

ROS AGREEMENT INDIVIDUAL SECURITY PLAN

ROS Agreement No.: _____

Individual's Name: _____

Type of Clearance Required: Q L No Clearance

Type of Badge Received: No Badge Required
 LANL Generic Uncleared US Visitor
 LANL Generic Uncleared US Visitor Escort Required
 LANL Uncleared Site-specific
 LANL Uncleared / Cleared Foreign National
 Uncleared DOE
 DOE L
 DOE Q

SECTION I

In the performance of the above referenced ROS Agreement and in order to comply with security requirements for on-site workers outlined in DOE O 470.4B, *Safeguards and Security Program*, LANS, LLC and the ROS worker agree to the following Individual Security Plan:

1. ROS worker shall comply with all security requirements outlined in this Individual Security Plan in addition to any other security requirements briefed by their LANL host.
2. All non-U.S. citizen foreign national ROS workers are required to have approval to work on-site from the LANL Foreign Visits and Assignments office PRIOR to their arrival at the Laboratory. They are required to present a valid passport and visa documentation before a badge will be fabricated and issued.
3. All non-U.S citizen foreign national ROS workers are required to have approval to work off-site with LANL information or data from the LANL Foreign Visits and Assignments office PRIOR to beginning work; unless all LANL information or data required to perform the work activity is non-sensitive and will be published in open literature intended for public release.
4. All required training shall be completed and documented prior to any work beginning. Either a record of all completed equivalent training shall be attached to this ISP; or the required and completed training shall be documented below.

Required Course	Course Title	Frequency
General Security		
	General Employee Training (GET) - On site 10 or more days	Once
	LANL Emergency Procedures and Protective Actions - All	12 months
	Annual Security Refresher (ASR) - L & Q-cleared Workers	12 months
	Comprehensive Security Briefing - L & Q-cleared Workers	Once
	Export Control Fundamentals – Based on SOW	12 months
	Substance Abuse Awareness - All	Once
	Last Angry Words (Workplace Violence) - All	Once
Classified Matter Protection And Control		
	Classified Matter Protection - Classified Matter Users	Once
	CMPC User Refresher - Classified Matter Users	24 months
Cyber Information Security		
	Initial Information Security Briefing - All Computer Users	Once
	Annual Information Security Refresher – All Computer users	12 months
	Classified Computer Security - Classified Computer Users	Once
Human Reliability Program		
	HRP Training for HRP Workers	12 months
Protecting Classified & Sensitive Information		
	Protecting UCNI - Users of Unclassified Controlled Nuclear Information (UCNI)	Once
Physical Security		
	Escort Responsibilities - Escorts & Vault or Vault Type Room Users, Custodians	12 months
	The Outsider - For Vault or Vault Type Room Users (AIS Escorts)	Once
	Vault or Vault Type Room User - Vault or Closed Area Users	12 months
Site-Specific Training		

5. Any ROS worker who will obtain a standard badge (non-Visitor or non-Generic) such as a DOE Q, DOE L, DOE Uncleared, Uncleared Site-specific LANL, or Cleared/Uncleared Foreign National badge from the LANL Badge Office shall successfully pass a drug test no more than 60 days before requesting and obtaining a standard badge; or provide documentation of active participation in a DOE-approved drug program.
6. Any badge provided by the LANL Badge Office under the above Agreement is strictly for use in the performance of the work outlined in this subcontract and the badge shall not be utilized for any other work or activities.

7. When the ROS Agreement is terminated, any associated security clearance obtained through LANL will also be terminated.

By signature below, the responsible LANL line manager (RLM) and the ROS worker acknowledge that all the security requirements contained herein have been briefed, read and agreed upon. A copy of this ISP shall be provided to the ROS worker.

Approved by LANL Manager (RLM)

Printed Name *Signature* *Date*

Accepted by ROS Worker

Printed Name *Signature* *Date*

SECTION II

In the following pages, additional security requirements that shall be complied with while working for Los Alamos National Laboratory are outlined.

ROS worker's signature on this Individual Security Plan acknowledges consent to comply with these requirements, in addition to any facility-specific security requirements the LANL host may present.

SecuritySmart

Prohibited Articles

Certain articles are prohibited from Laboratory property, including:

- personally owned firearms;
- dangerous weapons; explosives; and pocket, hunting, or other sharp knives with blades longer than 2.5 inches (Note: knives for official Laboratory work or knives used in the preparation of food are not prohibited);
- alcoholic beverages (opened or unopened), including items such as kegs;
- controlled substances (such as illegal drugs and drug paraphernalia, but not prescription medication); and
- items prohibited by local, state or federal laws.

Open vs. Controlled Access Areas

- East Jemez Road (Truck Route) is an open access area during normal security conditions. There are no restrictions on prohibited articles (unless they are illegal under local, state, or federal law) in private vehicles as long as drivers do not drive into Laboratory property.
- Portions of West Jemez Road, Diamond Drive, and Pajarito Road are protected by Vehicle Access Portals (VAPs) but accessible to the public. Workers are allowed to transport prohibited articles (unless they are illegal under local, state, or federal law) on these open roadways. Workers are not allowed to leave these roadways and access Laboratory property while transporting prohibited articles.
- Roads (including the Pajarito Corridor), parking lots, and open space within VAPs that are physically accessible to the public, but posted with "no trespassing" signs, are controlled access areas. Workers are not allowed to introduce prohibited articles in these areas, and vehicles are subject to random inspections by the Protective Force.

Confiscation

Workers found with prohibited articles in their vehicles in controlled access areas (not open access areas) during Protective Force inspections will be immediately escorted off Laboratory property. Prohibited articles may also be confiscated by the Protective Force or Los Alamos Police Department.



Resources

- SAFE-2 Special Projects Team, 665-7467
- Security Help Desk, 665-2002, security@lanl.gov

Reference

Prohibited and Controlled Articles Procedure, P202-5, <https://policy.lanl.gov/pods/policies.nsf/MainFrameset?ReadForm&DocNum=P202-5&FileName=P202-5.pdf>

View and download all Security Smarts for your safety and security meetings
<http://int.lanl.gov/security/documents/index.shtml#security-smarts>

SecuritySmart

Portable Electronic Devices

Portable Electronic Devices (PEDs) can potentially transmit or transport sensitive unclassified and classified information. The Department of Energy identifies two types of PEDs: Portable Electronic Storage Devices (PESDs) and Controlled Articles.

Portable Electronic Storage Devices (PESDs) can store, read, or write nonvolatile information and be plugged into a computer. PESDs, unlike Controlled Articles, are not "stand-alone" devices. PESDs include:

- CD/DVD write drives;
- external hard drives;
- flash memory (i.e., PC cards, SD memory cards); and
- USB memory devices (thumb drives, memory sticks, jump drives).

Controlled Articles are "stand-alone" devices that can record and/or transmit data. Some examples of Controlled Articles are:

- court-ordered devices (e.g., ankle-monitoring device);
- cameras (e.g., cell phones or other multifunction devices, such as a Blackberry, with photographic capability);
- cell phones and personal digital assistants;
- copiers or scanners with hard drives;
- digital audio players (e.g., iPod);
- laptop or palm-top computers;
- some medical devices (e.g., heart monitor); and
- two-way pagers and radios.



IMPORTANT

Approval to use PEDs on Laboratory property depends on their ownership (personal vs. government-owned), the security requirements of an area, and the risks associated with them. Workers should refer to the Portable Electronic Devices Procedure for details.

Resources

Information (Cyber) Security Help Desk, 665-1795, cybersecurity@lanl.gov
Security Help Desk, 665-2002, security@lanl.gov

References

1. Portable Electronic Devices Procedure, P217, <https://policy.lanl.gov/pods/policies.nsf/MainFrameset?ReadForm&DocNum=P217&FileName=P217.pdf>
2. Marking Information Systems and Media Procedure, P212, <https://policy.lanl.gov/pods/policies.nsf/MainFrameset?ReadForm&DocNum=P212&FileName=P212.pdf>
3. Prohibited and Controlled Articles Procedure, P202-5, <https://policy.lanl.gov/pods/policies.nsf/MainFrameset?ReadForm&DocNum=P202-5&FileName=P202-5.pdf>
4. Security Smart on Photographic Equipment and Activities, July 2009, <http://int.lanl.gov/security/documents/security-smart/2009/photo709.pdf>

View and download all Security Smarts for your safety and security meetings
<http://int.lanl.gov/security/documents/index.shtml#security-smarts>

SecuritySmart

E-books and Other Portable Electronic Devices

As portable electronic devices (PEDs) – including e-books such as the Kindle or tablet computers such as iPads – become more integrated into our daily lives, workers should be mindful of what they can and cannot take to various areas of the Laboratory.

A worker was recently discovered with a Kindle e-book in a Limited Area. Although the worker did not use the e-book while inside a Limited Area, security officials deemed its presence in the worker's office an incident.

Many PEDs such as e-books have broadband connectivity (the same wireless used by cell phones) and need to be considered and handled the same as a cell phone. They may also have other wireless capabilities that are restricted at LANL.

The restrictions on the use of a PED on Laboratory property differ depending on whether it is government- or personally owned, the security requirements of the area, and the potential risk associated with the PED.

Portable Electronic Storage Devices (PESDs) and Controlled Articles

There are two kinds of PEDs: portable electronic storage devices (PESDs) and controlled articles.

PESDs	Controlled Articles
CD/DVD write drives	Cell phones
External hard drives	Copiers or scanners with hard drives
Flash memory (e.g., SD memory cards)	Recording equipment (e.g., audio, video, optical, data)
USB memory devices (e.g., thumb drives)	Medical devices that collect and transmit data

Workers should contact their OCSRs or the Chief Information Officer (CIO) Help Desk if they are unsure about whether a PED is allowed in an area. Workers who find an unauthorized PED in a Limited Area should immediately report it to the Security Inquiry Team.

Resources

- CIO Help Desk, cybersecurity@lanl.gov
- Organizational Computer Security Representatives (OCSRs), http://int.lanl.gov/security/cyber/docs/ocsr_issu_list.xls
- Security Inquiry Team, 665-3505

Reference

1. Cyber Security Wireless Computing Devices Procedure, P213, [https://policy.lanl.gov/pods/policies.nsf/LookupDocNum/P213/\\$file/P213.pdf](https://policy.lanl.gov/pods/policies.nsf/LookupDocNum/P213/$file/P213.pdf)
2. Portable Electronic Devices Procedure, P217, [https://policy.lanl.gov/pods/policies.nsf/LookupDocNum/P217/\\$file/P217.pdf](https://policy.lanl.gov/pods/policies.nsf/LookupDocNum/P217/$file/P217.pdf)
3. Prohibited and Controlled Articles Procedure, P202-5, [https://policy.lanl.gov/pods/policies.nsf/LookupDocNum/P202-5/\\$file/P202-5.pdf](https://policy.lanl.gov/pods/policies.nsf/LookupDocNum/P202-5/$file/P202-5.pdf)



View and download all Security Smarts for your safety and security meetings
<http://int.lanl.gov/security/documents/index.shtml#security-smarts>
 Note: Security Smarts are current as of the date of publication.

SecuritySmart

Workplace Violence

Workplace violence consists of hostile or aggressive physical contact with another person, a statement or body gesture that threatens harm to another person, or conduct that would cause a reasonable person to believe that he or she may be harmed.

Preventing Workplace Violence

Know the people with whom you work and notice when their behavior seems out of place or out of character. The following behaviors can be warning signs of potential workplace violence:

- sudden changes in behavior or work pattern such as unwillingness to follow directions;
- yelling, slamming or throwing objects, verbally challenging or intimidating behavior;
- lying or participation in compulsive behaviors like gambling or addictive behaviors involving alcohol or other drugs;
- blaming others and refusing to take personal responsibility for concerning behaviors; and/or
- significant changes in social interactions (i.e., sudden withdrawal or seeming preoccupation with a specific individual or groups).

Reporting Concerning Behavior

Workers should always be alert for worrisome behavior by another employee or others near the workplace. Those with concern should notify the group or higher-level manager about the behavior, particularly if there is a threat of workplace violence.

A supervisor must act when a worker threatens or demonstrates violent behavior by having the worker removed from the workplace and notifying security. The supervisor must also report the incident to Human Resources-Employee Relations.

How to Handle a Violent Situation

If you believe the situation is life threatening or could result in bodily harm, call 911 immediately.

Resources

- Human Resources - Employee Relations, 667-8730
- Security Help Desk, security@lanl.gov, 665-2002

Reference

1. Workplace Violence Procedure, P724, <https://policy.lanl.gov/pods/policies.nsf/MainFrameSet?ReadForm&DocNum=P724&FileName=P724.pdf>
2. USDA Handbook on Workplace Violence Prevention and Response, <http://www.usda.gov/news/pubs/violence/wpv.htm>
3. Security Smart on Responding to an Active Shooting, <http://int.lanl.gov/security/documents/security-smart/2010/shooting1110.pdf>



View and download all Security Smarts for your safety and security meetings
<http://int.lanl.gov/security/documents/index.shtml#security-smarts>
 Note: Security Smarts are current as of the date of publication.

SecuritySmart

Responding to an Active Shooting

The workplace should never be a dangerous place. Unfortunately, shooting incidents have occurred across the country. In spite of the intense media coverage, such workplace assaults are very rare. Should such an incident occur at the Laboratory, however, employees should know how to respond to protect themselves and their coworkers.

In Case of a Shooting

When you become aware of a workplace shooting occurring or is about to occur:

- Try to stay focused so you can think more clearly and respond more effectively.
- Stay where you are and lock down if possible. Close and lock office doors and hide in your office, perhaps under a desk, to best protect yourself.
- Call 911 if it is safe to reach a phone. Quietly provide any pertinent details that might help responders (such as number of gunmen and number of building occupants). **Do not leave a safe location to look for a phone.**
- **Do not activate fire alarms.** Doing so might create panic and place people in greater danger.
- Emergency situations are unpredictable. There may not be a specific procedure to rely on for guidance. **Use common sense and focus on your safety and the safety of those around you.**

Remember, in the event of an active or imminent shooting, **protect yourself and call 911 if you can safely do so.** The Laboratory's Protective force, management, and all other Laboratory resources (the Security Inquiry Team, Internal Inquiries Group, Human Resources-Employee Relations) should be notified only if there is no immediate threat to health and safety.

After a Shooting

Do not leave your office or shelter, even if the shooting seems to have stopped. Staying in place will help law enforcement personnel, emergency responders, or hostage negotiators accurately assess the situation and collect evidence more effectively.

Practice Response Drills

Just as it is important to know emergency exits and muster areas in case of a fire or other building emergency, workers should know how to respond to an active shooting in the workplace. It may be useful to practice and role-play situations. Know your coworkers so you can assist each other in case of a violent episode. Develop signals if possible and learn to alert others of suspicious or unusual activities in the workplace.

Dealing with the Aftermath

The Laboratory will provide grief counselors and other assistance to help survivors should a shooting ever occur on Laboratory property. Workers who experience workplace violence are encouraged to seek help.

Reference

Department of Homeland Security's Active Shooter Booklet, http://www.dps.mo.gov/homelandsecurity/documents/Active%20Shooter/DHS%20ActiveShooter_Response%20Booklet.pdf



View and download all Security Smarts for your safety and security meetings
<http://int.lanl.gov/security/documents/index.shtml#security-smarts>
 Note: Security Smarts are current as of the date of publication.

SecuritySmart

Pause or Stop Work

Just as workers at the Laboratory have the authority and responsibility to pause or stop work if they discover that others are exposed to conditions of imminent danger or other safety hazards, workers must also pause or stop work if they discover a security risk.

Pause or Stop Your Own Work

If you identify a security risk in your own work, pause or stop work and take action. You may correct the problem without first notifying your supervisor if:

- the problem does not pose an immediate security risk;
- you can correct the problem immediately; and
- you have the ability and tools to correct the problem.

In all other cases, notify your supervisor before restarting work.

Pause or Stop the Work of Others

If you observe a security concern in someone else's work:

- inform that worker immediately and request an immediate pause or stop work; and
- if there is no imminent security risk, ask the worker to explain what he or she is doing.

If the worker does not offer an acceptable explanation, notify the worker's supervisor.

For subcontractor work, notify the worker's sponsoring organization or contract administrator.

If another worker raises a security concern about your work:

- stop the work immediately;
- if no imminent security risk exists, explain what you are doing; and
- do not resume work until the security concern is resolved.

Management-directed Stop Work

Responsible line managers (RLMs) may determine when a management-directed pause or stop work is necessary. If a pause or stop work is necessary, the RLM will:

- let workers and other affected RLMs know what operation or activities will be stopped;
- verify that those activities or operations have been stopped and develop an action plan that identifies the actions required before restarting work;
- let the workers and RLMs know what they are required to do to get their work restarted;
- document all pause- or stop-work actions and justification for restart; and
- authorize restart.

Note: Notify the Security Inquiry Team (665-3505) immediately to report potential or actual incidents of security concern.

Resources

- Security Help Desk, security@lanl.gov, 665-2002
- Deployed Security Officers, <http://int.lanl.gov/security/integrating/deployed.shtml>

Reference

Procedure for Pause/Stop Work (P101-18),

[https://policy.lanl.gov/pods/policies.nsf/LookupDocNum/P101-18/\\$file/P101-18.pdf](https://policy.lanl.gov/pods/policies.nsf/LookupDocNum/P101-18/$file/P101-18.pdf)



View and download all Security Smarts for your safety and security meetings

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

Note: Security Smarts are current as of the date of publication.

SecuritySmart

Export Control

Certain activities are subject to export control regulations:

- sending or transferring materials, equipment, and software (even commercial off-the-shelf software) to a foreign country;
- importing technology from a foreign country; and/or
- having contact with foreign nationals in the course of one's work.

Background

"Export control" does not mean that goods or technology cannot be taken out of the country; it does mean one may need a license to export to a particular country. Export licensing determinations are made on a case-by-case basis.

Export Control is intended to restrict the export of:

- goods and technology that would make a significant contribution to the military potential of another country or combination of countries;
- goods and technology to further the foreign policy of the United States or to fulfill its declared international obligations; and
- goods where necessary to protect the domestic economy from the excessive drain of scarce materials and to reduce the serious inflationary impact of foreign demand.

Deemed Export

One can "export" something to a foreign national without ever leaving the country. Transfer of technology to a foreign national in the US is deemed to be an export to that person's home country.

Violations of Export Control

Export control is regulated by various executive orders and federal statutes and agencies (e.g., the Department of Commerce, Department of State, and Nuclear Regulatory Commission). Both the Laboratory and workers may be liable if export control requirements are violated. Liabilities include (1) criminal sanctions of fines up to \$1 million and imprisonment for up to 10 years; (2) civil penalties; or (3) administrative sanctions, such as seizure of the items in question.

Customs Office

The Laboratory's Customs Office is available to help with obtaining licenses, commodity classifications, designating license exceptions, preparing shipping documents, approving all exports of commodities and software from the Laboratory, and maintaining central records of commodity and software exports.

Visit the Customs Office web site for more information:

<http://supply.lanl.gov/property/customs/default.shtml>

Resources

- Customs Office, 665-2194, customs@lanl.gov
- Classification Office, 665-6413



View and download all Security Smarts for your safety and security meetings
<http://int.lanl.gov/security/documents/index.shtml#security-smarts>

Note: Security Smarts are current as of the date of publication.



Official Use Only

Official Use Only (OUO) is intended to be viewed only by those individuals with a need-to-know. Ensure OUO is properly marked and protected.

W H A T I S O U O ?

Official Use Only must be unclassified and must meet both of the following criteria:

- Has the potential to damage government, commercial, or private interests if disseminated to people who do not need the information to perform their jobs or other DOE-authorized activities; and
- Falls under at least one of eight Exemptions 2 through 9 of the Freedom of Information Act (2-Circumvention of Statute; 3-Statutory Exemption; 4-Commercial/Proprietary; 5-Privileged Information; 6-Personal Privacy; 7-Law Enforcement; 8-Financial Institutions; 9-Wells)

I D E N T I F Y I N G

If the document is unclassified, as determined by an Authorized Derivative Classifier (ADC), determine the following:

- Does it contain information designated in an approved DOE classification guide as Official Use Only? If so, ensure the markings below are applied and the classification guide is cited.
- If guidance does not require an OUO marking, does the document contain unclassified information relating to any of the following eight exemptions listed above? If so, does the potential for damage as described above exist? If yes, then OUO markings may be applied but the "guidance" line is left blank. *Note: No specific authority is required to make an OUO determination, either by guidance or by category and damage determination.*

M A R K I N G

Mark the front page of **documents** with the following marking (Image A). *Note: both the exemption number and the category name must be entered.* Mark each subsequent page Official Use Only or, if space is limited, use the OUO acronym on the bottom of the page (Image B).

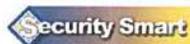
Image A

<p>OFFICIAL USE ONLY</p> <p>May be exempt from public release under the Freedom of Information Act (5 U.S.C 552), exemption and category: _____</p> <p>Department of Energy review required before public release</p> <p>Name/org: _____</p> <p>Date: _____</p> <p>Guidance (if applicable): _____</p>

Image B

<p>Official Use Only</p>
<p>Or</p>
<p>OUO</p>

Email messages must indicate OUO on the first line before the body of the text. Email messages must also indicate when attachments contain OUO information.



View and download all Security Smarts for your nested safety and security meetings <http://int.lanl.gov/security/documents/index.shtml#security-smarts>

P R O T E C T I N G

Nonelectronic media

When using OOU, reasonable precautions must be taken to prevent access of OOU information by persons who do not have the need-to-know. When not using it, store OOU matter in a locked receptacle (such as a room, desk, file cabinet, or safe).

Electronic Media

OOU information stored on a computer should have passwords, authentication, and file access control in place for protection.

T R A N S M I T T I N G

Mail outside the facility

Use a sealed, opaque envelope or wrapping, marked with recipient's address, a return address, and the words TO BE OPENED BY ADDRESSEE ONLY. Any of the following U.S. mail delivery categories may be used: First Class, Express, Certified, or Registered Mail. Any commercial carrier may be used.

Interoffice mail

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.

Hand-carrying between sites or within a site

The person carrying the information must control access to the information.

Over telecommunications circuits (including fax)

Protect by encryption whenever possible.

Email

OOU should be encrypted with NIST-validated encryption software (*Entrust*). When transmitted within the LANL yellow network, no encryption is required but it is suggested.

Note: If encryption capabilities are not available and transmission by mail is not a feasible alternative, then regular email or facsimile machines may be used to transmit the document. An email attachment can be password protected and the password communicated by other means. When using an unencrypted fax, transmission must be preceded by a telephone call to the recipient so that the document can be controlled when it is received.

R E P R O D U C I N G

OOU information can be reproduced (without the originator's permission) to the minimum extent necessary to carry out official activities. Copies must be marked and protected in the same manner as the originals. Copy machine malfunctions must be cleared and all paper paths checked for OOU information. Excess paper containing OOU must be destroyed as described below.

D E S T R O Y I N G

Nonelectronic media

At a minimum, destroy by using a strip-cut shredder that produces strips no more than 1/4 inch wide. Or collect in a sensitive unclassified burn box for destruction through burn-it@lanl.gov. The decision to dispose of any DOE or NNSA document, whether or not it contains OOU information, must be consistent with the policies and procedures for records disposition. Further questions about records disposition should be directed to your Records Management POC or IRM-RMMSO.

Electronic media

Users are not required to destroy electronic media that contains UCI. Disks should be overwritten using software such as BCWipe, available through ESD, before they are thrown away. Further questions about this topic should be directed to your OCSR.

Resources

Classification (SAFE-S7), 7-5011
 Classified Matter Protection and Control (SEC-SA5), cmpr@lanl.gov
 Security Help Desk, 5-2002 or security@lanl.gov
 Protecting Information,
<http://int.lanl.gov/security/protectinfo/index.php>
 ADC Listing,
<http://int.lanl.gov/security/security-contacts.shtml>
 Entrust webpage
<http://network.lanl.gov/entrust/index.php>

Security Smart

Unclassified Controlled Nuclear Information

Unclassified Controlled Nuclear Information (UCNI) is intended to be viewed only by those individuals with a need-to-know. Ensure UCNI is properly marked and protected.

W H A T I S U C N I ?

Unclassified Controlled Nuclear Information (UCNI) is certain unclassified but sensitive Government information whose unauthorized dissemination is prohibited under section 148 of the Atomic Energy Act. Such information may concern nuclear material, weapons, components, facilities that have utilized such items, and security relating to such facilities.

I D E N T I F Y I N G

Does the document contain unclassified information about nuclear material, weapons, or components, or information about a nuclear facility? If so, the document should be reviewed for UCNI in addition to classification review. Many, but not all Derivative Classifiers are also UCNI Reviewing Officials.

****UCNI determinations can only be made by UCNI Reviewing Officials based on approved UCNI Guidelines.****

M A R K I N G

The Reviewing Official ensures the following markings are added to the first page of the document (Image A). Mark documents on the top and bottom of every page or on the top and bottom of those pages containing UCNI with the following (Image B).

Image A

Unclassified Controlled Nuclear Information
NOT FOR PUBLIC DISSEMINATION
Unauthorized dissemination subject to civil and criminal sanctions under section 148 of the Atomic Energy Act of 1954, as amended (42 U.S.C. 2168)
Reviewing Official:

(Name/Organization)
Date:

Guidance used:

(list all UCNI guidance used)

Image B

Unclassified Controlled Nuclear Information
Or
UCNI

P R O T E C T I N G

Nonelectronic media

When using UCNI, an authorized individual must maintain physical control over the material to prevent unauthorized access. When not using it, store UCNI matter in a locked receptacle (such as a room, desk, file cabinet, or safe) to preclude unauthorized disclosure. The locked receptacle



View and download all Security Smarts for your nested safety and security meetings <http://int.lanl.gov/security/documents/index.shtml#security-smarts>

must have controls that limit access only to authorized workers.

Electronic media

UCNI stored on a computer should be restricted to only those that have a need to know. Examples of restrictions are passwords, authentication, file access control, encryption, and offline storage.

T R A N S M I T T I N G

If a transmittal document **does not** contain UCNI, mark the front of the transmittal document as follows:

Matter transmitted contains Unclassified Controlled Nuclear Information.
When separated from enclosures, this document is not UCNI.

If a transmittal document **does** contain UCNI information, mark the transmittal document as an UCNI document. The document originator obtains all reviews and approvals required for an UCNI document. Mark the front of the transmittal document as follows:

Matter transmitted contains Unclassified Controlled Nuclear Information.
When separated from enclosures, this document is UCNI.

Over telecommunication circuits (including fax)

Encryption must be used.

Mail outside the facility

Use an opaque envelope. Outer packaging must not indicate that the content within is UCNI. UCNI can be mailed using any of the following U.S. mail methods: U.S. First Class, Express, Certified or Registered Mail. Any commercial carrier may be used.

Interoffice mail

Use an interoffice envelope and mail through standard interoffice mail. Do not indicate that the content within is UCNI.

Email

When transmitted electronically outside LANL, UCNI must be encrypted with NIST-validated encryption software (**Entrust**). When transmitted within LANL's yellow network, no encryption is required but it is recommended. It is the sender's responsibility to ensure that the recipient understands the sensitivity of the information and the requirements for protecting that information.

R E P R O D U C I N G

The originator's permission is not required to reproduce UCNI. Reproduce to the minimum extent necessary. Mark and protect copies in the same manner as the original. If a copy machine malfunction occurs, clear all paper paths. Excess paper must be destroyed as described below.

D E S T R O Y I N G

Nonelectronic media

At a minimum, UCNI matter must be destroyed by using strip cut shredders that result in particles of no more than 1/4-inch wide strips. Or collect in a sensitive unclassified burn box for destruction through burn-it@lanl.gov. The decision to dispose of any DOE or NNSA document, whether or not it contains UCNI information, must be consistent with the policies and procedures for records disposition. Further questions regarding records disposition should be directed to your Records Management POC or IRM-RMMSO.

Electronic media

Users are not required to destroy electronic media that contains UCI. Disks should be overwritten using software such as BCWipe, available through ESD, before they are thrown away. Further questions about electronic media should be directed to your OCSR.

Resources

Classification (SAFE-S7), 7-5011
Classified Matter Protection and Control, (SEC-SA5), cmpe@lanl.gov
Security Help Desk, 5-2002 or security@lanl.gov
Protecting Information,
<http://int.lanl.gov/security/protectinfo/index.php>
ADC Listing,
<http://int.lanl.gov/security/security-contacts.shtml>
Entrust webpage
<http://network.lanl.gov/entrust/index.php>

SecuritySmart

Random Vehicle Inspections

The Laboratory's Associate Directorate for Security and Safeguards is continuously analyzing risks to facilities and assets. Recent vulnerability analyses indicate a need to expand random vehicle inspections by the Protective Force and a canine team.

Explosives detection had previously focused on commercial delivery vehicles at the Truck Inspection Station near the intersection of East Jemez Road (Truck Route) and NM Highway 4.

Beginning immediately, ALL vehicles — government, private, or commercial — that enter and exit Pajarito Road will be subject to random inspections by the Protective Force and explosives detection dogs.

Random vehicle inspections will take place at Pajarito Road and the Truck Inspection Station.

Inspection Process

- A Protective Force officer will notify a driver to pull over to a search area, which is marked with a sign and set off with traffic control devices.
- An inspection team, which includes a canine team, will inspect the entire vehicle (under the hood and chassis, the inside, and any items that are towed behind or secured to the roof of the vehicle).
- Upon completion of the inspection, the team will either give the driver permission to proceed or secure the vehicle and the surrounding area as necessary.



Important

Workers must cooperate with and follow the instructions of the Protective Force during inspections. Failure to do so may result in a security incident and notification of the Security Inquiry Team and the worker's line management.

Resources

- Security Help Desk, 665-2002, security@lanl.gov
- Security Perimeter Project, spp-questions@lanl.gov

Reference

Security Smart on Badge Checks and Inspections, <http://int.lanl.gov/security/documents/security-smart/2008/inspections708.pdf>

SecuritySmart

Property Protection Areas

Property Protection Area (PPA): All Laboratory-controlled property, including leased facilities, other than established Security Areas (Limited Areas and above).

Note:

The Laboratory permits the public to access certain PPAs (e.g., roads, parking lots, and vehicle access portals). The Laboratory also has PPA buildings (e.g., Otowi, Bradbury Science Museum) that are open to the public only during operating hours.



Worker Responsibilities

- Never discuss, work on, or store classified matter in a PPA.
- Wear a LANL security badge at all times while on LANL property (unless in a public access area).
- Do not introduce prohibited articles into PPAs.
- Permit the Protective Force to inspect vehicles and items being used or carried.
- Immediately notify the responsible line manager or Protective Force if theft, vandalism, arson, intrusion by unauthorized individuals, or other types of suspicious activity are observed or suspected.

Note:

Workers should also remind unbadged workers and visitors that badges are required in PPAs.

Division Leader, Responsible Associate Director, or Facility Operations Director (FOD) Responsibilities

- Implement controls to protect property used by workers from vandalism, arson, theft, and intrusion by unauthorized individuals.
- Ensure that signs prohibiting trespassing are posted at the perimeter of facilities under his or her control.

General Requirements

- Barriers are used to provide graded protection for properties and facilities. Outside operating hours, all doors must be locked.
- Signs prohibiting trespassing are posted at each entrance and at intervals along the perimeter of the property to ensure reasonable notice to persons who enter or attempt to enter the area.
- Access to the PPA building by the public outside operating hours requires written authorization by the FOD or designee.

Resources:

Physical Security Team: 667-2510, jey@lanl.gov
Security Help Desk, 665-2002, security@lanl.gov

Reference:

Property Protection Areas P202-3: <http://policy.lanl.gov/pods/policies.nsf/MainFrameset?ReadForm&DocNum=P202-3&FileName=P202-3.pdf>

View and download all Security Smarts for your safety and security meetings
<http://int.lanl.gov/security/documents/index.shtml#security-smarts>

SecuritySmart

Proof of United States Citizenship for the Badge Office

The Badge Office is required by law to verify US citizenship. The following lists the acceptable documents that individuals can bring to the Badge Office.

Native-born US Citizens

Primary Evidence

For an individual born in the United States, a current United States passport or a birth certificate are the primary and preferred means of citizenship verification. Acceptable birth certificates must show that the record was filed shortly after birth and must be certified with the registrar's signature. The birth certificate must bear the raised, impressed, or multi-colored seal of the registrar's office. The only exception is if a state or other jurisdiction does not issue such seals as a matter of policy. Uncertified copies of birth certificates are not acceptable. A delayed birth certificate (one created when a record was filed more than one year after the date of birth) is acceptable if it shows that the report of birth was supported by acceptable secondary evidence of birth.

Secondary Evidence

Secondary evidence may include baptismal certificates, hospital birth records, or affidavits of persons having personal knowledge about the facts of the birth. Other documentary evidence can be early census, school, or family records; newspaper files; or insurance papers. All documents submitted as evidence must be original or certified.

Note: An expired US passport is no longer acceptable as proof of US citizenship.

Naturalized US Citizens

For an individual claiming citizenship by naturalization, a Certificate of Naturalization (Form N-550 or N-570) showing the individual's name is required.

Foreign-born US Citizens

For an individual claiming citizenship acquired by birth abroad to a US citizen, one of the following (showing the individual's name) is required:

- Certificate of Citizenship (Form N-560 or N-561);
- Report of Birth Abroad of a Citizen of the United States of America (State Department Form FS 240);
- Certificate of Birth (Form FS 545 or DS 1350);
- A current US passport; or
- Record of Military Processing-Armed Forces of the United States (DD Form 1966), provided it reflects that the individual is a US citizen.

Resources

- Badge Office, 667-6901, badge@lanl.gov
- Security Help Desk, 665-2002, security@lanl.gov



View and download all Security Smarts for your safety and security meetings
<http://int.lanl.gov/security/documents/index.shtml#security-smarts>
 Note: Security Smarts are current as of the date of publication.

SecuritySmart

Generic "Visitor" and "Escort Required" Badges



The generic "Visitor" and "Escort Required" badges are intended for short-term visits by uncleared US citizens. These badges **MUST NOT** be given to foreign nationals.



Specific LANL sites that use the generic badges must develop procedures for their control, issue, and recovery. Organizations that fail to develop and implement control procedures will lose the privilege of issuing generic badges.

By default, generic "Visitor" and "Escort Required" badges will be issued by the Badge Office without a magnetic stripe.

- If a Laboratory organization requires "Visitor" or "Escort Required" badges with a magnetic stripe, the responsible line manager (RLM), in conjunction with subject matter experts from the Associate Directorate for Security and Safeguards (ADSS), must develop a security plan to control, issue and recover these badges. Encoded badges will be issued to the organization when the security plan is accepted by the Badge Office.
- "Visitor" or "Escort Required" badges with a magnetic stripe will be encoded only with a unique badge number.

Use of generic "Visitor" and "Escort Required" badges is limited to the specific building or facility covered by those badges. Use of these badges outside of these buildings or facilities is prohibited.

The RLM of the host organization must ensure uncleared official visitors have limited and controlled access to LANL facilities.

- Issuing the official visitor a badge with no magnetic stripe is a sufficient measure to limit and control access.
- If uncleared official visitors are issued a badge with a magnetic stripe, then the RLM is responsible for developing controls that preclude passage through access control systems outside the official visitor's work area(s) during and after normal work hours.

Collecting the official visitor's badge at the end of each day is a sufficient measure to limit and control access.

Other methods of limiting and controlling uncleared official visitor access to LANL facilities must be discussed with and approved by appropriate ADSS deployed personnel.

Resources

Badge Office: 667-6901, badge@lanl.gov
 Security Help Desk: 665-2002, security@lanl.gov

Reference

P203-1 Security Badges: <http://policy.lanl.gov/pods/policies.nsf/MainFrameset?ReadForm&DocNum=P203-1&FileName=P203-1.pdf>

View and download all Security Smarts for your safety and security meetings
<http://int.lanl.gov/security/documents/index.shtml#security-smarts>



SecuritySmart

Substance Abuse Testing and Reporting UPDATE

Reporting

In addition to reporting arrests or convictions of any criminal drug statute violations to PS-3, **ALL WORKERS** are now required to report arrests or convictions of any alcohol-related incidents (e.g., driving under the influence, driving while intoxicated, public intoxication). PS-3 will notify Occupational Medicine (OM-MS). OM-MS may conduct a medical and or psychological evaluation of the worker as part of monitoring for Fitness For Duty or the Human Reliability Program.



LANL's Mobile Testing Units

Note

Workers restricted from driving as a result of alcohol related arrests or convictions are prohibited from driving government vehicles.

Testing Requirements

- In addition to the drug and alcohol testing conducted under our institutional program (see P732 Substance Abuse), drug testing is now being conducted for L- and Q-cleared workers as part of a federally mandated and regulated program (10 CFR 707). **All new L and Q security clearance applicants will be drug tested before a clearance is granted.**
- When work is being performed outside of business hours, drug and/or alcohol testing under reasonable suspicion or post incident/accident can now be performed. Managers are instructed to contact SOC-LA, LANL's Protective Force, for testing procedures.

Resources

- Personnel Security (PS-3): 667-4264
- Human Resources-Employee Relations (HR-ER): 667-8370
- SOC-LA: 667-4437
- Internal Inquiries (SAFE-2): 665-2002
- Security Help Desk: 665-2002, security@lanl.gov

References

1. Substance Abuse Policy (P732): <http://policy.lanl.gov/pods/policies.nsf/MainFrameset?ReadForm&DocNum=P732&FileName=P732.pdf>
2. Contractor Workplace Substance Abuse Program at DOE Sites (10 CFR 707) Website: <http://www.hss.energy.gov/HealthSafety/WSHP/rule851/rule707.html>

View and download all Security Smarts for your safety and security meetings
<http://int.lanl.gov/security/documents/index.shtml#security-smarts>

Security Smart

Clearance Reporting Requirements

Workers or their managers must notify Clearance Processing within one work day of the following events:

1. When a cleared worker or applicant declines an offer of employment or fails to report for duty.
2. When made aware of information of a personnel security interest, including but not limited to:
 - Legal action effected for a name change;
 - Change in citizenship status;
 - Use of an illegal drug or use of a legal drug in a manner that deviates from approved medical direction;
 - Arrests, criminal charges (including charges that are dismissed), citations, tickets, summons or detentions by Federal, State, or other law enforcement authorities (including Tribal authorities) for violations of law within or outside of the US. Traffic violations for which a fine of up to \$300 was imposed need not be reported, unless the violation was alcohol- or drug-related;
 - An immediate family member assuming residence in a sensitive country;
 - Hospitalization for mental health reasons or treatment for drug or alcohol abuse;
 - Employment by, representation of, or other business-related association with a foreign or foreign-owned interest or non-US citizen or other individual who is both a US citizen and a citizen of a foreign country;
 - Personal or business-related filing for bankruptcy;
 - Garnishment of wages;
 - Situations or incidents that may impact an individual's eligibility for a security clearance.
3. Whenever a cleared worker or applicant learns of the presence of any situations listed in number 2 above with regard to anyone they know to possess a DOE security clearance or to be in the process of obtaining a DOE security clearance.
4. Matters of potential counterintelligence interest (including approaches by individuals seeking unauthorized access to classified information or SNM and foreign travel).
5. When line management restricts or withdraws a worker's access to classified information or special nuclear material (SNM) without Department of Energy direction.
6. When made aware of the death of a cleared worker or applicant.
7. When a cleared worker or applicant terminates employment.
8. When a cleared worker or applicant no longer requires access to classified information or SNM.
9. When a cleared worker or applicant is transferred to another location internal or external to LANL.

Note: Refer to the Security Smart on Reporting Requirements for Marriage or Cohabitation for more information about reporting requirements for marriage and cohabitation.

Resources

- Clearance Processing, clearance@lanl.gov, 667-7253
- Security Help Desk, security@lanl.gov, 665-2002

Reference

DOE Order 472.2, Personnel Security, <https://www.directives.doe.gov/directives/current-directives/472.2-BOrder/view?searchterm=472.2>

View and download all Security Smarts for your safety and security meetings
<http://int.lanl.gov/security/documents/index.shtml#security-smarts>

Note: Security Smarts are current as of the date of publication.



SecuritySmart

BADGE HOLDER RESPONSIBILITIES

Every Laboratory worker and visitor is badged. Whether cleared or uncleared, badge holders must follow Department of Energy and Laboratory rules regarding protecting their badges.

Workers must:

- Remove their badges and protect them from public view off Laboratory-owned, leased, or rented property.
- Not use their badges for identification or unofficial purpose (e.g., cashing checks or checking into a hotel when on vacation). Workers must not scan their badges to fax, post on Web sites, or email for any reason. Note: Workers on official Laboratory travel may use their badges to qualify for discounts, provided they do not allow others to make copies of the badges.
- Submit a Notification of Permanent Inactivation of Badge (Form 1672) in person to the Badge Office if their badges are lost or stolen.



The new federal security badge

Frequently Asked Questions

Q. Can I wear my badge at the Hot Rocks Cafe?

A. Because Hot Rocks is housed in the Research Park, which is a leased facility adjacent to the Otowi, workers may wear their security badges at the cafe.

Q. Can I wear my badge on the Park and Ride bus?

A. Park and Ride is public transportation. Laboratory workers should not wear their badges at bus stops and buses.

Q. When I am going to lunch or running an errand, can I leave my badge in the car?

A. You can leave your badge in the car provided it is out of sight and the car is locked. Badges should not be left in the car for extended periods such as overnight.

Q. When I go to a gas station in town to fill up a Laboratory vehicle, can I keep my badge on?

A. Badges should not be worn while filling up vehicles. Note: If the gas station attendant requests to see a worker's badge as proof of employment, one may show the attendant the badge.

Resources

Badge Office, badge@lanl.gov, 667-6901
Security Help Desk, security@lanl.gov, 665-2002

References

- 1) Security Smart: Protecting Your New Federal Security Badge, April 2008:
http://int.lanl.gov/security/documents/security-smart/2008/badge_care0408.pdf
- 2) Security Smart: Badge Troubleshooting Tips, April 2008:
http://int.lanl.gov/security/documents/security-smart/2008/badge_trouble0408.pdf

View and download all Security Smarts for your safety and security meetings
<http://int.lanl.gov/security/documents/index.shtml#security-smarts>

SecuritySmart

Photography on Laboratory Property

The use of photographic equipment (e.g., video recorders, film and digital cameras, including cell phones with camera) is prohibited on Laboratory property without approval.

Workers who want to take photographs must:

1. Request prior approval by electronically submitting [Form 1897PA](#);
2. Carry a copy of the approved [Form 1897PA](#) while taking photographs; and
3. Present the approved [Form 1897PA](#) to anyone who requests to see it.

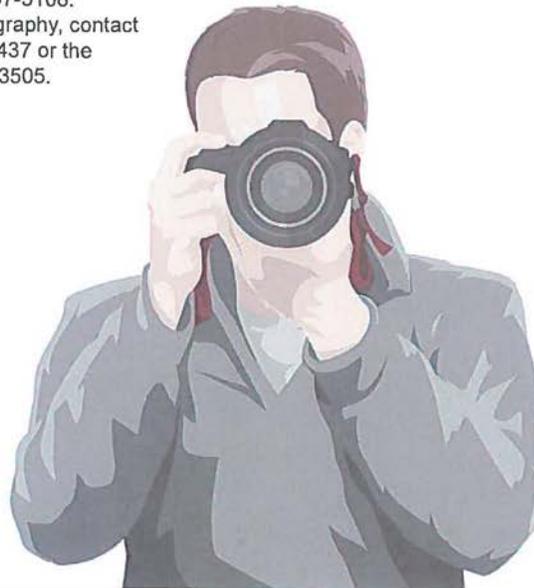
Note: The completed [Form 1897PA](#) expires one year after the issue date. When using a previously completed form, double check to ensure it has not expired.

Workers who see photography on Laboratory property should:

1. Question anyone taking the photographs;
2. Ask to see the photographer's approved [Form 1897PA](#); and
3. Immediately notify the Protective Force or Security Inquiry Team to report unauthorized photography.

Resources

- For more information, contact the Classified Matter Protection Group at 667-5108.
- To report unauthorized photography, contact the Protective Force at 667-4437 or the Security Inquiry Team at 665-3505.



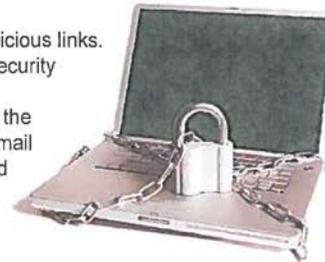
SecuritySmart

Protecting Your Computer

The Laboratory's Yellow network prevents most cyber attacks. Computer users are an integral part of Yellow network defenses and must ensure their own systems are protected.

Steps to Take

- Do not open unknown email attachments or click on suspicious links.
- Download and install the most recent operating system security patches.
- Ensure an anti-virus application is installed, updated with the latest definitions, and functioning to frequently scan (1) email for viruses, (2) all files being accessed by the system, and (3) all files on the system.



Passwords

Wherever possible, a token card (CRYPTOCARD) that generates a one-time passcode should be used for authentication. When a token card cannot be used, creating strong passwords is important in preventing unauthorized access to your computer. Reusable passwords:

- must be a minimum of 8 characters and be changed at least every 180 days;
- must contain a variety of characters (upper-case letters, lower-case letters, numbers, and symbols);
- cannot be names or common words (those found in a dictionary); and
- must never be shared.

See Attachment A of Cyber Security Access Controls, P218 (<https://policy.lanl.gov/pods/policies.nsf/MainFrameset?ReadForm&DocNum=P218&FileName=P218.pdf>), for more information.

Traveling

Computers (usually laptops) that are taken on travel or used at home are generally more susceptible to being infected than computers that stay within the Yellow network. Some precautions to take:

- Before taking a system off site, ensure that it has the latest patches and anti-virus definitions. Laptops must be checked for viruses (using the latest anti-virus definitions) BEFORE they are re-connected to the Yellow network.
- All laptops taken on foreign travel must be borrowed from the Laboratory's laptop pool. There are property, export control, and security issues that must be addressed. Contact your Organizational Computer Security Representative (OCSR) for more information.

Reporting an Information Security Incident

Report all potential information security incidents to the Security Inquiry Team (SIT) at 505-665-3505. After hours or on weekends, page the On-call Duty Officer at 505-949-0156.

For more information, see the Security Smart on Computer User Responsibilities:
http://int.lanl.gov/security/documents/security-smart/2009/comp_resp509.pdf

Resources

Information on anti-virus definitions is available at <https://esd.lanl.gov>
Send questions regarding network security to csirt@lanl.gov

SecuritySmart

Computer User Responsibilities

Computer users are the most important component of the Laboratory's information security program. Heeding the following guidelines will help protect the Laboratory's information assets.

- Get to know your Organizational Computer Security Representative (OCSR) and Systems Security Officer (SSO).
Visit http://int.lanl.gov/security/cyber/docs/ocsr_issso_list.xls
- Complete required initial and annual information security training:
<http://int.lanl.gov/security/cyber/training/training.shtml>
- Know the sensitivity level of the data you process and how to protect that data.
- Understand the "need-to-know" concept before you share information with others.
- Recognize when a computer security incident has occurred and promptly report it to the Security Inquiry Team (SIT) at 665-3505 and your responsible line manager.



Minimum Computer Protections

- Ensure your system has been accredited for use by meeting Institutional Security Requirements (see Certification and Accreditation at <http://int.lanl.gov/security/cyber/accreditation/index.shtml>).
- Implement Laboratory password guidelines for all of your accounts and your screensaver. (See P218, Cyber Security Access Controls.)
- Enable screensaver protections whenever you're away from your computer. Configure your system to automatically engage the screensaver after 15 minutes of inactivity.
- Display the official DOE warning banner on all computer systems:
<http://int.lanl.gov/security/cyber/access/banner.shtml>
- Ensure virus protection software is installed on your system(s) and update definition files at least weekly.
- Use approved methods to complete regular backups of your data.
- Ensure that you have licenses (or proof of legal ownership) for all your applications.
- Follow the established guidelines for destroying data and salvaging computer equipment. Coordinate these activities with your OCSR and property administrator.

For more information, also see the Security Smart on Protecting Your Computer:
http://int.lanl.gov/security/documents/security-smart/2009/protect_comp509.pdf

Resources

Information Security Website: <http://int.lanl.gov/security/cyber/>
Contact: cybersecurity@lanl.gov, 665-1795

Security Smart

Protecting Emails and Attachments

Workers must ensure that email containing classified information is not transmitted over unclassified email channels.

Review Before Sending

Review the entire content (text in email and attachments) to verify that it does not contain classified information. If the email could potentially contain classified information, have a derivative classifier (DC) review it.

Emails with Classified Information

If the emails contain classified information, they must be transmitted only on systems approved for classified transmission and sent only to individuals with the appropriate clearance level and need to know.

Marking the Email and Attachments

Mark, as the first item of information in the text, either the highest level and category of the accredited classified information systems or the appropriate markings for the classification of the information as determined by a DC. Also mark any applicable caveats or special handling and dissemination requirements.

Emails without Classified Information

If the email does not contain classified information, it can be sent over unclassified email channels. However, keep in mind that emails with controlled unclassified information (CUI), such as Official Use Only (OUO), Unclassified Controlled Nuclear Information (UCNI), and Personally Identifiable Information (PII), have additional requirements:

- OUO: Indicate OUO on the first line before the body of the text.
- UCNI: When transmitted electronically outside LANL, UCNI must be encrypted with NIST-validated encryption software (Entrust). When transmitted within LANL's yellow network, no encryption is required but it is recommended.
- PII: Emails containing PII must be encrypted before sending outside the Laboratory.

Remember: Compilation of one or more unclassified attachments and a string of unclassified emails may make the entirety of an email **classified**.

Resources

- Classification Group, 7-5011
- Security Help Desk, 5-2002 or security@lanl.gov
- Security Inquiry Team, 5-3505

References

1. Derivative Classifier (DC) List http://int.lanl.gov/security/protectinfo/class/docs/restricted/ADC_List.pdf
2. Controlled Unclassified Information Procedure, P204-1, <https://policy.lanl.gov/pods/policies.nsf/MainFrameset?ReadForm&DocNum=P204-1&FileName=P204-1.pdf>

SecuritySmart

Wireless Networking

Wireless networking may provide a means to transmit or transport sensitive unclassified and classified information in an unauthorized manner.

Restrictions on wireless networking (802.11) vary by area:

- **Public Access Areas**
The use of wireless networking, Bluetooth, and cell phones is allowed in areas accessible by the public (within the identified publicly accessible portions of buildings and in public access areas outside buildings, such as roadways, sidewalks, and parking lots).
- **Property Protection Areas (PPAs)**
The use of cell phones is typically allowed in PPAs (always check local restrictions). However, the use of wireless networking and Bluetooth is prohibited unless approved by the National Nuclear Security Administration (NNSA).
- **Limited Areas**
The use of wireless networking, Bluetooth, and cell phones is prohibited in Limited Areas unless approved by the NNSA.

Other Wireless Protocols

Radio frequency (RF) and infrared (IR) data communications are allowed in **SOME** instances:

- IR data communications and wireless keyboards are allowed in PPAs on unclassified systems that do not process sensitive information. They are prohibited in Limited Areas.
- RF keyboards are prohibited in all LANL areas.
- IR and RF wireless mice that do NOT use Bluetooth are allowed on unclassified systems where there is no classified processing (unclassified computing environment).
- RF and IR remote controls are allowed on unclassified presentation equipment in unclassified workspaces without restrictions; they are prohibited on classified computers (IR and RF controls are permitted to control classified projectors).

Disabling Wireless Capabilities

Owners of Laboratory computers must ensure that wireless networking capabilities are disabled. Organizational Computer Security Representatives (OCSRs) can help with this task. Users of classified systems must physically disable wireless capabilities. The Cyber Systems Security Officer (CSSO) oversees this process.

Obtaining Approval for Wireless Devices

Contact the Wireless Team by e-mailing wireless@lanl.gov.

Resource

Information Security (Cyber) Help Desk, cybersecurity@lanl.gov

References

1. Cyber Security Wireless Computing Devices, P213, <https://policy.lanl.gov/pods/policies.nsf/MainFrameset?ReadForm&DocNum=P213&FileName=P213.pdf>
2. Cyber Security Certification and Accreditation, P216, [https://policy.lanl.gov/pods/policies.nsf/LookupDocNum/P216/\\$file/P216.pdf](https://policy.lanl.gov/pods/policies.nsf/LookupDocNum/P216/$file/P216.pdf)
3. OCSR and ISSO List, http://int.lanl.gov/security/cyber/docs/ocsr_issso_list.xls

View and download all Security Smarts for your safety and security meetings
<http://int.lanl.gov/security/documents/index.shtml#security-smarts>

SecuritySmart

Unclassified Video Teleconferencing

Video teleconferencing (VTC) allows workers to conduct a meeting with colleague in another location using video and audio communication. This technology saves time and money by allowing workers to participate in meetings locally rather than requiring travel for face-to-face meetings. However, video teleconferencing can increase the risk of unauthorized disclosure of classified information and controlled unclassified information (CUI).

Workers must be aware of the security vulnerabilities associated with VTC equipment and be aware of the procedures and controls in place to protect data.

Note: Only approved webcams and microphones may be used. LANL currently is testing a standard device for compliance with national security requirements, and will release a standard as soon as testing is complete. Protect classified and sensitive matter.

Protect classified and sensitive matter.

Workers must prevent classified information and CUI from being exposed during the VTC.

- Limit VTC interaction to only unclassified and non-CUI information.
- Ensure that CUI and classified matter are stored, covered, or otherwise removed from the view of the camera.
- Ensure that the area where the VTC is located is protected from accidental disclosure of classified information or CUI. Controls may include closing doors and windows, posting signs announcing VTC, and informing coworkers that VTC is taking place.
- Disconnect external cameras and microphones when not in use.

Using a Computer System Configured for Document Sharing

Workers may also conduct a VTC using a dedicated computer with an external web camera with microphone, and sharing documents from the desktop. If a VTC is conducted on a computer configured for document sharing, the user must take additional measures to protect data.

- The user must load only the data required for the VTC on the computer and remove the data after the session is complete.
- Disconnect network shared resources (such as a shared server or network drive) from the computer.
- Use a CRYPTOCARD to authenticate with the Web proxy which will be used to connect to the remote system.

Resources:

Cyber Security, cybersecurity@lanl.gov

References

P 217, Controlled Articles

P 218, Cyber Security Access Controls

P 204-1, Controlled Unclassified Information



View and download all Security Smarts for your safety and security meetings
<http://int.lanl.gov/security/documents/index.shtml#security-smarts>
 Note: Security Smarts are current as of the date of publication.

SecuritySmart

Security Awareness

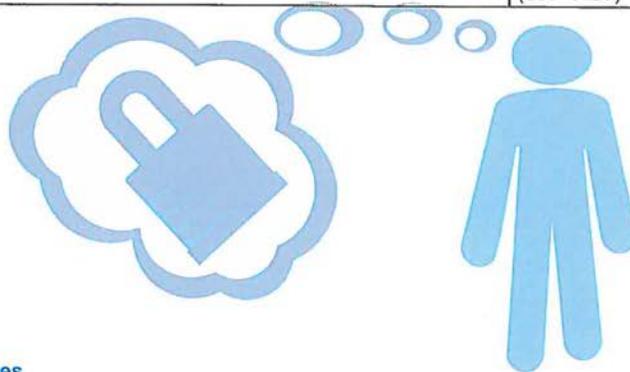
Laboratory workers should always be vigilant of their surroundings.

Workers should inspect work areas frequently for

- suspicious activities;
- unattended packages; and
- signs of tampering or indications of forced entry into doorways or windows.

In addition to locking parked vehicles, workers should also get in the habit of inspecting their vehicles for suspicious items before entering and driving.

Situations to Report	Whom to Call
Suspicious or unknown persons, particularly those carrying suitcases or other containers or those observing, photographing, or asking questions about site operations or security measures; protesters and unauthorized demonstrations	Protective Force (667-4437) or Security Inquiry Team (665-3505)
Unidentified vehicles parked or operated in a suspicious manner on or near Laboratory facilities	Protective Force (667-4437)
Abandoned packages; low-flying aircraft	Emergency Operations (667-6211) or Protective Force (667-4437)
All other unauthorized activities or anything out of the ordinary	Protective Force (667-4437)



Resources

- Security Help Desk, 665-2002, security@lanl.gov
- Physical Security Team, 667-1607



View and download all Security Smarts for your safety and security meetings
<http://int.lanl.gov/security/documents/index.shtml#security-smarts>

SecuritySmart

Reporting Requirements for Vehicle Accidents

For many years, the Laboratory has conducted substance abuse testing following accidents. Testing protects both Los Alamos National Security, LLC, and the employee by, in most cases, ruling out substance abuse as a causal factor. In the past year, the Laboratory has increasingly focused on vehicle safety following serious automobile accidents. As part of this effort, the Laboratory is ensuring it obtains timely information to determine if substance abuse testing is appropriate in any given circumstance. Effective immediately, all workers must now notify their managers when involved in a vehicle accident that resulted in or had the potential for injury when:

- the worker is driving any government-owned vehicle, including motorized equipment such as a forklift, on or off Laboratory property, **or**
- the worker is driving any private vehicle (including rental vehicles) within the boundaries of a Laboratory Technical Area other than TA 00, which comprises downtown Los Alamos.

Examples

- If a worker is driving a private vehicle on Laboratory property for any reason (e.g., returning from lunch) and is involved in an accident that resulted in or had the potential for injury, the worker must notify his or her manager.
- If a worker is driving a private vehicle in downtown Los Alamos and has an accident, even if the travel was for a work-related purpose, the worker is not required to notify his or her manager.
- If a worker is driving a government-owned vehicle to a meeting at Sandia National Laboratories and is involved in an accident in Albuquerque that resulted in or had the potential for injury, the worker must notify his or her manager.

Notification

A worker must notify his or her manager as soon as possible after being involved in a vehicle accident as described above. The manager must coordinate with Personnel Security (PS-3); in consultation with the manager, PS-3 will determine if testing is appropriate, based on all circumstances. If the worker's manager is unavailable, the worker must notify the next level manager or PS-3.

See the [Substance Abuse Procedure, P732](#), for details on testing protocols and notification requirements.

Refusal to be Tested

Consistent with the LANS Procedure on Substance Abuse, P732, a worker who refuses to be tested, will be treated in same manner as if there is a confirmed positive result.

Resources

- Human Resources-Employee Relations, employee_relations@lanl.gov, 667-8730
- Personnel Security, 667-4264
- Security Help Desk, security@lanl.gov, 665-2002

Training

Course #42095, Substance Abuse Policy and Procedure P732, for all Laboratory workers.



View and download all Security Smarts for your safety and security meetings
<http://int.lanl.gov/security/documents/index.shtml#security-smarts>

Note: Security Smarts are current as of the date of publication.

SecuritySmart

Reporting Security Incidents

All **potential** and **actual** incidents of security concern must be reported **IMMEDIATELY** to the Security Inquiry Team (SIT).

Why?

Timely reporting of incidents allows security professionals to mitigate breaches, address vulnerabilities, and notify higher authorities at the Laboratory and Department of Energy.

A Few Examples of What Must be Reported

- Compromise or loss of personally identifiable information (e.g., social security numbers, dates of birth)
- Unsecured classified and sensitive (e.g., Official Use Only, Unclassified Controlled Nuclear Information) matter
- Unauthorized disclosure of classified or sensitive information to a person without a need to know
- Cell phones and other unapproved portable electronic devices in security areas
- Unknown or unescorted persons in security areas
- Suspicious emails (e.g., scams, phishing) received on work computers
(Note: **NEVER** forward suspicious emails.)

Reporting Guidelines

- Call the SIT immediately.
- Notify a responsible line manager and deployed security professional.
- Do not email or use other unsecure forms of communication to provide details about an incident.
- Do not discuss the incident with others unless they have a need to know.
- Discontinue the use of an affected system (e.g., cell phone, computer).
- Secure a breached area or unprotected classified / sensitive matter.
- If unsure whether something odd or suspicious is a security incident, report.

For more information about reporting, consult the **Reporting Known and Potential Incidents of Security Concern Procedure**, P 201-3, <https://policy.lanl.gov/pods/policies.nsf/MainFrameset?ReadForm&DocNum=P201-3&FileName=P201-3.pdf>

Contacts

- Security Inquiry Team: 665-3505
- Security Help Desk: 665-2002, security@lanl.gov
- SOC-Los Alamos: 667-4437
- After-hours Duty Officer: 949-0156 (pager)

View and download all Security Smarts for your safety and security meetings
<http://int.lanl.gov/security/documents/index.shtml#security-smarts>
Note: Security Smarts are current as of the date of publication.

SecuritySmart

Foreign National Access into LANL Buildings

Foreign national workers and visitors (including those who have US permanent residency status) must be approved by the Office of Counterintelligence/Foreign Visits & Assignments Office (OCI/FVA) prior to their arrival at LANL. A request through the Database for International Visits and Assignments (DIVA) must be approved before foreign nationals access a LANL facility.

If a foreign national needs access to a building not listed on DIVA, his or her host can update the approved DIVA record.

Non-secure Areas

All foreign nationals approved by OCI/FVA will automatically have approved access into the following uncleared areas:

- TA-3, Bldg. 261 (Otwi Cafeteria and Badge Office);
- TA-3, Bldg. 207 (Study Center—first floor only from 8:30 to 4:00);
- TA-3, Bldg. 443 (University House);
- TA-00, Bldg. 760 (Legal Counsel); and
- TA-3, Bldg. 1411 (Occupational Medicine).

All other buildings in non-secure areas must be individually accounted for in DIVA. A list of approved buildings for foreign national access is online at <http://diva.lanl.gov/fva/doc?page=exemption-list-webpage>.

Secure Areas

Access to secure areas by uncleared foreign nationals is generally prohibited. Contact OCI/FVA for guidance with the process as it requires approval of the following: DIVA, Form 1726, Specific Access Agenda, Maps, Escort Forms, and coordination with the Protective Force by OCI/FVA.

Reporting Requirements

Entry into an unauthorized building by a foreign national may be a security event. If a foreign national worker has entered a non-secure or secure LANL building that was not approved in DIVA, it is a potential incident of security concern and must be immediately reported (via secure means) to the Security Inquiry Team (SIT).

Resources

OCI/FVA: 665-1572, foreignvisit@lanl.gov
 Security Help Desk: 665-2002, security@lanl.gov
 SIT: 665-3505

Reference

Foreign Visits and Assignments Web Site, <http://int.lanl.gov/security/isec/fva/>
 DIVA, <http://int.lanl.gov/security/isec/fva/diva.shtml>



SecuritySmart

Unclassified Foreign Visits in Leased Facilities

Laboratory workers must protect government equipment, real property, Controlled Unclassified Information (CUI), and intellectual property by controlling access to leased facilities.

LANL leases privately owned facilities throughout Los Alamos County. Some examples include the Research Park, Pueblo Complex, Central Park Square, and the White Rock Training Center. All leased space are considered Property Protection Area's (PPA), with the exception of the Bradbury Science Museum, which is an Open Area where the general public is allowed.



Access Requirements to PPAs

All non-US visitors and assignees MUST be:

- vetted and approved prior to their arrival and must be processed through the Badge Office for a standard site-specific badge;
- approved and badged prior to their access to ANY Laboratory facilities, whether owned or leased.

DIVA

The Database for International Visits and Assignments (DIVA) is the means by which the Laboratory processes requests to have foreign nationals on Laboratory-owned or -leased property for work or visits. Following DIVA approval, Foreign Visits and Assignments (FV&A) authorizes the Badge Office to issue badges to foreign national visitors.

Non-US visitors are confined to access facilities that are specifically listed on their DIVA records. Hosts may select these areas from the Approved Building List (<http://diva.lanl.gov/fva/doc?page=exemption-list-webpage>).

Important Note

Hosts and other workers must not invite non-US visitors to a Laboratory facility until those visitors have an: 1) approved visit request in DIVA, and 2) active Oracle record and Z#.

Resources

- Foreign Visits and Assignments, 665-1572
- Security Help Desk, security@lanl.gov, 665-2002

Reference

- 1) Property Protection Areas Procedure, P202-3, [https://policy.lanl.gov/pods/policies.nsf/LookupDocNum/P202-3/\\$file/P202-3.pdf](https://policy.lanl.gov/pods/policies.nsf/LookupDocNum/P202-3/$file/P202-3.pdf)
- 2) Personnel Security Procedure, Part 6, P200-3, [https://policy.lanl.gov/pods/policies.nsf/LookupDocNum/P200-3/\\$file/P200-3.pdf](https://policy.lanl.gov/pods/policies.nsf/LookupDocNum/P200-3/$file/P200-3.pdf)