Prohibited Articles

The following articles are **prohibited** on LANL property, including parking lots and leased areas:

- any dangerous weapons, explosives, or other dangerous instrument or material likely to cause substantial injury or damage to persons or property
- alcoholic beverages;
- controlled substances (e.g., illegal drugs and associated paraphernalia, but not prescription and over-the-counter medication); and
- other items prohibited by law.

Controlled Articles

The following are **controlled** articles and are not allowed in Limited Security Areas or above:

- personal **computers** and associated media (including palm-top computers, non-government-owned media or software) that have not been approved for use;
- **cell phones**, **two-way** pagers, and personal digital assistants;
- recording equipment (audio, video, optical, or data);
- cameras (video or still, film or digital);
- electronic equipment with a data exchange port (USB thumb drives, iPods) that can be connected to automatic information system equipment; and
- radio frequency transmitting equipment (including computers or peripherals with active Bluetooth, infrared, and/or RF capabilities, unless disabled).

Note 1: Government cell phones are allowed into Security Areas as long as the batteries are removed.

Note 2: Visitors may have non-government controlled articles on LANL property outside Security Areas, but unless approved in advance they cannot: 1) take photographs on LANL property; 2) connect the article to LANL computers or networks; and 3) load sensitive government data on the article.

Note 3: Your host will work on any exemptions you need.

Resources

Cyber Security: http://int.lanl.gov/cyber/
Personnel Security: http://int.lanl.gov/security/personnel/index.shtml
Photography Policy: http://policy.lanl.gov/pods/policies.nsf/MainFrameset?ReadForm&DocNum=Notice0184&FileName=notice0184.pdf
Prohibited and Controlled Articles: http://int.lanl.gov/security/personnel/badge/prohibited.shtml
Protecting Information: http://int.lanl.gov/security/protectinfo/
Safety: http://int.lanl.gov/safety/index.shtml
Security: http://int.lanl.gov/security/index.shtml

Security Areas

In addition to specially designated Security Areas (e.g., Sensitive Compartmented Information Facilities and Special Access Program Facilities), LANL has the following types of Security Areas:

Material Access Area (MAA): A Security Area authorized to contain a Category I quantity of Special Nuclear Material.

Limited Area (LA): A Security Area used for the protection of classified matter and/or Category III or IV quantities of Special Nuclear Material, and provides a location where protective personnel or other internal controls prevent access by unauthorized persons to classified matter or Special Nuclear Material.

Exclusion Area (EA): A Security Area where one's mere presence can be expected to result in access to classified information.

Protected Area (PA): A Security Area used for protection of Category II Special Nuclear Material and classified matter and/ or to provide a concentric security zone surrounding an MAA.

Property Protection Area (PPA): All LANL controlled property, including leased facilities, other than established Security Areas (LAs or above). PPAs are not authorized for storage or processing of classified matter; PPAs are established to protect Government-owned property against damage, destruction, or theft.

Emergency

- Ask your host about your building's evacuation routes and your group's muster area in case of an emergency.
- If you are handling classified, your safety comes first and you must do what is necessary to evacuate safely. If possible, however, ensure classified matter is secure before leaving the site.

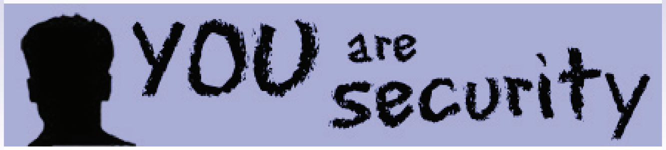
Contacts

• Security Help Desk	665-2002
• Badge Office	667-6901
• Cyber Security	665-1795
• Emergency Response	667-6211
• Fire, Bomb Threat, etc.	911
• Fraud, Waste, and Abuse	665-6159
• Office of Inspector General	800-541-1625
• Protection Technology Los Alamos (PTLA)	665-1279
After Hours Duty Officer	667-4409
• Safety Help Desk	665-7233
• Security Inquiry Team	665-3505

Visitor Guide to Smart Security

Welcome to Los Alamos National Laboratory. As an official visitor, you are considered a LANL "worker". As such, you must follow the Laboratory's security policies and procedures. Whether you are here fewer than 10 days or much longer, following the Laboratory's established procedures will help you avoid compromising national security.

Note: If you are a visitor for longer than 10 days during a calendar year, you must take at least the General Education Training (GET) and additional safety and security training depending on your work and work site. Consult your host(s) for specifics.



Los Alamos
NATIONAL LABORATORY
EST. 1943

Personnel Security

Badges

LANL-issued badges are the property of the U.S. Government. Visitors must return their badges when they are no longer needed, become invalid, or are damaged. Since badges are individually accountable, failure to return them will preclude future badging services. Know your badgeholder responsibilities.

- Report lost or stolen badges to the Badge Office in person.
- You must wear your badge above the waist with the photo facing out at all times while on LANL-owned or -leased property.
- You must wear your badge when participating in recreational activities if the activities take place on LANL-owned or -leased property.
- You must remove your badge when leaving LANL-owned or -leased property and when entering businesses or other locations where the badge may be seen by other members of the public.
- Good Practice: If leaving your badge in a vehicle during the day, make sure the badge is out of sight and the vehicle is locked. Do not leave your badge in a vehicle overnight.

Escortee/Escort

As a visitor, you may be escorted into an area to which you are not permitted unescorted access. A visitor may not escort another visitor or an uncleared person.

If you are being escorted:

- Wear your visitor badge, if the area you visit requires it, and return it to your host when the escorted visit is over.
- Stay with your escort at all times.
- Adhere to local requirements of your host organization. If being escorted into a Security Area, help your host by ensuring you do not have a cell phone or other prohibited/controlled articles. See section on Prohibited and Controlled Articles.

Stop Work

You have the authority and responsibility to stop work if you discover that you or your co-workers are exposed to imminent danger or if there is a potential for security risk. Contact the Safety Help Desk (safety@lanl.gov) or Security Help Desk (security@lanl.gov) for more information. See the Contacts list.

Physical Security

Automated Access Control Posts

The automated posts require that cleared visitors swipe their badges and enter personal identification numbers (go to the badge office to obtain a PIN).

Vehicle Access Portals (VAPs)

VAPs limit access to sensitive locations at LANL to authorized personnel or vehicles. All vehicles are subject to inspection.

LANL's security perimeter controls access to the Lab through three external VAPs: two on East and West Jemez and one on the southeast end of Pajarito Road at NM 4. A fourth VAP is located within the security perimeter and is located on the northwest end of Pajarito Road.

At the current SECON 3+, it is not necessary to hand over your badge at the East and West Jemez VAPs, but you must do so at the Pajarito Road VAPs.

Additional limits on access through VAPs may be imposed if LANL's Security Condition (SECON) is raised. Since September 2001, the Laboratory has never been at lower than 3+.

Note: Contact your host about details for your specific work site or visit the SECON website for additional SECON access requirements.

- Keep safety in mind when approaching a VAP. Stop at the VAP and follow the directions of Protective Force officers before proceeding.
- Pay attention to the traffic control signs and watch for pedestrians or other personnel in the area. Each VAP has at least one standard traffic stop sign that is visible to oncoming traffic.

Computer Security

Be sure to ask your host about LANL's cyber security rules that pertain to your work. You must adhere to them.

Visitor Network

The LANL Visitor Network provides short-term LANL visitors with external Internet access. User access of the network must be on LANL property, including leased facilities, using either a LANL- or user-provided computer.

User Access Requirements

"LANL Visitor Network User Authorization Form," Form 1861, must be completed for each visitor using the LANL Visitor Network. All network users must agree to the LANL Visitor Network Rules of Use, as stated on Page 2 of Form 1861. All non-Laboratory-owned computers on the visitor network must be approved and documented on Form 1861.

Information Security

Classified Matter

For cleared visitors, access to information depends on the nature of his or her work. The visitor's host must ensure the visitor knows how to handle information to which the visitor has access.

Official Use Only (OUO)

OUO information 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.

Access to OUO information is allowed only on a need-to-know basis. The person who has authorized possession, knowledge, or control of the OUO information must determine the recipient's need-to-know in order to perform DOE-authorized activities.

Unclassified Controlled Nuclear Information (UCNI)

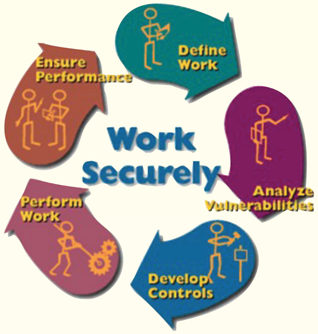
UCNI is certain unclassified but sensitive government information concerning nuclear material, weapons, components, and facilities that use such items and security relating to such facilities. Although no security clearance is required to access UCNI, access is permitted only to those authorized for routine or special access and those who have a need to know the specific UCNI to perform their official duties or DOE-authorized activities.

Integrated Safeguards and Security Management (ISSM)

ISSM requires that every worker at the Laboratory integrate safeguards and security into his or her work.

The ISSM Five-Step Process

1. Define the Scope of Work
2. Analyze the Security Risk
3. Develop and Implement Security Controls
4. Perform Work Within Security Controls
5. Ensure Performance



May 2007