR before your training expiration date will result in badge deactivation, which will deny you access to some LANL facilities. Employees who hold a security clearance and do not complete the ASR may have their security clearance suspended.

Course Objectives

After completing the *Annual Security Refresher* awareness training, you will be able to identify security requirements for LANL, which are derived from the Department of Energy (DOE) Safeguards and Security Program and Los Alamos National Security (LANS) guidelines.

After taking this course, you will be able to

- identify general security requirements,
- identify the fundamental concepts of the ISSM process,
- identify physical security requirements,
- identify personnel security requirements,
- identify cyber security requirements, and
- identify classified and unclassified controlled matter security requirements.

Target Audience

This course is required for all workers at Los Alamos National Laboratory.

About This Course

This self-study course consists of an introduction and five modules—General Security, Physical Security, Personnel Security, Cyber Security, and Classified and Unclassified Controlled Matter Security—and a resources module.

You will find a link to request course credit at the end of this online course. If you have difficulty accessing the course credit webpage, please contact your training coordinator (TC), the Institutional Training Services Group (CT-ITS) registrar at 667-0059, or the Security Awareness Program office at 667-5984.

Limitations

The completion of this course does NOT authorize you to perform escort duties. To perform escort duties, you must complete institutional escort training, course #18366, *Escorting U.S. Citizens in Security Areas*. Workers intending to perform escort duties may also be required to take site-specific escort training.

Resources

At the end of this self-study manual, you will find a discussion of the various security resources at the Laboratory, pertinent telephone numbers, and a list of acronyms.

Photo courtesy LANL archives

Module 1: General Security

Module Overview

This module describes the ISSM process at Los Alamos National Laboratory and presents and analyzes a lessons learned security incident. It also discusses the Security Inquiry Team (SIT) and directs the reader to ISD 201-1, *General Security*, for requirements supporting LANL policy.

The ISSM program is a complement to the Integrated Safety Management (ISM) program; more information about ISSM implementation at LANL is available in the Integrated Safeguards and Security Management system description (SD**).** The ISSM program applies to all workers at the Laboratory.

Module Objectives

When you have completed this module, you will be able to

- identify general security requirements as they relate to ISSM core functions and guiding principles,
- identify general security requirements as they relate to the SIT, and
- recognize that ISD 201-1 contains guidance on general security requirements.

Integrated Safeguards and Security Management

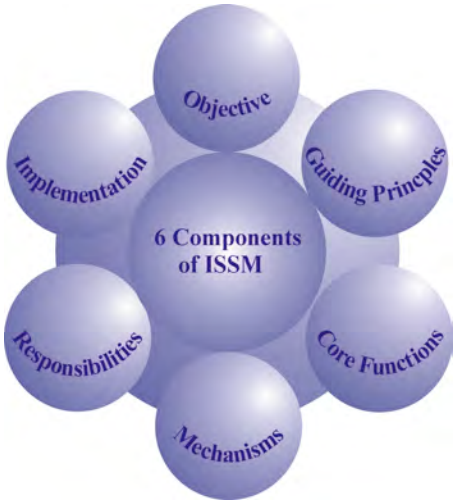
All employees have a security responsibility

ISSM establishes security expectations for employees at LANL. All employees, regardless of position, must constantly be aware of the part they play in preventing security violations.

ISSM is an employee-based security management system that promotes and supports positive security behavior through various mechanisms, such as training, lessons learned, reporting processes, the analysis of previous behavior, and the reinforcement of desirable behavior. However, ISSM is not a standard. It is a set of principles and a methodology that integrates security into all work practices at all levels by all LANL workers so that LANL can accomplish its mission securely and effectively.

The ISSM program at LANL consists of the following six components:

- ISSM objective
- ISSM guiding principles
- ISSM core functions
- ISSM mechanisms
- ISSM responsibilities
- ISSM implementation

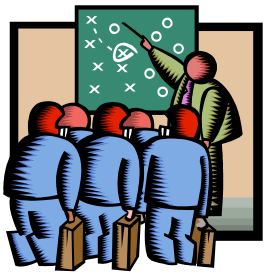


ISSM Objective

The objective of ISSM is to systematically integrate security into all management and work practices at all levels so that the Laboratory mission is accomplished while protecting security interests and striving for zero safeguards and security incidents.

Integrated Safeguards and Security Management—continued

ISSM Guiding Principles



Line managers are responsible for protecting security interests.

- All workers (managers and nonmanagers) are directly responsible for participating in ISSM to ensure that all work is performed securely.
- Line managers are directly responsible for protecting all security interests, including analysis of security risks and implementation of security controls.
- Workers and managers establish, maintain, and clearly communicate their security roles and responsibilities.
- Managers ensure that work is performed by workers who have sufficient experience, knowledge, skills, and abilities to fulfill their responsibilities.
- Managers allocate resources effectively to address security, safety, programmatic, and operational considerations while achieving programmatic goals.
- Before work is performed, the associated security risks are analyzed and security standards and requirements are established.
- Administrative and physical controls to reduce or eliminate security risks are tailored to the work being performed.
- Managers authorize the work and the workers before work is performed based on clearly established conditions and requirements.

Core Functions

- Define the Scope of Work: Set goals and objectives, identify security interests, identify security requirements, identify and prioritize tasks, and allocate resources.
- Analyze the Security Risk: Identify the security threats and analyze the security risks associated with the defined scope of work.
- Develop and Implement Security Controls: Identify security requirements, and develop and implement work-tailored security controls to prevent or mitigate security risks.

Integrated Safeguards and Security Management—continued

- Perform Work within Security Controls: Confirm that required security controls are in place and then perform work securely within controls.
- Ensure Performance: Evaluate security controls and identify opportunities for improving work definition, planning, and execution.

ISSM Responsibilities

ISSM responsibilities must be clearly established and understood by all workers (managers and nonmanagers) at LANL. The LANL document that describes the Lab's implementation of ISSM is SD 200, *Integrated Safeguards and Security Management* (found at http://policy.lanl.gov). This document states that each worker has the responsibility and authority to

- ensure that work is authorized and performed in accordance with the ISSM five-step process;
- conduct daily work within security requirements and contribute to the protection of security interests around him or her;
- report security anomalies or violations of security requirements to the security responsible line manager and the SIT immediately;
- promote security awareness, including sharing and using lessons learned from control failures, near misses, or security incidents to pursue system improvements;
- provide input or feedback, especially for the development, implementation, and improvement of security requirements and ISSM;
- seek help from deployed security representatives or the Security Help Desk regarding security requirements, methods for accomplishing a security task, or other questions, concerns, and suggestions;
- participate in security self-assessments and develop corrective actions as requested; and
- stop or pause work when there is a security concern and, if a worker observes a concern in another person's work, inform that person or his/her supervisor immediately.

ISSM Implementation

All LANL workers must participate in the implementation of ISSM by ensuring that security is integrated with all management and work practices that they plan, perform, or supervise. One of the ways this is done is through Integrated Work Management (IWM).

IWM, as described in Implementation Procedure (IMP) 300.5, *Integrated Work Management,* establishes the general expectations for the conduct and authorization of activity-level work at LANL. IWM combines work control with ISM and ISSM. This system is used to fully identify hazards and to ensure that controls are effective and procedures are workable. A hazard is defined as any source of environmental, safety, or health danger **or** *a safeguards and security threat* with the potential to cause harm to people, the environment, property, and/or national security.

The IWM process states that all LANL work is governed by the five steps, or core functions (described earlier), that are shared by ISM and ISSM. When these five steps are performed as part of preparing a work document, ISM and ISSM are included in the process.

The IWM process is truly integrated. By looking at safety, security, health, and environmental issues as part of one overall process, hazards can be evaluated and controls can be determined for each type of issue. IWM implements the processes at once.

ISSM Mechanisms

ISSM Help Resources

Security Smarts

http://int.lanl.gov/security/documents/index.shtml#security-smarts

Security Tips

http://int.lanl.gov/security/news/sectip_archive.shtml

Anatomies of an Incident

http://int.lanl.gov/security/documents/index.shtml#anatomy

ISSM Mechanisms—continued

Security Websites

(http://int.lanl.gov/security/) provides information on all security and safeguards topics

(http://int.lanl.gov/orgs/adss/) provides information about the Security and Safeguards Directorate

(http://int.lanl.gov/orgs/s/) provides information about the Physical Security Division

(http://int.lanl.gov/orgs/sg/) provides information about the Safeguards Division

Security "Brown Bag" Presentations

The "brown bag" security program is a series of periodic discussions concerning specific security topics. Contact the Security Awareness Program office at 667-5984 for this program.

Tailored Security Presentations

Any worker may request a tailored safeguards and security presentation by contacting the Security Help Desk (665-2002).

Security Help Desk

The Security Help Desk (665-2002) is a resource available to help workers from across the Laboratory resolve security-related issues.

ISSM Mechanisms—continued

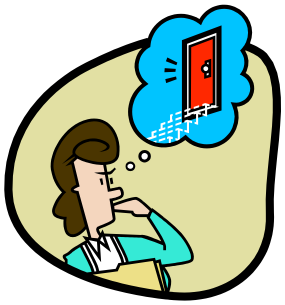
Lessons Learned

LANL workers shoulder a major responsibility for securing their work. Custodians and users who operate a vault/vault-type room (V/VTR) are responsible for properly opening and securing the V/VTR, ensuring that security is maintained, and ensuring that the V/VTR is attended at all times when open. The improper performance of V/VTR duties is a major threat to the security of the Lab. A couple of years ago, a security inquiry found several anomalies in the conduct of a VTR custodian, including the following deviations:

- Occasionally locking, but not alarming, the VTR when leaving it unattended while remaining in the Security Area (although not in the same building as the VTR)
- Locking, but not alarming, the VTR and leaving it unattended while going to lunch
- Leaving the VTR door unlocked and unalarmed for a few minutes after failing to pull on the door to ensure that it had latched or locked
- Twice trying to leave work without checking the VTR after being told to do so
- Forging a coworker's initials on a security form

In addition, the organization was allowing workers in certain VTRs to leave the VTRs locked, unalarmed, and unattended for up to one hour if the workers did not leave the Security Area. This variation from requirements had not been granted by the DOE's Los Alamos Site Office.

ISSM Mechanisms—continued



The use of the ISSM process could have reduced the seriousness of these security infractions:

- Before work is performed, security standards and requirements are established (guiding principle and core function). The use of standard security procedures instead of deviations could have prevented several of the infractions.
- Develop and implement work-tailored security controls (core function). Finding doors unlocked and unalarmed should have prompted the coworkers to add further controls.
- Report security anomalies or violations of security requirements immediately (responsibility of all employees). The coworkers were reluctant to say anything about the poor security practices of the custodian. If a worker observes a concern in another person's work, inform that person or his/her supervisor immediately.
- The custodian was often "in a hurry" or "being lazy" and generally had a lackadaisical attitude about security. Evaluations of security practices may have pinpointed the problem and allowed the custodian to be counseled or trained before major infractions occurred.

ISSM principles and practices can be applied to day-to-day work. Look around to see if they can be used in your work area.

Key Questions to Ask Yourself

ISSM can apply to both a large, formal project and to your everyday work. In considering ISSM in your workplace, you might ask yourself the following questions:

- How can ISSM help me perform the security part of my job successfully?
- When defining the work, analyzing risks, and developing security controls, do I feel included in the outcome?
- How well do I think my coworkers understand ISSM? Do they look for ways to improve security?
- Are clear roles and responsibilities defined in my work? Are my coworkers and I empowered to stop work if necessary?
- Are my work and workplace secure? Are there ways to make my work environment more secure?

Security Inquiry Team

The LANL SIT evaluates security events to determine if the events are incidents of security concern (IOSC). The SIT

- collects and evaluates initial information;
- determines the IOSC category;
- assists organizations in timely identification and mitigation of vulnerabilities;
- makes initial notifications;
- conducts inquiries; and
- provides detailed inquiry reports of IOSC, which form the basis for causal analyses and corrective actions.

IOSC are categorized by an impact measurement index (IMI) ranging from the most serious (IMI-1) to the less serious (IMI-4).

The SIT produces and distributes extensive weekly and monthly statistical reports to LANL managers, security program leads (SPLs), deployed security officers (DSOs), and others. These statistical reports are a key asset to LANL managers in preventing and addressing IOSC.

Reporting Requirements

All LANL employees are required to immediately report known or potential security incidents to the SIT and their responsible line manager (RLM).

Reports must be made to a SIT inquiry official in person or by phone and may not be emailed or left on voice mail. Ensure that potentially classified information is discussed only by way of secure means. After normal business hours, contact SOC Los Alamos to report any known or potential security incidents.

Potential Federal Fines

Under federal law (10 Code of Federal Regulations [CFR] 824), LANS can be fined up to $100,000 **per day** for each classified information security violation.

Guidance for General Security Requirements

ISD 201-1, *General Security* establishes implementation requirements supporting the LANL policy established in IMP 201, *Safeguards and Security*.

This ISD contains the requirements for

- ISSM implementation;
- Safeguards, Security, and Counterintelligence Awareness Training; and
- reporting incidents of security concern.

These requirements apply to all Laboratory workers.

Note

To resolve any questions about

- Security and Safeguards training, contact the Security Integration Group (PS-2), 5-7565, or CT-ITS, 7-0059;
- Cyber Security training, contact Chief Security Officer-Cyber Security (CSO-CYSEC), 5-1795; or
- Counterintelligence awareness and training, contact ISEC, 5-6090.

Module 2: Physical Security

Module Overview

Physical security is more than just “guns, guards, and gates.” To help workers identify and meet physical security requirements, LANL has consolidated the requirements into one guidance document, ISD 201-2, *Physical Security*. This ISD presents the processes and methods for implementing physical security requirements established in the LANL Site Safeguards and Security Plan (SSSP) and policies established in IMP 201, *Safeguards and Security*.

In this module, you will review the physical security requirements for access into Security Areas, the use of prohibited and controlled articles and devices, the photography policy, and policies for technical surveillance countermeasures.

Module Objectives

When you have completed this module, you will be able to identify physical security requirements discussed in the following sections of this module:

- Security Areas
- Protective Force (SOC Los Alamos)
- Controlled and Prohibited Articles
- Photography Policy
- Technical Surveillance and Countermeasures
- Guidance for Physical Security Requirements

Security Areas

LANL uses various methods to safeguard and secure its resources, including controlling access into specific areas of the LANL complex.

Property Protection Areas

All LANL-owned or leased facilities (other than established security areas) are considered Property Protection Areas (PPAs). PPAs are not authorized for storage or processing of classified matter; they are established to protect government-owned property against damage, destruction, or theft. Access into a PPA may be controlled.

Security Areas

Security Areas are designed to contain classified matter and/or nuclear materials. Types of Security Areas include

- Exclusion Areas,
- Limited Areas,
- Material Access Areas, and
- Protected Areas.

Access into a Security Area is usually controlled by a badge reader and hand geometry unit or PIN pad.

Security Areas are generally restricted to L- or Q-cleared employees. Some areas, such as the National Security Science Building (NSSB), are restricted to Q-cleared employees or escorted L-cleared or uncleared personnel.

Photo courtesy LANL archives

Security Areas—continued

Tailgating

Only those individuals with authorized access should be present in a PPA or a Security Area. “Tailgating” is not allowed. Tailgating occurs when someone enters an area behind an employee with authorized access without having his or her access authorization verified.

Piggybacking

“Piggybacking” (also known as vouching) is **no longer allowed** anywhere on LANL property where badge access authorization is required. Piggybacking occurs when an employee with access authorization allows an individual to enter an area with him or her by verifying the individual’s access authorization via badge examination.

Protective Force

“We proudly serve our nation by providing vigilant and ever-present protection that enables the Los Alamos National Laboratory to make the world a better and safer place.” SOC Los Alamos vision statement

SOC Los Alamos (formerly Protection Technology Los Alamos, or PTLA) is LANL’s subcontractor charged with providing a uniformed protective force that helps protect LANL’s varied assets. SOC Los Alamos achieves its mission to protect LANL through training, professionalism, respectfulness, and demonstration of teamwork. As a LANL employee, you must also demonstrate respect toward Protective Force officers so that they can effectively accomplish their mission.

Protective Force Yesterday: Photo courtesy LANL archives

Protective Force—continued

Protective Force Today: Photo courtesy LANL archives

When SOC Los Alamos officers direct employees to do something, employees must follow their directions. At the scene of an emergency, officers are not obligated to respond to questions, offer explanations, or justify their instructions. Although officers are trained to be courteous, they are also trained to take control of any situation.

LANL personnel who interact inappropriately with SOC Los Alamos officers will be identified, a security incident report will be prepared, and the incident will be referred to Human Resources Staff Relations and line management for appropriate action.

For issues involving the conduct of SOC Los Alamos officers, please contact the SOC Los Alamos shift commander.

Controlled and Prohibited Articles

There are restrictions on portable electronics and storage devices at LANL. Do not bring any portable electronics or storage devices into LANL Security Areas unless approval has been obtained. Do not connect any non-LANL-owned device to LANL networks or computers without approval.

Controlled and Prohibited Articles—continued

IPODs and other portable electronic devices are prohibited in Security Areas.

Portable electronic equipment and storage devices should NEVER be brought into an area with classified computers unless the device is an approved part of the classified system or a risk assessment has been performed and approved. *P217 Portable Electronic Devices, January 2008.*

Consult your organizational computer security representative (OCSR) for help in obtaining approvals for portable electronics and storage devices.

Vault and Vault-Type Rooms

Controlled/prohibited article restrictions apply to vaults and VTRs. Prior authorization is required if any item that is considered a controlled article needs to be inside a vault for official business purposes.

Controlled Articles

Controlled articles are items not permitted in Security Areas without **prior** authorization by Physical Security and/or Cyber Security. Controlled articles are items that are capable of recording information or transmitting data (radio frequency [RF], infrared [IR], and/or data link) and may include the following equipment and restrictions:

- Equipment with RF, IR, or any other wireless transmission capability, such as cell phones, cordless phones, two-way pagers, and two-way radios; however, government-owned cell phones are allowed in Security Areas **if** the battery has been removed (they can be used in an emergency)
- Permanently installed vehicle telephones and radios may enter a Security Area but must **not** be turned on
- A personal cell phone or government cell phone may be used outside the perimeter of a Security Area
- Recording equipment (audio, video, optical, or data)
- Cameras (film or digital, video or still)
- Court-ordered electronic monitoring devices (“ankle bracelets”)
- Portable computers, such as laptops, personal digital assistants (PDAs), palm-top computers, Blackberrys, or iPods
- Copiers or scanners with hard drives

Controlled and Prohibited Articles—continued

Prohibited Articles

Prohibited articles are those items not permitted on LANL property, including parking lots, unless approved in advance by the Internal Inquiries Group (SAFE-2). The following articles are prohibited:

- Dangerous or deadly weapons, explosives, or other instruments or materials likely to cause substantial injury or damage to persons or property
- Alcoholic beverages, including unopened bottles or cans
- Controlled substances such as illegal drugs and associated paraphernalia, but not prescription medicine that is prescribed to the person in possession
- All items prohibited by law

Lessons Learned

LESSONS LEARNED

Cell phones are controlled articles and are not allowed within a security area because of their potential to unintentionally transmit classified matter. Because cell phones are small and lightweight, it is easy to slip one into a pocket or bag and forget that it is there. This happened to “Julia.”

Julia was rushing one morning to get to work and to get her daughter off to college. She was also waiting for an important call that morning so she put the cell phone in her back pants pocket while they hurriedly loaded her daughter’s car. After her daughter drove away, Julia went to work, forgetting she had the cell phone in her pocket. When she arrived in her secure office area, the phone rang. She immediately removed the battery from the phone, without answering the call, and then returned the phone to her car. She then reported the incident to the SIT and to her RLM.

The day of the incident, Julia was operating outside her established routine as she rushed to get her daughter off to school. Julia had used a cell phone for three years and purposefully never placed her cell phone in a bag, pocket, or anything else that would conceal it.

Controlled and Prohibited Articles—continued

To ensure that this does not happen again, Julia has programmed her phone to sound an alarm at 7:50 a.m., the time she is usually pulling into the parking lot. This forces her to acknowledge the location of her phone. This action is part of ISSM—Julia developed effective controls to prevent a known security risk.

Note: *To prevent the same type of event, another group has hung a toy cell phone (made of foam) at the entrance to their secure area. Employees can't enter without noticing the toy and thinking of their own cell phones. Think about a unique way to apply the ISSM process to prevent commonplace security infractions in your area.*

The Photography Policy

This section contains highlights of Notice 184.1. Read Notice 184.0 to understand the photographic policy in its entirety.

Camera use on LANL property requires appropriate prior authorization. A camera is defined as a photographic device that captures still or video images, either digitally or on film. A multifunction device with photographic capability (e.g., a camera cell phone) is considered a camera.

Cameras have changed over the years at LANL, but the photography policy has remained consistent.

LANS- or DOE-employed camera users must obtain approval from their RLM if they will be using a government or non-government-owned camera on LANL property. Camera users who are not employees of LANS or the DOE must obtain the same approval and make their request through the appropriate LANL oversight personnel for the work being performed at LANL (e.g., construction subcontractor employees must submit a request for authorization through the LANL project manager of the construction project).

The Photography Policy—continued

If you are a camera user, you must complete the following requirements for authorization:

- Submit a request describing the camera activity to your RLM.
- If granted approval, carry the RLM authorization (email or letter) while using the camera. Possession of the letter constitutes agreement to the conditions in the letter.
- While using a government-owned camera outside or inside a Security Area or if using a non-government-owned camera outside a Security Area, have a valid DOE/LANL badge.
- While using a government-owned camera on LANL property, have a valid LANL property pass.
- Maintain control of the camera(s), and control all images taken with the camera(s) until the images are reviewed. Images are to be treated as official use only (OUO) until the review process is completed.
- Once photographic or moving images have been taken, have your images reviewed as outlined in the authorization letter. Review of images by an authorized derivative classifier (ADC) may be required if specified in the authorization letter.

RLMs are responsible for the authorized use of government- and non-government-owned cameras for official business on LANL property. RLMs may need to coordinate authorized camera use with other organizational RLMs depending on the location where the camera user will use the camera. DSOs are available to assist with contacting other RLMs. Approvals may be in the form of an email or dated letter to the camera user. The letter must contain required conditions and restrictions for camera use including a description of the content review process.

RLMs must ensure that the camera user understands and follows the camera user responsibilities and the guidance in the approval letter.

Protective Force (SOC Los Alamos) and Physical Security Division (PS) personnel are authorized to challenge persons using cameras anywhere on LANL property and will validate “authorized use” in accordance with the requirements stated above.

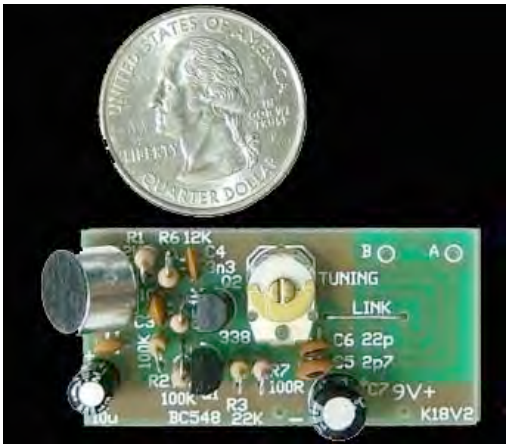
The Photography Policy—continued

If use is authorized, no content review by SOC Los Alamos or PS personnel is required and the camera user may resume activity after the Protective Force officer verifies authorization and collects data to complete a report.

If use is not authorized, a report will be taken and the contents of the camera will be reviewed. If a camera user refuses to relinquish cameras or film, he or she will be instructed to leave LANL property. If he or she refuses to leave LANL property, he or she may be arrested for trespassing.

Technical Surveillance Countermeasures (TSCM)

The TSCM Program is designed to detect, deter, isolate, and nullify technical surveillance penetrations and technical security hazards. TSCM technicians use several techniques and a variety of electronic and electrical equipment to detect illegal devices designed to listen and/or transmit information. These illegal devices are more commonly known as "bugs."



Miniature "Bug"

Technical Surveillance Countermeasures (TSCM)—continued

All LANL employees should be aware of the TSCM threat, which can come from an insider or an outsider. You can take the following precautions to reduce the threat of TSCM:

- Be alert to strange or unauthorized personnel performing maintenance in your area.
- Listen for strange occurrences when using your telephone, such as clicking noises, callers complaining about one line being busy most of the time, long delays in dial tones when you pick up the receiver, echoes in your phone during local calls, or telephone repairmen on your telephones without your request.
- Be aware of your surroundings, especially changes to furniture, clocks, and other office furniture.

In the event that you suspect or become aware of a technical surveillance penetration, take the following steps:

1. Stop all classified discussions while maintaining other normal activities in the area.

2. Protect the area so that the suspected device can't be removed.

3. Immediately report the incident to your RLM and the TSCM Team, but do so away from the area where the threat is believed to be. Keep in mind that

   — any requests for TSCM services are classified as Secret/ National Security Information (S/NSI) and must be arranged by a secure means (in person, classified hard-copy correspondence, or secure communications methods); and

   — if reporting cannot be done by a secure means, simply state that you need to talk to a member of the TSCM Team immediately.

If you are on travel to a foreign country and suspect that your equipment has been tampered with during your stay, you must contact the TSCM Team upon your return. Do not take the equipment into any Limited Areas.

Upon returning from travel to a sensitive country with LANL electronic equipment (e.g., laptops, PDAs, government-issued cell phone, etc.), you must notify the TSCM Team and submit your equipment for inspection.

Guidance for Physical Security Requirements

ISD 201-2, *Physical Security*, establishes implementation requirements supporting the LANL policy established in IMP 201, *Safeguards and Security*.

This ISD contains the requirements for

- Security Areas,
- V/VTRs,
- PPAs,
- security locks and cores,
- prohibited and controlled items, and
- escorting uncleared U.S. citizens in Security Areas.

These requirements apply to all Laboratory workers.

Module 3: Personnel Security

Module Overview

While everyone on Laboratory property or Laboratory-lease property is required to have an official LANL badge, only Laboratory workers who perform classified work have the need for a security clearance. Their access to classified information is determined by proper clearance level and the need-to-know.

The granting of a security clearance and the completion of the Comprehensive Security Briefing culminate in a cleared individual signing the Classified Information Nondisclosure Agreement, Form 312. This legal document binds the cleared worker to protect sensitive and/or classified matter (information in documents or media, parts, or any combination) from unauthorized disclosure both during and following his or her career at the Laboratory.

This module reminds workers of requirements for

- security badges;
- security clearances;
- Human Reliability Program (HRP);
- Operations Security (OPSEC);
- Counterintelligence (CI);
- hosting cleared visitors and hosting visitors for unclassified purposes;
- official visits by cleared Laboratory workers to other sites having security interests;
- official travel to foreign countries; and
- foreign ownership, control, or influence (FOCI).

These requirements are documented in ISD 201-3, *Personnel Security*.

Module Objectives

When you have completed this module, you will be able to identify personnel security requirements addressed in the following sections of this module:

- Clearances: Reporting Requirements
- Security Badges
- Escorting
- Substance Abuse
- Violence in the Workplace
- Office of Counterintelligence
- Guidance for Personnel Security Requirements

Clearances: Reporting Requirements

DOE identifies the following reporting requirements for employees who currently possess a DOE security clearance (L or Q) or are in the process of obtaining a DOE security clearance.

Employees and Managers

In order to fulfill DOE reporting requirements, the Personnel Security Group (PS-3) must receive the information from employees and managers concerning the following situations:

- An applicant declines the offer of employment or fails to report for duty.
- Termination of employment (the employee must complete DOE F 5631.29, *Security Termination Statement* within two working days of termination).
- Nonutilization of access authorization for 90 working days.
- An employee is on a leave of absence or on extended leave and will not require access to classified information, classified matter, or special nuclear material (SNM) for 90 consecutive working days. (The employee must complete a DOE F 5631.29 Security Termination Statement.)

Clearances: Reporting Requirements—continued

90-Day Policy

Note: *The DOE now requires the Laboratory and other sites to terminate the clearance of any worker, including temporary workers such as consultants, guest scientists, students, associates, etc., who does not use his or her clearance at least once every 90 working days. Also, workers are required to surrender badges to Personnel Security before an extended absence or after a limited-term work assignment.*

Previously, the Laboratory was permitted to deviate from this policy, which is stated in the DOE Manual 470.4–5, Personnel Security, Attachment 2–13, Contractor Requirements Document (CRD), paragraph 7.c.(3), 08-26-05:

> *Access Authorization Termination Requests. The contractor must request that the DOE processing personnel security office(s) terminate an employee's access authorization and must provide a DOE F 5631.29, Security Termination Statement, completed by the employee whenever any of the following occur:*
>
> *(3) the individual is on a leave of absence or on extended leave and will not require access to classified information or matter, or SNM, for 90 consecutive working days. Upon request, this interval may be adjusted at the discretion of the DOE processing personnel security office;*

Additional information is online:

http://www.hss.energy.gov/indepOversight/SecEvaluations/directives/m4704-5.pdf

- Access to classified information or matter or to SNM is no longer required to perform assigned job duties.
- The employee leaves for foreign travel, employment, assignment, education, or residence of more than three months (see 2.4.6 of hyperlink) not involving official U.S. government business. (This requirement applies even if the employee remains employed by the contractor.) (See same requirement under *Recovering Security Badges*.)

Clearances: Reporting Requirements—continued

- An employee is transferred from one company to another. (The manager must complete DOE F472.1c. The employee must complete DOE F 5631.29, *Security Termination Statement* and go to the PS-3 office to complete the transfer before being re-badged with the new company.)
- An employee who holds a clearance is hospitalized for mental illness or has received other treatment for a condition that, in the supervisor's opinion, may cause a significant defect in the individual's judgment or reliability.
- When employees and/or managers are aware of information of personnel security interest (e.g., espionage, sabotage, treason, terrorism), such information must be characterized as reliable and relevant and must create a question as to an individual's access authorization eligibility as exemplified in 10 CFR 710.8 (see the reverse of DOE F 5631.18).
- A foreign national under the contractor's cognizance becomes a U.S. citizen through naturalization or effects any other change in citizenship status.
- The contractor restricts or withdraws an employee's access to classified information, classified matter, or SNM without DOE direction.

Clearance Holders/Individuals in Process of Obtaining Clearance

The following are reporting requirements for LANL employees who hold a clearance (L or Q) or those who are in the process of obtaining a DOE security clearance:

- Provide full and truthful answers to questions
- When requested, furnish or authorize others to furnish information that the DOE deems pertinent to the access authorization eligibility process

Clearances: Reporting Requirements—continued

This condition applies

- when completing security forms;
- during the course of an initial investigation and reinvestigations;
- at any stage of access authorization processing but not limited to
  - letters of interrogatory,
  - personnel security interviews,
  - DOE-sponsored mental evaluation, and
  - other authorized DOE investigative activities.

An individual may elect not to cooperate; however, such refusal may prevent the DOE from granting or continuing access authorization. In this event, any access authorization then in effect may be terminated or further processing may be suspended.

Pre-employment Unauthorized Access (UA)

Report the following occurrences within two working days to PS-3:

- All arrests, criminal charges (including charges that are dismissed), or detentions by federal, state, or other law enforcement authorities within or outside the U.S. for violations of the law, other than traffic violations for which a fine of $250 or less was imposed, unless the traffic violations are drug or alcohol related
- Personal or business-related filing for bankruptcy
- Garnishment of wages
- Legal action effected for name change
- Change in citizenship
- Employment by, representation of, or other business-related association with a foreign or foreign-owned interest, or foreign national
- Hospitalization for a mental illness, treatment (inpatient or outpatient) for drug abuse or alcohol abuse

Clearances: Reporting Requirements—continued

Photo courtesy LANL archives

Provide notification to PS-3 or the facility security officer, as appropriate, immediately after any approach or contact by any individual seeking unauthorized access to classified information, classified matter, or SNM. If such an approach or contact is made while on foreign travel, employees should notify a Department of State official at the local U.S. embassy or consulate with a request that the Department of State report the incident to the director, Office of Security, at DOE Headquarters.

Note: *This requirement is in addition to any similar reporting requirements implemented under DOE directives or regulations.*

Provide a completed DOE F 5631.34 *Data Report on Spouse/Cohabitant* directly to the PS-3 Clearance Processing office within 45 working days of marriage or cohabitation. These forms must be obtained from the personnel security office. A name change must also be reported.

Security Badges

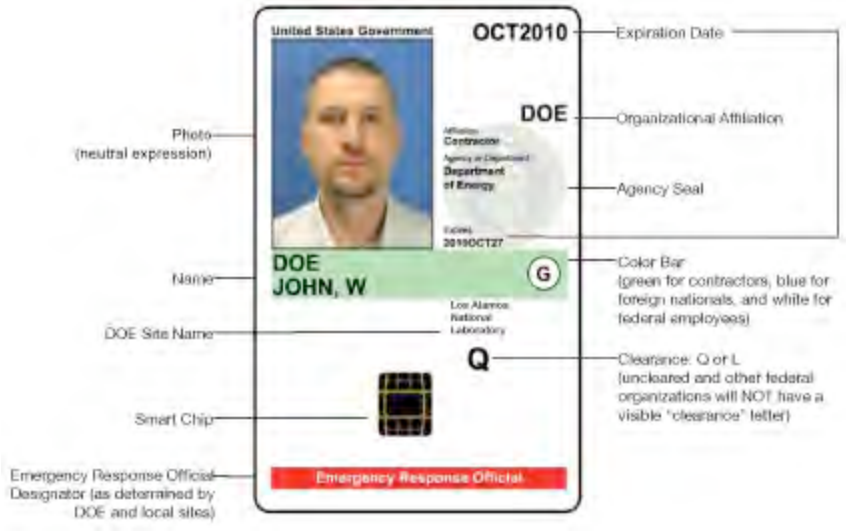
As an employee of LANL, you are issued a DOE/LANL security badge. Your badge contains information (such as your name and clearance level) that the general public does not need to know. Wearing your badge in public may make you a target, putting your personal safety and LANL's security at risk. Badge holder responsibilities include the following:

- Wear your badge, photo side out, above the waist on the front side of the body while on LANL-owned or -leased property (including the Los Alamos Research Park).
- Do not leave your badge unattended when on LANL property, including private offices.
- Remove your badge when you are not on LANL property (i.e., at restaurants, grocery stores, gas stations, the library, financial institutions, retail stores, Park & Ride bus, etc.). Remind badged visitors to remove their badges when they are off LANL property.

Security Badges—continued

- Do not use your badge for identification or unofficial purposes (e.g., cashing checks or checking into a hotel while on vacation). While on official business, your badge may be used when checking into a hotel to obtain a government discount. However, **do not surrender your badge, and ensure that no one makes a copy of the badge.**
- Report the loss or theft of your badge within 24 hours or by the next business day; immediately submit *Form 1672, Notification of Permanent Inactivation of Badge*, in person to the Badge Office.
- For more information, visit http://int.lanl.gov/security/personnel/badge/badges.shtml.

Security Badges—continued



A new federal security badge (shown above) will be used at LANL in the near future

Recovering Security Badges

Both cleared and uncleared security badges are DOE property. These badges must be surrendered

- when terminating employment,
- when a security clearance is no longer required,
- when going on extended leaves of absence of greater than 90 consecutive calendar days, and
- when the badge is no longer required.

Individuals who do not return their security badge are automatically flagged by the badging system and are precluded from further badging services as long as their badge remains “not accounted for.”

Escorting

Employees without the proper clearance level may be escorted into Security Areas, but the following procedures must be met:

- the visit is for official business that can be accomplished only in a Security Area, OR
- the visitor has a required skill or ability that cannot be performed by an individual with the proper clearance level.

The following escorting requirements are from ISD 201-2, *Physical Security*:

- An escort must take the online escort training (#18366).
- The escortee must be a U.S. citizen; if the escortee is not a U.S. citizen, contact the Foreign Visits and Assignments Office, or the Classified Visits office if the foreign national is participating in classified discussion.
- Contact the organization you will be visiting (in advance) to inform them that you will be escorting a visitor into their area.
- Ask the organization you will be visiting if there are any site-specific requirements for escorting.
- Escortees must wear a valid DOE uncleared badge or visitor badge.
- Log the visit according to the requirements of the facility you are visiting; if escorting in the TA-3 area, log the visit through the online escort log.
- Notify area occupants that an uncleared visitor/escortee is present.
- Maintain physical and/or visual and/or verbal control of the escortee at all times.
- If necessary, make arrangements to “hand off” the escortee to another approved escort who has completed escort training #18366.
- Ensure that the escortee never has access to classified matter, information, or discussions.

Escorting—continued

Nonescortable Gray Badge Holders

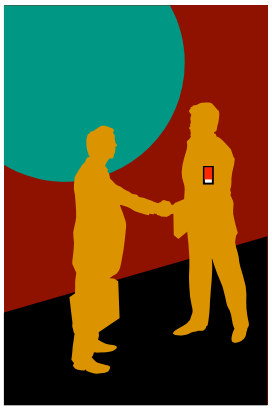
LANL has implemented a badging program to clearly identify uncleared personnel who are not permitted escorted access into LANL security areas. You must not escort a nonescortable gray badge holder. That person is not allowed into any LANL Security Area—no exceptions.

Lessons Learned

LESSONS LEARNED

Hosts and escorts take on a major responsibility when they agree to host or escort a visitor or uncleared worker. The responsibility increases significantly if the escortee is a foreign national because one must also know policies and procedures pertaining to non-U.S. citizens.

A dozen employees of the XYZ Company were to work at LANL for two weeks. Group Leader J. Jones was informed that one of the XYZ employees, S. Smith, was a permanent resident alien. The other workers were badged while Smith worked in the group office in an open area for two days, *without a badge*. During this time he was always escorted. Smith eventually received a red foreign national badge and worked at LANL for two more weeks, during which time two group workers escorted him into a Limited Area. An alert worker noticed the red-badged worker in the Security Area and questioned the escorts. Smith was immediately taken from the area, and the SIT was notified. The two escorts knew that uncleared foreign nationals were not allowed in Security Areas; however they assumed that since Jones had authorized Smith's work and they had not been told anything to the contrary, Smith could enter Security Areas. Jones, the official host, had briefed neither the escorts nor Smith as to where Smith could work, nor had Jones briefed anyone else.



The group leader failed to follow the principles of ISSM by not properly planning the hosting of a foreign national worker. Accordingly, Jones did not brief the escorts or the escortee about where Smith was allowed. Jones also allowed an unbadged worker to work on LANL property for two days. The escorts did not question taking a foreign national into a Limited Area, nor did group workers question the presence of an unbadged worker in their open area. The group members were not empowered to "question the boss" and feared retaliation in doing so.

Escorting—continued

Managers and escorts are responsible for following the ISSM process before executing work, especially work that involves a new process for them. Designated hosts must be fully aware of their host responsibilities. Workers must question possible violations of security procedures and policies.

Substance Abuse

On March 5, 2007, LANL implemented a substance abuse policy (Institutional Policy and Implementation Procedure [IPP] 732.1) to maintain a workplace that is free from the illegal use, possession, or distribution of controlled substances. The policy applies to all individuals who perform work at LANL as employees, subcontractor employees, students, guest scientists, loaned employees, or visitors.

Drug testing will be conducted

- on a random basis for all LANL employees (not including guests and affiliates) and subcontractor employees who hold a standard badge, and
- for initial hires at LANL (as LANS or subcontractor employees).

Additional drug and/or alcohol testing will be conducted if there is a reasonable suspicion or as a result of an accident or incident on LANL property. Employees will be evaluated at Occupational Medicine-Medical Services to determine the type of testing required.

Substance Abuse—continued

Positive Tests

A positive drug test is defined as a test result that shows the unauthorized presence of a controlled substance that has been confirmed by the medical review officer. If a worker refuses to be tested, the refusal will be reported and treated as a confirmed positive result. Employees who test positive for one or more illegal substances may be terminated from LANL.

Violence in the Workplace

LANL aims to provide a work environment that is free from violent behavior and threats of violence. For immediate help with threats or violence that pose a physical danger to yourself or others, call (505) 667-8730 and a special, multidivisional team will respond, review the issue, and provide a course of action to managers and officials. For more information, visit http://int.lanl.gov/health/gettinghelp/.

If there is an imminent threat, you may also dial 911. Dialing 911 from a cell phone may route your call to responders outside Los Alamos. In this instance, you may contact the Los Alamos Police Department directly at (505) 662-8222.

Office of Counterintelligence

The mission of the Office of Counterintelligence (OCI) is to protect LANL and its employees, systems, and property from foreign intelligence and terrorist activity.

OCI provides leadership in the U.S. intelligence community in support of vital energy security, nuclear security, and other national security interests. LANL's OCI includes the following programmatic elements:

- Counterintelligence and Counterterrorism
- Foreign Visits and Assignments
- Immigration Services
- Operations Security
- Counterintelligence Analysis
- Cyber Counterintelligence

Counterintelligence and Counterterrorism

While educating the LANL population about foreign intelligence threats, the Counterintelligence and Counterterrorism element of OCI attempts to detect, deter, and mitigate those threats to LANL.

Foreign Visits and Assignments

Foreign Visits and Assignments (FV&A) facilitates foreign participation in LANL/DOE projects by processing requests for approval. All foreign national guests, including individuals who have obtained U.S. permanent residency, are required to have approval before arriving at LANL.

Visits and assignments are generally confined to approved nonsecure areas. The FV&A Office of Counterintelligence policy and procedural guidance can be obtained at the Foreign Visits & Assignments (FV&A) website or by contacting FV&A.

Office of Counterintelligence—continued

Immigration Service

The Immigration Services Office (ISO) of OCI attempts to respond to the queries of our foreign national employees as they try to weave through the myriad of regulations applicable to their situation while here in the U.S.

For more information, contact the ISO office.

Operations Security

The Operations Security (OPSEC) element of the OCI helps identify and protect sensitive information and assists OCI's counterintelligence and counterterrorism awareness effort.

Five processes are critical to your success and the success of the OPSEC program:

1. Determine Critical and Sensitive Data
2. Analyze the Threat
3. Determine the Vulnerabilities
4. Analyze the Risk
5. Develop and Implement Countermeasures

OPSEC is a continuous process. Completing the OPSEC process once is not enough. You should apply the process to every project, and repeat it many times during each project.

Cyber Counterintelligence

The Cyber Counterintelligence element of OCI attempts to detect and deter and, where possible, mitigate attempts by foreign intelligence services or state sponsors of terrorism to interfere with, monitor, and/or compromise the LANL cyber infrastructure. This office of OCI has substantial interface with the Computing, Telecommunications, and Networking Division.

Office of Counterintelligence—continued

Counterintelligence and You

Threats

The intelligence threat to LANL from hostile intelligence services and terrorist networks is multifaceted. Information obtained about classified programs can be used to damage U.S. national security. Illegally acquired research and development technology could result in significant loss to the U.S.

Methods They Use

Although hostile intelligence agencies and terrorist organizations use many methods to collect information, the methods that will most concern you if you work with classified or sensitive programs at LANL are

- cyber attacks by hostile intelligence services or international terrorist entities to collect information or sabotage machines, operations, or programs;
- trained information collectors trying to elicit information from you; and
- foreign intelligence (or terrorist organization) intermediaries trying to manipulate LANL employees with knowledge about facilities or programs of interest to them toward recruitment. A person may not even be aware that he or she has been compromised; therefore it is important to take advantage of the presence of the OCI experts to help sort out an event or anomaly.

If You Are Approached

The threat from hostile intelligence services and terrorist organizations is real. You could be the target of illegal or unauthorized attempts to gain access to classified or sensitive information, technology, or SNM. You should not hesitate to contact OCI if you are concerned about an issue of counterintelligence significance and/or OPSEC matters. You must report **any** and **all** attempts to breach LANL security.

Office of Counterintelligence—continued

Contacts Must Be Reported

While employed at LANL, you must report all contacts you have—on or off the job—with individuals of any nationality who attempt to obtain illegal or unauthorized access to classified or sensitive information and may be targeting you for actual or attempted exploitation by a foreign country or terrorist organization.

Travel to Sensitive Countries

Any LANL employee and subcontractor (cleared or uncleared, U.S. citizen or foreign national) planning to travel to a sensitive country for pleasure or for business must contact OCI at least 30 days before departure. A current list of sensitive countries is available online at http://int.lanl.gov/security/isec/fva/countries.shtml. Contact OCI if you have questions or need more details.

Guidance for Personnel Security Requirements

ISD 201-3, *Personnel Security*, establishes implementation requirements supporting the LANL policy established in IMP 201, *Safeguards and Security*.

This ISD contains the following parts that include requirements:

- Security Badges
- Security Clearances
- Human Reliability Program
- Operations Security and Counterintelligence
- Incoming Classified Visits
- Unclassified Foreign Visits and Assignments
- Outgoing Classified Visits
- Security Requirements for Foreign Travel
- FOCI

These requirements apply to all Laboratory workers.

The following offices are the responsible offices (ROs) for this document:

- PS-3
- The OCI Internal Security Team

Note: *To resolve any questions about*

- *security badges, contact the Badge Office, PS-3;*
- *the HRP, incoming security visits, or FOCI, contact PS-3; and*
- *security requirements for foreign travel, contact the OCI.*

Module 4: Cyber Security

Module Overview

Changes in computer technology are coming at an ever-increasing rate. Security guidance is in a never-ending race with the latest and greatest new gadget or software. Cyber security is a challenge for all computer users at the Laboratory.

Cyber security training and awareness is a critical element for the success of the cyber security program at LANL. The goal of the LANL cyber security training program is to educate users about their security responsibilities and about what is necessary to be in compliance with security requirements. For details regarding job-specific cyber training requirements, refer to Cyber Security Education and Awareness No. P220.

In this module, you will review cyber security requirements for all computer users, foreign national computer users, marking and protecting media, wireless technology, and classified computing.

Module Objectives

When you have completed this module, you will be able to identify the cyber security requirements presented in the following sections of this module:

- Cyber Security (computer users)
- Foreign National Computer Users
- Marking and Protecting Media
- Wireless Technology
- Classified Computing
- Guidance for Cyber Security Requirements

Cyber Security

Photo courtesy LANL archives

All Computer Users

Every computer user is a link in the LANL cyber security chain, and all information has value. Always protect information from unauthorized access. The Cyber Security website and your OCSR are valuable resources to refer to when you are working with LANL computers.

To protect yourself and your computer from the majority of threats, observe the following minimum computer protection guidelines:

- Use computer resources for official use only and never for pornography, gambling, music downloading, or other inappropriate activity.
- Ensure that all software is licensed and that you are following all licensing agreements.
- Install virus protection and update it regularly.
- Follow established LANL password guidelines.
- Back up your files regularly.
- Enable password-protected screen savers when you are away from the computer.

Foreign National Computer Users

Foreign nationals must obtain pre-approval for computer access. Written authorization is obtained for the foreign national by his/her LANL host through the online DIVA system. Additionally, the facility hosting the foreign national must document in the DIVA request the degree of risk posed by the foreign national worker. This is achieved by conducting a risk assessment and identifying and fortifying access controls.

Marking and Protecting Media

If you need assistance in marking and protecting media, or getting a system accredited for use, consult your OCSR or the Cyber Security Team.

Email

Use caution when dealing with email. Spam and “phishing” are a growing problem. Spam is unsolicited "junk" email sent to large numbers of people to promote products or services. Phishing is the act of sending an email to a user by falsely claiming to be a legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

Never open email attachments or click on a URL within an email message from an unfamiliar source. Some attachments and URLs are infected with viruses and worms or can otherwise do damage to your computer. When you send email, be sure to personalize it in such a way that the recipient knows that it is a legitimate email.

If you receive anything that is suspicious, report it to your OCSR. Remember that deleting an email message may not delete the attachment. You must find where your email system stores attached files and delete them from there.

Wireless Technology

The use of wireless technology is restricted, as follows:

- IR wireless keyboards are allowed on unclassified computers in nonsecure areas;
- RF keyboards are prohibited;
- wireless mice, IR, and RF are allowed on unclassified computers in both secure and nonsecure areas.

Most computers and computing devices are now shipped with wireless technology. Wireless capabilities must be disabled anywhere on LANL-owned or LANL-leased property unless the usage has been specifically accredited by NNSA for operation. This requirement includes (but is not limited to) Bluetooth and 802.11 protocols. On classified computers, wireless capabilities must be *physically* disabled.

The DOE must pre-approve the use of wireless local area network or wireless computing. Contact Cyber Security for further information.

Cyber security incidents disrupt cyber resources. These incidents include

- physical damage to resources,
- interfering with software or applications,
- introducing malicious code,
- unclassified system contamination, and
- unauthorized access.

All potential cyber security incidents must be reported to your OCSR. Classified information cannot be processed on an unclassified system. If an unclassified system is contaminated by classified information, the system must be unplugged from the network and protected. The potential security incident must be reported immediately to your OCSR, the Cyber Security Team, and the SIT.

Classified Computing

Processing classified information has serious risks. These risks include access by unauthorized users, breaches of security mechanisms such as passwords and firewalls, and disclosure or loss of information. It is your responsibility to protect the classified information you process at all times. Systems must not be used to process classified information until the DOE has accredited the system.

Every classified system must be operated according to its security plan. Significant changes to the system require reaccreditation of the system. If you use classified computers, ensure that you have read and understood the requirements outlined in the system security plan. Access to a classified system depends on your need-to-know and proper clearance level; you must have both before access can be granted.

Lessons Learned

LESSONS LEARNED

Your LANL password, along with your user identification (UID), validates your identity as an authorized computer user on a computer system or network. Your validated identity is then used to control your activities within the system or network, areas that are limited to authorized users or groups of users based on need-to-know.

Jane, an L-cleared employee, was authorized by her group leader to use a Lab computer so she could work from home. Her OCSR created an account on the computer for Jane but failed to check for sensitive information left by the previous owner. After a few weeks, Jane logged in and allowed her children to use the computer for their schoolwork because the family did not own a computer. The children had unauthorized and unsupervised access to the LANL yellow network. Eventually Jane gave her UID and password to the children so they could log in without bothering her. The children used Jane's LANL UID and password at will and routinely downloaded Internet files and used peer-to-peer software.

Classified Computing—continued

Jane knowingly violated DOE and LANL policies by giving her children her LANL UID and password. Doing so put the entire yellow network at risk. Jane's children easily could have downloaded items that could have affected almost every computer system at the Lab. Additionally, a review of the computer's hard drive revealed an unclassified controlled nuclear information (UCNI) file that had been left by its former owner. Jane's children could have had unauthorized access to that file or made it vulnerable to unauthorized access by others.

REMEMBER: Your UID and password are valuable data that protect your computer system and others at the Lab. Do not share them even with close friends and family members.

Be Cyber Safe!

Because computer technology is ever changing, new questions regarding cyber security come up all the time. We must be continually mindful of new threats posed to our cyber resources. Your OCSR and the Cyber Security Team are available to address specific questions. Contact information is available on the Cyber Security website.

Guidance for Cyber Security Requirements

The program description Cyber Security Program No. PD210 institutes the management framework for the LANL Cyber Security Program. The Cyber Security Program implements controls to protect electronic information systems and associated data.

Procedures (P211 through P220) are under development and will address cyber security requirements. P217, Portable Electronic Devices (PEDs), was issued on February 21, 2008. The regulations related to using PEDs across the LANL site are included in this document.

For the latest guidance, refer to the Cyber Security website.

These requirements apply to all Laboratory workers.

Module 5: Classified and Unclassified Controlled Matter Security

Module Overview

How well Laboratory workers handle classified and unclassified controlled matter has an effect on how others perceive our ability to perform the important work we all do for our nation's security interests. Depending on their work assignments, workers with classified and/or unclassified controlled matter may perform accessing, storing, marking, reproducing, receiving and transmitting, and accounting—or combinations of these related functions.

Whatever levels or categories of information you need to access, remember to follow the appropriate procedure, contact your ADC, and never wing it!

Module Objectives

When you have completed this module, you will be able to identify the classified and unclassified controlled matter security requirements presented in the following sections of this module:

- DOE "No Comment" Policy
- Unclassified Controlled Information
- Classified Matter Protection and Control (CMPC)
- Classification
- Classified Removable Electronic Media
- Guidance for Classified and Unclassified Controlled Matter Security Requirements

DOE "No Comment" Policy

Information that is considered classified by the U.S. government may on occasion appear in the public domain, in print, or in broadcast media reports. However, the appearance of such information in open sources does not automatically make it unclassified, and employees must ensure that

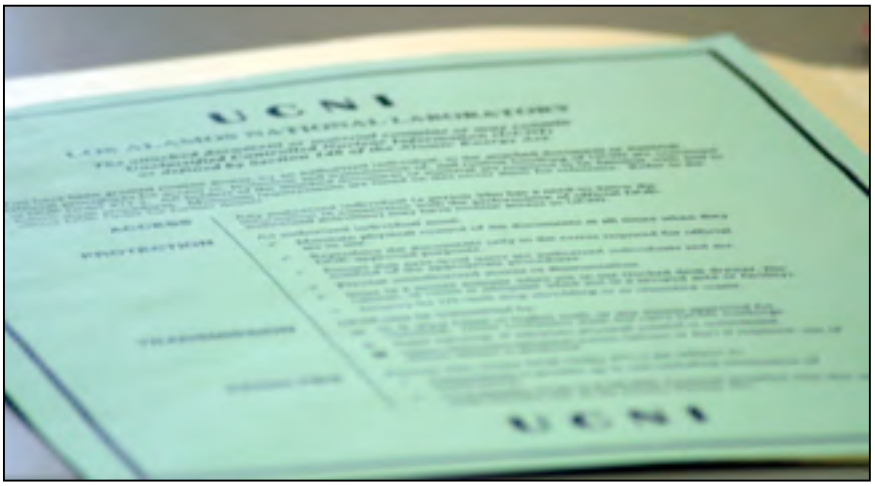
- the information is not used or referred to in an unclassified setting;
- no comment is made in any way regarding the accuracy, classification, or technical merit of such information;
- due care is exercised when discussing such information, even among fellow employees who may not possess the required clearance policy and/or need-to-know; and
- if such information is classified, that fact itself must be protected as classified information.

For example, if a published book contains information classified as Secret Restricted Data, the fact that the book (identified by title and/or author) contains classified information is itself classified as Secret. Therefore, questions raised about open-source information that is considered classified by the U.S. government must be responded to with "no comment."

Photo courtesy LANL archives

Unclassified Controlled Information

Unclassified controlled information (UCI) is unclassified information that may be exempt from public release under the Freedom of Information Act. Although unclassified, the disclosure, loss, misuse, alteration, or destruction of UCI could adversely affect the public welfare, government, or private interests. Thus, UCI requires special protection.



The following designations are two types of UCI that are encountered frequently:

- Unclassified Controlled Nuclear Information (UCNI)
- Official use only (OUO)

UCNI is sensitive government information that is controlled even though it is not classified. A designated UCNI reviewing official makes the determination that a document contains UCNI. A designated UCNI reviewing official is a subset of ADCs (see page 56 for more information on ADCs).

OUO is applied to information that is unclassified yet exempt from release to the public under the Freedom of Information Act. In general, this information consists of sensitive administrative, proprietary, or personal information that warrants protection from unauthorized disclosure.

Unclassified Controlled Information—continued

Controlling Access

You do not have to hold a clearance to view UCNI or OUO but you must have a need-to-know. Need-to-know is based on the determination by an authorized holder of the information that the intended recipient needs the information to carry out his or her official duties.

Marking

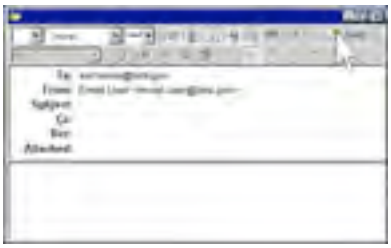
LANL Procedure No. P204-1 states the requirements and procedures for identifying, marking, handling, and protecting UCI. Matter containing OUO must be marked on the front page of the document and on the bottom of subsequent pages containing OUO information. Matter containing UCNI must be marked on the front page of the document and on the top and bottom of subsequent pages containing UCNI information. The front page of a document containing both UCNI and OUO information must be marked with both OUO and UCNI markings. A stamp containing information regarding who reviewed the information and why it is considered UCNI or OUO must also be on the first page.

Protecting

UCNI and OUO must be protected by a means that will prevent unauthorized disclosure. Store UCNI and OUO in a locked receptacle. Reproduce UCNI and OUO only to the minimum extent necessary to carry out official activities.

Unclassified Controlled Information—continued

Protecting UCNI



When mailing UCNI within LANL, use an interoffice envelope. When mailing outside LANL, use an opaque envelope. In both cases, do not indicate that the contents within the envelope is UCNI.

Encryption **must** be used when sending UCNI via fax or email.

When transmitting UCNI within the LANL yellow network, no encryption is required but it is suggested.

Protecting OUO

When mailing OUO within LANL or outside LANL, use a sealed, opaque envelope with the recipient's address and the words

TO BE OPENED BY ADDRESSEE ONLY

on the front of the envelope.

When OUO information is sent over networks, including email, it should be encrypted with encryption software that is validated by the National Institute of Standards and Technology (NIST).

If encryption capabilities are not available and transmission by mail is not a feasible alternative when transmitting OUO, then regular email or facsimile machines may be used to transmit the document.

All nonelectronic UCNI or OUO documents must be destroyed by any means that prevents the retrieval or export of the information. Shredding or destruction by means of a sensitive burn box is required.

Unclassified Controlled Information—continued

Personally Identifiable Information (PII)

Carefully consider the types of data that you process on your computer and ensure that security is in place for protecting that data. The rules for processing unclassified controlled information have already been discussed in this document.

A new category of information has been introduced: personally identifiable information (PII). PII refers to information that could be used to compromise an individual's identity. PII includes social security numbers, place and date of birth, mother's maiden name, biometric records, etc.

If you process PII, you must understand and fulfill all requirements for managing the data securely:

- PII data on all laptops must be **encrypted**.
- All desktop and laptop computers used or transported off-site must be assessed for PII. All PII on such machines must be **encrypted**. The SRLM must approve the processing of PII off-site.
- Any PII data contained in email sent outside LANL networks must be **encrypted**.
- ***Immediately* report any potential loss of PII to the Office of the Security Inquiry Team (665-3505).**

Additional information is online:

http://int.lanl.gov/security/cyber/access/pii.shtml

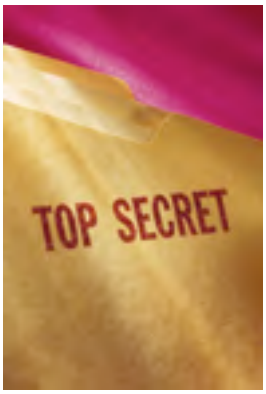
Classification

Classified information is information that is classified as Restricted Data or Formerly Restricted Data under the Atomic Energy Act of 1954, or information that is identified as National Security Information under the Presidential Executive Order.

Classification—continued

Classified information is designated by a classification level and category. The classification level is based on how much our national security could be damaged if the information were to be released to unauthorized person(s). There are three levels:

- Top Secret information can be expected to cause **exceptionally grave damage** to national security,
- Secret can be expected to cause **serious damage** to national security, and
- Confidential can be expected to cause **damage** to national security.



The classification category describes the type of information contained in the material. There are three categories:

- Restricted Data is information that is related to the design, manufacturing, and utilization of atomic weapons; production of special nuclear material; or use of special nuclear material in the production of energy.
- Formerly Restricted Data is information that pertains to the military utilization of atomic weapons and has been removed by the DOE from the Restricted Data category.
- National Security Information is information that requires protection in the interest of national defense or foreign relations of the U.S. that is not related to nuclear weapon design, manufacturing, testing, or utilization.

Classified Matter Protection and Control (CMPC)

Classified information requires protection against unauthorized disclosure to avoid damage to national security. The term *classified matter* is commonly used as an all-encompassing term that includes documents, parts, and/or media that may contain classified information.

If you will be working with classified matter, you are required to take the *Classified Matter Protection & Control Overview* training (#16028). After this initial training, classified matter users must take the online course #35043 every two years.

Classified matter custodians (CMCs) are required to take CMPC for Custodians (#40143). After the initial training, CMCs must take the online course #35044 every two years.

Controlling Access

The following table indicates the clearance level required for each category and level of classified matter. Access to classified matter must be limited to persons who possess appropriate access authorization and any formal access approvals, and who have a need-to-know for the performance of official duties (access is not obtained by position only). In addition, an individual must view Sigma information only if he or she has the authority to do so. Check the signature authority system for Sigma authorization. (For information on Sigma categories, go to http://int.lanl.gov/security/isec/fva/guidelines/sigmas.shtml)

	Restricted Data	Formerly Restricted Data	National Security Information
Top Secret	**Q**	**Q**	**Q**
Secret	**Q**	**Q/L**	**Q/L**
Confidential	**Q/L**	**Q/L**	**Q/L**

Classified Matter Protection and Control (CMPC)—continued

Marking

Classified matter must be marked with

- classification level;
- category; and
- any other information that is applicable (e.g., caveats, unique identifier number, etc.).

Markings must be clearly distinguishable from the text of information in the document. Markings may be of a larger font size, different color, or both to distinguish between information and text.

Keep in mind that required markings are different for each type of classified matter; consult your CMC or refer to the Protecting Information website for further instructions on marking classified matter.

Protecting

The following requirements apply to protecting classified matter:

- Classified matter must be protected from unauthorized disclosure.
- All work involving classified information must be performed in approved Security Areas.
- Conduct classified discussions in approved areas, and ensure that those without a need-to-know do not overhear the conversation.
- Do not leave classified matter unattended at any time. When not in your physical control, classified matter must be stored in an approved General Services Administration safe, certified vault, or certified vault-type room.

- Classified processing must be done on approved classified computers.
- Telephone conversations involving classified information must be conducted over approved telecommunications (such as a secure telephone unit [STU] or secure terminal equipment [STE]).
- The removal of classified matter from approved facilities to private residences or other unapproved places (e.g., hotel or motel rooms) is prohibited.

Classified Matter Protection and Control (CMPC)—continued

To prevent unauthorized disclosure, classified matter has specific requirements for

- generation,
- marking,
- physical protection,
- storage,
- reproduction,
- accountability,
- transmission (including hand-carrying),
- destruction,
- incident reporting, and
- emergency procedures.

Refer to the Protecting Information website or the CMPC Handbook, P204-2, for more details on these topics.

Vault and Vault-Type Rooms

Controlled/prohibited article restrictions apply to V/VTRs. See the section on *Controlled and Prohibited Articles* (pp. 17–20).

Authorized Derivative Classifiers

At LANL, the responsibility for identifying classified information rests with the Classification Group (SAFE-1). Employees throughout LANL are trained as ADCs and have the authority to classify documents and other material according to approved classification guidance. The SAFE-1 classification staff also serves as ADDs.

The originator of any form of information (including email) must obtain an ADC or SAFE-1 classification review for any information prepared in a subject area that is or may be classified. If you are even slightly unsure of the classification level, consult an ADC. Pending a classification review, the information must be protected at the highest potential classified level and category. A list of ADCs by organization is available on the SAFE-1 website.

Classified Matter Protection and Control (CMPC)—continued

SAFE-1 review is also required for any material intended for public release, such as professional journal articles, conference proceedings or posters, open web postings, and formal or informal reports. For more information, visit the SAFE-1 website or contact the SAFE-1 Publications Office.

Any employee may challenge a classification determination made by an ADC or by SAFE-1. SAFE-1 will coordinate such a challenge and assist the employee in obtaining a resolution to the challenge from the appropriate authority at LANL or at DOE/NNSA.

If any employee believes that a classified document no longer contains classified information and should therefore be declassified, the employee must submit the document to SAFE-1 for declassification review.

Any questions about classification and declassification should be directed to SAFE-1.

Classified Removable Electronic Media

Classified removable electronic media (CREM) is used to store classified information. Classified electronic media are those materials and components manufactured to provide nonvolatile storage of classified digital data that can be read by an automated information system.

"Removable" refers to media that are

- designed to be introduced to and removed from an automated information system without adverse impact on system functions,
- separated from the system for any reason, OR
- personal electronic devices.

The following items are examples of removable electronic media:

- Removable hard drives
- Laptops with nonremovable hard drives
- Floppy diskettes (8", 5 ¼", 3 ½", magnetic and optical)
- Compact discs (CDs), all types
- Digital video discs (DVDs), all types
- Zip disks, all types

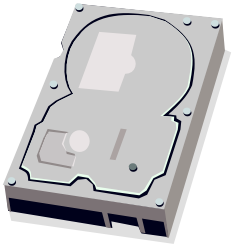
Classified Removable Electronic Media—continued

- Jaz disks, all types
- Bernoulli cartridges, all types
- USB flash drives (solid state memory)
- Magnetic tapes used to store digital data
- Optical and floptical disks
- PDAs or PEDs that are accredited for classified processing
- Compact flash cards such as those used in digital cameras (solid state memory)
- Digital cameras with any nonremovable memory

Not Classified Removable Electronic Media (CREM)

The following media containing classified data are NOT considered CREM:

- Videotapes
- Audiotapes
- Viewgraphs
- Motion picture films
- Hard drives in classified photocopiers if the photocopier is not connected to a network ***and*** the hard drive does not retain image data
- Printer cartridges
- COMSEC/CRYPTO keying material
- Scanners with volatile memory



Accountable and Nonaccountable CREM

LANL categorizes CREM into two groups: accountable CREM (ACREM) and nonaccountable CREM.

Classified Removable Electronic Media—continued

CREM is considered to be accountable if it contains the following information:

- Top Secret (TS)
- Secret Restricted Data (SRD)
- Sigma 14, 15, or 20
- Deployable Nuclear Emergency Search Team (NEST) and Accident Response Group (ARG) operations
- Secret Foreign Government Information (FGI), including
  - — Secret and Confidential United Kingdom (UK) “Atomic”
  - — Secret and Confidential North Atlantic Treaty Organization (NATO) “Atomal”

Note: *Nonaccountable CREM does not contain information that falls within any of the categories above.*

All workers must complete training plan #6943, (Course #36175 *ACREM Borrower/SRLM*) before they are authorized to borrow ACREM items. Line managers responsible for borrowers must also complete training plan #6943.

To ensure that work involving ACREM is conducted in a secure manner, LANL has established

- classified media libraries (CMLs) and
- classified library custodians (CLCs).

Classified Media Library (CML)

A CML is similar to a traditional library. All ACREM is stored in a CML, and a borrower must “check out” the ACREM from a CLC. The borrower’s name must be on the borrower list, which is provided to the CLC by the borrower’s RLM, before he or she can check out a piece of ACREM. The borrower is solely responsible for the ACREM during the time that it is checked out of that library.

Classified Removable Electronic Media—continued

ACREM must be protected, stored, and handled in accordance with CMPC requirements. Refer to the Protecting Information website for more information.

Creating CREM and ACREM

CREM is created when a piece of media is inserted into a classified computer. The media become ACREM

- if the media are placed in the read/write drive of a classified computer system that is accredited for SRD, or
- if the information put on the media falls under one of the accountable CREM categories.

For more information, refer to *Classified Matter Protection and Control Handbook,* P204-2, Section 3.7.6 Accountable Classified Removable Electronic Media (ACREM).

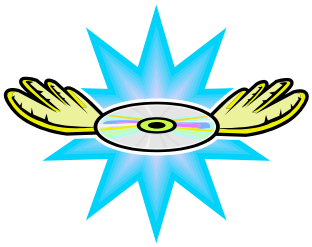
Note: *CREM must be marked at the highest level and category that the system is approved to process as stated in the CMPC Handbook, P204-2,*

If a person creates ACREM, he or she is responsible for taking the ACREM to his or her CLC for entry into the accountability system. A newly created piece of ACREM must be entered by close of business the day it was created. If it was created after hours, it must be done by close of business the following day. Refer to *Classified Media Library Procedure*, Version 6.0, located on the ACREM homepage.

Lessons Learned

Bert retrieved an externally generated S/NSI compact disc (a nonaccountable CREM) from Colin, the CLC at a CML. Bert then took the CD to his colleague Al, who needed it for his work. The CD was properly marked but packaged in a nonstandard way inside an unmarked brown envelope. Later, Al returned it in its original package to Colin.

Classified Removable Electronic Media—continued



Colin removed the CD from the nonstandard packaging, placed the CD in a properly marked package, and returned it to Bert who needed it for further work. As part of his standard practice, Bert stored the CD in a locked cabinet in an adjacent VTR before leaving for the day. The following week, Bert tried to locate the CD and recruited Colin and Al to help. Neither Colin nor Bert remembered repackaging and relocating the CD so all three were looking for the nonstandard envelope. All three failed to locate the CD. After four days, they reported the suspected loss to their managers and the SIT.

During the inquiry another CLC mentioned to the SIT that CLCs at his CML routinely repackage items correctly. Derek's statement prompted Al and Bert to look for the new packaging. They located the repackaged CD and verified that it had been properly protected at all times.

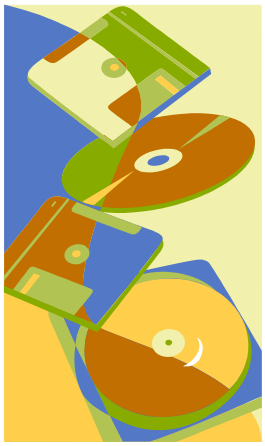
There are some ways that can prevent this type of mix-up:

- Workers must pay attention to their work, especially when in stressful or unfamiliar situations.
- Remember to apply the five-step process of ISSM when working on tasks with high security risks.
- Workers and managers must continuously look for ways to ensure the security of their workplace.
- Workers must *immediately* report potential security incidents to the SIT and RLMs.
- Managers must create an environment that encourages self-reporting and emphasizes timeliness.

Guidance for Classified and Unclassified Controlled Matter Security

ISD 201-4, *Classified and Unclassified Controlled Matter Security*, establishes implementation requirements supporting the LANL policy established in IMP 201, *Safeguards and Security*. This ISD contains requirements that apply to all Laboratory workers.

Guidance for Classified and Unclassified Controlled Matter Security—continued



The RO for *Unclassified Controlled Information Handbook* is SAFE-1, while the *Classified Matter Protection and Control Handbook* is a product of the PS-1, the Classified Matter Protection Group. Any questions should be directed to the following resources:

- SAFE-1 at 667-5011
- PS-1 at 665-1802
- cmpc@lanl.gov
- Security Help Desk 665-2002
- security@lanl.gov

ACREM items are subject to additional rules, procedures, and restrictions. The procedures and requirements in the *Classified Matter Protection and Control Handbook* are augmented by policy and procedures for ACREM in LANL Notice 155, *Accountable Classified Removable Electronic Media Policy*.

The RO for the *Classification of Matter* manual is SAFE-1. The requirements contained in this attachment apply to Laboratory workers, ADCs, ADDs, SAFE-1, and RLMs.

Resources

The Annual Security Refresher covers a wide range of security topics. If you have further questions about security requirements and how to meet them, you can consult some of the resources described in the following sections. You will find a list of phone numbers followed by a list of acronyms at the end of the Resources Module.

The Security Help Desk

The Security Help Desk provides answers or assists in obtaining answers for security-related questions. Contact the Security Help Desk at (505) 665-2002 or security@lanl.gov.

Security Program Leads

SPLs, formerly senior security advisors, provide security expertise and provide a single point of contact on security matters for directorate personnel. A listing of SPLs can be found online at

http://int.lanl.gov/security/integrating/deployed.shtml .

Deployed Security Officers

DSOs coordinate and oversee all division security activities. DSOs are available to answer any security-related questions. A listing of DSOs can be found online at

http://int.lanl.gov/security/integrating/deployed.shtml .

Organizational Computer Security Representatives

OCSRs are the main point of contact for all cyber security activities for unclassified and classified systems. A listing of OCSRs can be found online at

http://int.lanl.gov/security/cyber/ .

Cyber Systems Security Officers (formerly ISSOs)

Cyber systems security officers (CSSOs) are responsible for ensuring that protective measures are installed and operational security is maintained for one or more specific classified information systems and/or networks. A listing of CSSOs can be found online at

http://int.lanl.gov/security/cyber/ .

Implementation Support Documents

ISDs are policy documents written specifically for LANL. These documents ensure compliance with DOE directives. Safeguards and Security ISDs (at http://int.lanl.gov/security/documents/#ISDs) include the following documents:

- ISD 201-1, General Security
- ISD 201-2, Physical Security
- ISD 201-3, Personnel Security
- ISD 201-4, Classified and Unclassified Controlled Matter Security
- ISD 201-5, Nuclear Safeguards

Security Website

The Security website (http://int.lanl.gov/security) provides information on all security-related topics, including the following topics:

- Protecting information
- Personnel
- Cyber security
- Nuclear materials
- Facility security
- Integrated security

Phone Numbers

Badge Office	667-6901
Chief Security Officer-Cyber Security (CSO-CYSEC)	665-1795
Classification Group (SAFE-1)	667-5011
Classified Matter Protection (PS-1)	665-1802
Classified Visits	667-5587
Clearance Processing	667-7253
CT-ITS Registrar	667-0059
Cyber Security	665-1795
Foreign Visits & Assignments (FV&A)	665-1572
Immigration Services (ISO)	667-8650
Internal Inquiries (SAFE-2)	665-6159
Internal Security (ISEC)	665-6090
Los Alamos Police Department	662-8222
Office of Counterintelligence (OCI)	665-6090
Personnel Security (PS-3)	665-6565

Phone Numbers—continued

Physical Security (PS) Division	667-2510
SAFE-! Publications Office	667-5013
SOC Los Alamos (after-hours incident reporting)	667-4437
SOC Los Alamos Shift Commander	665-1279
Security Awareness Program Office	667-5984
Security Help Desk	665-2002
Security Inquiry Team (SIT)	665-3505
Security Integration (PS-2)	665-7565
Technical Surveillance Countermeasures (TSCM) Team	665-3409
Violence in the Workplace	667-8730

All Laboratory workers must take responsibility for security, involving themselves while relying on management support. Do NOT improvise when it comes to security. For security help or for questions about the content of this course, contact your deployed security personnel or the Security Help Desk at 5-2002 or security@lanl.gov. For administrative help with this course (such as to obtain credit), contact the CT-ITS registrar at 667-0059 or the Security Awareness Program office at 667-5984.

Acronyms

ACREM	accountable classified removable electronic media
ADC	authorized derivative classifier
ADD	authorized derivative declassifier
ARG	Accident Response Group
ASR	Annual Security Refresher

Acronyms—continued

ATOMAL	A North Atlantic Treaty Organization marking applied to (1) Restricted Data or Formerly Restricted Data provided by the United States to the North Atlantic Treaty Organization or (2) "U.K. Atomic Information" provided by the United Kingdom.
CD	compact disc
CFR	Code of Federal Regulations
CI	Counterintelligence
CLC	classified library custodian
CMC	classified matter custodian
CML	Classified Media Library
CMPC	Classified Matter Protection and Control
COMSEC	Communications Security
CREM	classified removable electronic media
CSO-CYSEC	Chief Security Officer-Cyber Security
CSSO	Cyber Systems Security Officer (formerly ISSO)
CT-ITS	Central Training Division-Institutional Training Services
DOE	Department of Energy
DSO	deployed security officer
DVD	digital video disc
FOCI	foreign ownership, control, or interest
FV&A	foreign visits and assignments
HRP	Human Reliability Program
IMI	impact measurement index

Acronyms—continued

IMP	implementation plan
IOSC	incidents of security concern
IPP	Institutional Policy and Implementation Procedure
IR	infrared
ISD	implementation support document
ISEC	Internal Security
ISM	Integrated Safety Management
ISO	Immigration Services Office
ISSM	Integrated Safeguards and Security Management
IWM	Integrated Work Management
LANL	Los Alamos National Laboratory
LANS	Los Alamos National Security
NEST	nuclear emergency search team
NIST	National Institute of Standards and Technology
NNSA	National Nuclear Security Administration
NSSB	National Security Science Building
OCI	Office of Counterintelligence
OCSR	organizational computer security representative
OPSEC	Operations Security
OUO	official use only
PDA	personal digital assistant
PED	portable electronic device

Acronyms—continued

PII	personally identifiable information
PPA	Property Protection Area
PS-1	Classified Matter Protection Group in Physical Security Division
PS-2	Security Integration Group in Physical Security Division
PS-3	Personnel Security Group in Physical Security Division
RD	restricted data
RF	radio frequency
SAFE-1	Classification Group in Safeguards Division
SAFE-2	Internal Inquiries Group in Safeguards Division
SIT	Security Inquiry Team
S/NSI	Secret/National Security Information
SSSP	Site Safeguards and Security Plan
RLM	responsible line manager
SD	system description
SNM	special nuclear material
SPL	security program lead
SOC Los Alamos	SOC Los Alamos (SOC is the name, not an acronym), formerly Protection Technology Los Alamos (PTLA), is the company that provides the protective force for LANL
SRD	secret restricted data
STE	secure terminal equipment
STU	secure telephone unit
TC	training coordinator

Acronyms—continued

TS	top secret
TSCM	technical surveillance countermeasures
UCI	unclassified controlled information
UCNI	Unclassified Controlled Nuclear Information
UID	user identification
V/VTR	vault/vault-type room

Credit for Reading This Document

To receive credit for reading this document, go to the following URL:

http://www.hr.lanl.gov/scourses/all/1425/credit-page.html