LA-UR-20-25541
Approved for public release; distribution is unlimited.

Title: LANL Security Overview

Author(s): Scarlett, Harry Alan

Intended for: Nuclear Fundamentals Orientation (NFO)

Issued: 2021-10-21 (rev.1)

Disclaimer:
Los Alamos National Laboratory, an affirmative action/equal opportunity employer, is operated by Triad National Security, LLC for the National Nuclear Security Administration of U.S. Department of Energy under contract 89233218CNA000001. By approving this article, the publisher recognizes that the U.S. Government retains nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or to allow others to do so, for U.S. Government purposes. Los Alamos National Laboratory requests that the publisher identify this article as work performed under the auspices of the U.S. Department of Energy. Los Alamos National Laboratory strongly supports academic freedom and a researcher's right to publish; as an institution, however, the Laboratory does not endorse the viewpoint of a publication or guarantee its technical correctness.

Nuclear Fundamentals Orientation Module 1

LANL Security Overview

Los Alamos NATIONAL LABORATORY

Managed by Triad National Security, LLC for the U.S. Department of Energy's NNSA

LANL Security Overview

Presentation Overview:

- Personnel Security
- Substance Abuse Program
- Physical Security
- Prohibited and Controlled Articles
- Information Protection & Cyber Security
- Operations Security (OPSEC)
- Policies and Resources
- Questions and Answers

LANL Security Overview

The **Personnel Security Group** works to mitigate the risk individual workers pose by using a unique set of policies and procedures to:

- confirm identity and citizenship;
- issue security badges;
- process clearances;
- monitor human reliability for workers handling our nation's most sensitive nuclear materials.

LANL Security Overview

What would you do?

- You are going on travel for official business and the hotel asks to see your badge to verify that you work for the government so that you can take advantage of the government rate. Can you use your badge for identification?
- You are heading to a doctor's appointment mid-work day. What is the best way to secure your badge?
- What should you do if your badge is stolen?
- What is the Human Reliability Program (HRP) and how do you know if you need it?
- You are on vacation and get called on your LANL iPhone for a random drug test?

LANL Security Overview

Substance Abuse Program

- LANL does not tolerate illegal activity and must ensure a work environment that is free from unauthorized or illegal use, possession, or distribution of alcohol or controlled substances.
- Any use of an illegal drug, or use of a legal drug in a manner that deviates from approved medical direction is prohibited.
- DOE/NNSA may terminate or refuse to grant or renew a security clearance for a worker who is an unlawful user of a controlled substance or an addict.
- If a LANL badge holder fails to appear to a scheduled drug and/or alcohol test, the test will be treated as a confirmed positive.

LANL Security Overview

Marijuana and CBD

- Marijuana
  - Remains a controlled substance under federal law
  - Per LANL Procedure P732 *Substance Abuse*, marijuana is prohibited for use by LANL workers, even on an individual's private time or property

- CBD
  - The concentration of tetrahydrocannabinol (THC) in CBD products is not regulated in CBD products
  - Can potentially cause a failed drug test, which is a termination-level offense
  - Use of a product containing CBD is not a valid excuse for a failed drug test

LANL Security Overview

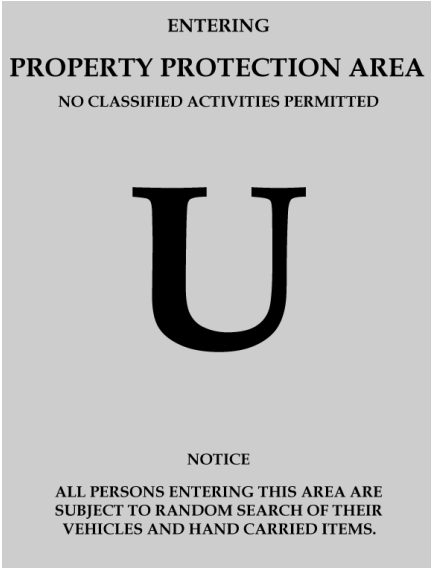
What would you do?

- You took a controlled substance (prescription) five hours ago. Can you report to work?
- Do you need to report any medications you are taking to Occupational Health?
- You have a migraine and your spouse has prescription migraine medication. Can you take one?
- You have used a controlled substance and want to self-report. Who do you talk to?

LANL Security Overview

Physical Security: Know the Different Types of Security Areas

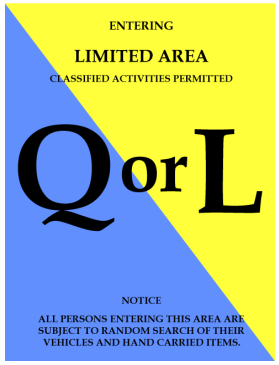
- **General Access Areas (GAAs)** are accessible to all workers and the public. Badges are not required for entry and are open to the public during normal business hours.
- **Property Protection Areas (PPAs**) are designed to protect security interests and government-owned property and equipment against damage, destruction or theft, and to control public access.

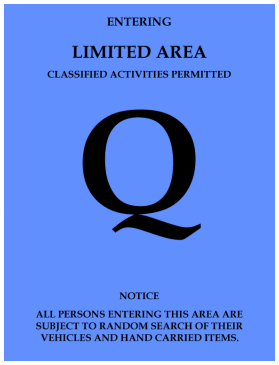


LANL Security Overview

Physical Security: Know the Different Types of Security Areas (cont.)

- **Limited Areas (LAs)** are security areas established for the protection of classified and/or Category III special nuclear material (SNM). Require L or Q clearances for unescorted access unless more stringent controls are implemented by the responsible line manager (RLM) or facility operations director (FOD).





- **Secure Spaces** are areas within LAs and above where classified computing is performed. These areas are posted as No Mobile Device Zones.

LANL Security Overview

Incidents of Security Concern

- **Incidents of security concern are actions, inactions, or events that:**
  - pose threats to national security interests and/or critical Department of Energy (DOE) assets;
  - create potentially serious or dangerous security situations;
  - degrade the effectiveness of the Security and Safeguards (S&S) program; or
  - adversely impact the ability of organizations to protect DOE S&S interests.

LANL Security Overview

Reporting Incidents of Security Concern

- **Workers must immediately report any known or potential incident of security concern to:**
  - the Security Incident Team (SIT) at 665-3505, or
  - a Deployed Security Officer (DSO)/Security Program Leader (SPL), and
  - their Responsible Line Manager (RLM)
- **Use caution when reporting information about known or potential security vulnerabilities may be sensitive or classified**
  - workers must ensure that sensitive and classified information is properly protected from unauthorized disclosure
  - don’t report security concerns in e-mail or by leaving voicemail messages detailing the concern
  - when in doubt, request to speak with your DSO or SIT inquiry official in person

LANL Security Overview

Escorting Tips

- **Plan ahead: escorts must**
  - determine the need for the escorted activity;
  - be eligible to escort (take the Escort Training and be cleared for the area to be visited);
  - coordinate with workers in the site to be visited; and
  - know site-specific requirements.
- **Before escorting: escorts must**
  - acquire the necessary badge for the visitor, if applicable (e.g., visitor badge);
  - not allow the visitor access into a Limited Area if they have an uncleared “no escort” badge
  - brief the visitor about prohibited and controlled articles, security, safety, emergency; procedures, and other site-specific requirements.

LANL Security Overview

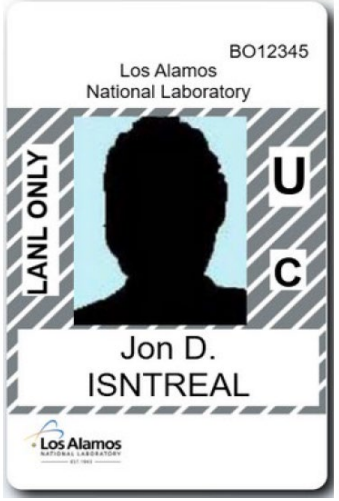
Escorting Tips

- **During escorting: escorts must**
  - not exceed the escorting ratio of five visitors per escort;
  - ensure visitor is wearing the appropriate badge visibly;
  - maintain visual and aural control of the visitor;
  - protect classified and sensitive unclassified material; and
  - hand off the visitor to a qualified escort, if needed.
- **After escorting: escorts must**
  - Retrieve and return visitor badges;
  - Comply with any site-specific requirements exiting the area; and
  - Hand off the visitor to a qualified escort, if needed.

LANL Security Overview

No Escort Badges

- **Badges issued to workers NOT allowed escorted access into Limited Areas and above**
  - Provides a visual alert for those performing escorting responsibilities
- **Look very similar to the standard LANL-issued uncleared badge**
  - Contain an additional notice and symbol at the bottom of the badge



LANL Security Overview

LANL Security Incidents

- What types of incidents do you think are the most common for workers at LANL?
- How would you know if you are entering location that has been designated as a “Secure Space”?
- You accidentally enter a “Secure Space” with a LANL-owned cell phone. What would you do as soon as you realize your mistake?

LANL Security Overview

Controlled Articles

- Any devices that are easily portable and can store, read, write, record and/or transmit information are considered controlled articles.
- Bluetooth and Wi-Fi devices are only allowed in GAAs PPAs. They are prohibited in Limited Areas and above.
- Photographic activity is prohibited.

LANL Security Overview

Prohibited Articles

The following prohibited articles **MUST NOT** be brought onto Lab property:

- Firearms, dangerous weapons and explosives (including knives with blades larger than 2.5 inches)
- Alcoholic beverages
- Controlled substances (i.e. illegal drugs and associated paraphernalia, but not prescription medication)
- Pepper spray/mace *(permitted in GAAs, PPAs and LAs, but **NOT** allowed in either the TA-55 Protected Area or the TA-55 Material Access Area)
- Privately owned unmanned aerial vehicles, drones, unmanned aircraft systems, and remotely piloted aircrafts
- Items prohibited by law

LANL Security Overview

What would you do?

- You have prescription medication in its original bottle in your car, can it be brought on LANL property?
- Can a cake/kitchen knife be used on LANL property?
- You have Bluetooth in your car – does it need to be turned off/disabled on Lab property?
- You just updated the software on your Lab iPhone. It reset the Bluetooth and wireless settings automatically without your knowledge and you brought the phone into a limited area (LA). Do you need to report this?
- You are under escort in an LA and discover that you have your personal phone in your pocket. What do you do?
- You are going on a camping trip after work and you want to pack everything you need in your vehicle. Can you bring your rifle and wine on Lab property?
- You saw someone taking a picture at the study center. What do you do?

LANL Security Overview

What would you do?

- You are an uncleared worker and have a meeting in an LA, can you be escorted?
- You are being escorted and need to visit the restroom. Do you need an escort with you at all times?
- You are being escorted into an area. Do you need to swipe your badge?
- Your colleague left his/her badge in their PIV reader and cannot get back into the building. Can you bring him/her in so they can retrieve it?
- Your colleague keeps getting denied at the badge reader. You know they were able to get in this morning. Can you let them follow you in to your shared office?
- During your lunch you come across a backpack in the lobby of the NSSB that doesn’t appear to have a tag on it. What do you do?

LANL Security Overview

Information Protection and Cyber Security

All Laboratory General Users are required to actively comply with all information security policies and procedures set forth by DOE and the Laboratory. When you use a Laboratory system, you agree to the terms and conditions of use.

- Using government computing systems for official work, except in emergencies threatening loss of life or government personal property, or for incident use (as specified in P821);
- Protecting systems from unauthorized access (e.g. locking your computing system when not in use; following the Laboratory's password policy);
- Install only information-architecture-approved hardware and software.

LANL Security Overview

Information Protection and Cyber Security

- Be aware of the threats to information security (e.g. phishing).
- Do not download attachments or click on links in suspicious
- Do not insert nongovernment USB devices into government systems.
- Promptly report any suspected information security incidents to the Security Incident Team (SIT), Deployed Security Officer RLM.

LANL Security Overview

Unclassified WebEx Meetings – Standard WebEx Version

- LANL's **Standard** WebEx Enterprise license is authorized for sharing the following types of unclassified information

  (ref: Standard WebEx Rules of Use; Collaboration & Teleworking Tools webpage):

  – Official Use Only (OUO) *

  – Export Control Information (ITAR, EAR, NAP-476.1 [previously NAP-23]) *

  – Triad Proprietary Information (TPI) *

  – Open/Unrestricted unclassified information (LA-UR, DUSA, etc.)

- Certain categories of Controlled Unclassified Information (CUI) may have additional regulatory restrictions and users are required to comply with those restrictions

- LANL's **Standard** WebEx version may **not** be used to store, process or display Unclassified Controlled Nuclear Information (UCNI)

* Need-to-know applies to **all** categories of information

LANL Security Overview

Unclassified WebEx Meetings – FedRAMP Version

- LANL's **FedRAMP** WebEx Enterprise license is approved for sharing Unclassified Controlled Nuclear information (UCNI), as well as CUI and TPI
- FedRAMP WebEx provides for Point to Point encrypted conferencing
- Participants cannot dial a phone number to connect to a conference

* Any export of information determined to contain UCNI to a foreign national must be approved by the appropriate DOE Program Office via the foreign national's approved FVTS record

LANL Security Overview

Unclassified WebEx Meetings – Know Which Version Is Being Used

- LANL's **Standard** WebEx meeting invitations will begin with **lanl-us.webex.com**
- LANL's **FedRAMP** WebEx meeting invitations will begin with **lanl-nm.webex.com**

LANL Security Overview

Teleworking

- Cyber requirements for Teleworking can be found on the LANL Telework Hub (https://int.lanl.gov/computing/network-connectivity/remote-access/telework-hub.shtml), and includes guidance on:
  - Use of personal computers
  - Collaborating
  - PIV, zToken and CRYPTOCards
  - Information protection
  - Encryption
  - Mobile Devices
  - Training

LANL Security Overview

What would you do?

- Your son's iPad's battery is low, he asks to log onto your work iPad. Can you share your password with him and allow him to use it?
- You were at a conference last week and were given a thumb drive by a vendor who your group would like to do business with. Can you insert it into your LANL computer to see what is on it?
- You are on your lunch hour and need to look up the number for your doctor's office. Can you use your LANL computer?
- When should you shut and lock you office door/computer screen?
- You accidentally clicked on a link that seems to be a phishing attempt. What do you do?
- You would like to charge your personally owned cell phone from a LANL-owned laptop or docking station. Is that permissible?

LANL Security Overview

Operational Security (OPSEC)

OPSEC assists workers in identifying and protecting unclassified information that could be useful to the Laboratory's adversaries. Knowing what to protect and how to protect it are key.

- Know what Critical Information (CI) your organizations deal with. CI is information that if lost or disclosed, would help the adversary and damage the Laboratory.
- CI Examples:
  - Utility, service, maintenance and construction
  - Planning, budget, logistics and procurement
  - Mission-critical projects and capabilities;
  - Safety, security and emergency response
  - Personnel issues

LANL Security Overview

Operational Security (OPSEC)

- Adversaries are smart, patient and persistent.
- Adversaries look for information on the web, social media, trash and recycle bins, and by observing patterns and deviations.
- To safeguard CI workers should ask themselves:
  - What is the easiest way an adversary can get this CI?
  - Do policies or procedures expose CI?
  - Has anything been posted on the web that gives clues to an adversary?

LANL Security Overview

Operational Security (OPSEC)

Workers can do the following to protect CI:

- Be OPSEC aware at work, on travel and at home
- Shred information instead of placing it in a
- Keep LANL information off of social media and pe
- All LANL information must be reviewed before it is made public!

For more information on OPSEC go to

http://int.lanl.gov/news/news_stories/2019/august/0812-operations-security.shtml

LANL Security Overview

What would you do?

- You attend a professional meeting and someone is asking you a lot of questions about your job at the Laboratory. What do you share?
- You are finishing up a draft of an OUO document and need to dispose of the previous versions. What are appropriate disposal methods?
- Someone posts an article regarding nuclear waste handling activities at the Laboratory. How do you respond to the post?

LANL Security Overview

Safeguards and Security Policies

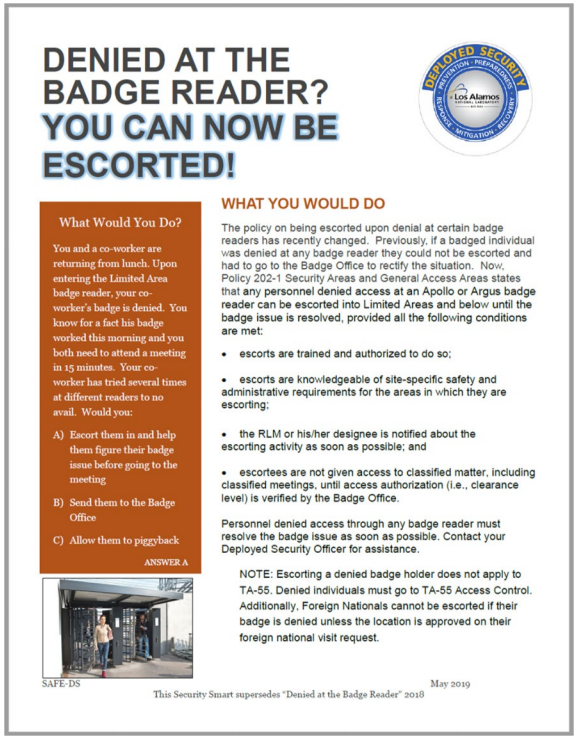
- **SD 200** *Integrated Safeguards and Security Management*
- **P 201-1** *Minor Visitors on LANL Property*
- **P 201-3** *Reporting Known and Potential Incidents of Security Concern*
- **P 201-4** *Public Demonstrations*
- **P 202-1** *Security Areas and General Access Areas*
- **P 202-2** *Vaults and Vault-Type Rooms*
- **P 202 4** *Security Locks and Keys*
- **P 202-5** *Prohibited Articles*
- **P 202 6** *Security Escorting*
- **P 202-7** *Security Conditions*
- **P 203-1** *Security Badges*
- **P 203-2** *Access Authorizations*
- **P 203-3** *Human Reliability Program*
- **P 203-4** *Counterintelligence Reporting Requirements*
- **P 203-5** *Incoming Classified Visits*
- **P 203-6** *Unclassified Foreign Visits and Assignments*
- **P 203-7** *Outgoing Classified Visits*
- **P 203-9** *Foreign Ownership, Control, or Influence (FOCI)*
- **P 204-1** *Controlled Unclassified Information*
- **P 204-2** *Classified Matter Protection and Control Handbook*
- **P 204-3** *Classification of Matter*
- **P 204-5** *Protection of Weapon Use Control Information (Sigma 14 & 15)*
- **PD 205** *Nuclear Material Control and Accountability*
- **P 213** *Cyber Security Wireless Computing Devices*
- **P 217** *Controlled Portable Electronic Devices*
- **P 218** *Cyber Security Controls*
- **P 223** *Open Desktop Collaboration: Video Teleconferencing*
- **P 225** *Protecting Electronic Controlled Unclassified Information (CUI)*
- **P 805 –** *Export Control*

Always make sure you are working to the latest versions of these policies.

LANL Security Overview

Safeguards and Security Resources

- Deployed Security Services (https://adss.lanl.gov/ds/Lists/DSOSPLContacts/AllItems.aspx)
- Security Help Desk 665-2002
- Security Incident Team (SIT) 665-3505
- Badge Office 667-6901
- Clearance Processing 667-7253



DENIED AT THE BADGE READER? YOU CAN NOW BE ESCORTED!

DEPLOYED SECURITY · PROTECTION · PREPARDNESS · RESPONSE · MITIGATION · RECOVERY · Los Alamos

What Would You Do?

You and a co-worker are returning from lunch. Upon entering the Limited Area badge reader, your co-worker's badge is denied. You know for a fact his badge worked this morning and you both need to attend a meeting in 15 minutes. Your co-worker has tried several times at different readers to no avail. Would you:

A) Escort them in and help them figure their badge issue before going to the meeting

B) Send them to the Badge Office

C) Allow them to piggyback

ANSWER A

WHAT YOU WOULD DO

The policy on being escorted upon denial at certain badge readers has recently changed. Previously, if a badged individual was denied at any badge reader they could not be escorted and had to go to the Badge Office to rectify the situation. Now, Policy 202-1 Security Areas and General Access Areas states that any personnel denied access at an Apollo or Argus badge reader can be escorted into Limited Areas and below until the badge issue is resolved, provided all the following conditions are met:

- escorts are trained and authorized to do so;
- escorts are knowledgeable of site-specific safety and administrative requirements for the areas in which they are escorting;
- the RLM or his/her designee is notified about the escorting activity as soon as possible; and
- escortees are not given access to classified matter, including classified meetings, until access authorization (i.e., clearance level) is verified by the Badge Office.

Personnel denied access through any badge reader must resolve the badge issue as soon as possible. Contact your Deployed Security Officer for assistance.

NOTE: Escorting a denied badge holder does not apply to TA-55. Denied individuals must go to TA-55 Access Control. Additionally, Foreign Nationals cannot be escorted if their badge is denied unless the location is approved on their foreign national visit request.

SAFE-DS

May 2019

This Security Smart supersedes "Denied at the Badge Reader" 2018

Thank you!

Questions?

Email us: **NFO@lanl.gov**