

Preparer Note (PN):

This document contains comments and instructions on clauses in **blue hidden text**. To view the **blue hidden text**, click on "Tools" on your tool bar above, then click on "Options", then click on the "View" tab, then check the box in front of "All" in the "Formatting marks" section, and lastly click OK to save the change. By clicking on the paragraph icon (¶) on your tool bar you can then view or hide the **blue hidden text** and other formatting marks. The hidden text will not affect the format of the document. Regardless of whether instructions are shown or hidden, **blue hidden text** will not show up on your printed document, unless you want it to; if so, go to "Tools", "Options", "Print", check the "Hidden text" box, then click OK.

Asterisks highlighted in yellow (i.e., *) have been used throughout this document as placeholders to indicate where information is to be inserted in clauses.

The proposed subcontract number (if known), and date the Exhibit was created shall be filled in where indicated, in the footer of Exhibit G.

Make sure to close all Preparer Notes, before sending this document to ASM.

PN: This Exhibit G is intended to be used when the Subcontractor's sole purpose for coming on-site is to attend meetings, presentations, making deliveries or provide training in certain low-risk areas. It shall be used in lieu of tailoring the Long-form version of Exhibit G Physical Security only if the Requester's Deployed Security Officer (DSO) or Security Program Lead (SPL) and Requester or STR/AdSTR determine that all requirements listed in Section 2.0 below apply to the SOW and no other security requirements are necessary. This version may also apply to work being performed entirely off-site if all conditions under 2.1-2.10 are met.

**EXHIBIT G PHYSICAL SECURITY LOW RISK
SECURITY REQUIREMENTS**

G1.0 Definitions and Acronyms (Jan 2020)

Definitions and acronyms may be accessed electronically at <http://www.lanl.gov/resources/assets/docs/Exhibit-G/exhibit-g-definitions-acronyms-green.pdf>

G2.0 Statements Applicable to Scope of Work (Jan 2020) PN: Every condition identified below must be applicable to the SOW in order to use this document. If even one condition is not met, then an Exhibit G long-form will need to be tailored for the purchase order / subcontract.

CONTRACTOR represents that all of the statements listed below are factually correct and applicable to the scope of work (SOW) for this subcontract. SUBCONTRACTOR has an affirmative duty to immediately notify the Contract Administrator in writing if performance of the SOW contradicts any statement in Section G2.0. In addition, if there is contradiction during the performance of the SOW, CONTRACTOR reserves the right to impose additional security requirements on SUBCONTRACTOR as deemed necessary and appropriate.

- 2.1 Work under this subcontract shall be limited to attending a meeting, presentation, training, making deliveries, or conducting equipment installation, repair or maintenance for a short period of time only, which will take place at a LANL location that is designated as a General Access Area, a Property Protection Area (PPA) or Limited Area (LA); **OR** work will be conducted entirely off-site and all conditions under 2.2 through 2.10 are met.
- 2.2 Access authorizations (clearances) are not required for Subcontract workers to perform work under the subcontract. Subcontract workers may already hold a DOE or LANL Cleared or Uncleared badge.
- 2.3 Work under this subcontract may require the development and approval of an OPSEC Plan.
- 2.4 Subcontract workers shall not require any LANL security training to perform work under the subcontract.
- 2.5 Subcontract workers shall include **US citizens ONLY**.

- 2.6 If a Subcontract worker does not hold a valid DOE badge, a LANL Generic Un-cleared U.S. Citizen Visitor's badge will be issued while in DOE / LANL owned or leased facilities, or on DOE / LANL property.
- 2.7 Access to LANL PII information or data shall not be allowed under this subcontract.
- 2.8 Access to OOU (excluding PII), CPI (CONTRACTOR Proprietary Information) and UCNI information or data shall be granted on a need-to-know basis only and shall be protected in accordance with U.S. Government policy.
- 2.9 Subcontract workers shall not have access to or process any LANL classified information or matter.
- 2.10 Subcontract workers shall not have access to Special Nuclear Material, Nuclear Material or Nuclear Material data.

G3.0 Security Requirements (Oct 2020)

SUBCONTRACTOR shall ensure compliance with all security requirements specified in this subcontract and all documents incorporated by reference. All measures taken by CONTRACTOR to correct Subcontract workers' non-compliance shall be at SUBCONTRACTOR'S expense and the cost thereof, including any stipulated penalties resulting from such non-compliance, shall be deducted from payments otherwise due SUBCONTRACTOR.

Work on this subcontract shall be subject to random periodic inspections and assessment by LANL Security personnel to verify compliance with the security requirements in this Exhibit G.

3.1 DOE Directives Incorporated By Reference

SUBCONTRACTOR shall provide such information, assistance and support as necessary to ensure CONTRACTOR'S compliance with the following DOE/NNSA Directives, as applicable. In addition, SUBCONTRACTOR shall comply with the requirements of the Contractor Requirement Document (CRD) attached to a Directive when required by such CRD. The Directives are prefaced with certain conditions for applicability to the subcontract. A referenced Directive does not become effective or operative under this subcontract unless and until the conditions precedent are met through the scope of work. The DOE Directives referenced herein may be found at <http://www.directives.doe.gov/>

Clause Number	Title	Instructions
DOE M 470.4B Chg 2 (MinChg)	Safeguards and Security Program	Applies when contract requires information regarding reporting potential security incidents.
DOE O 471.1B	Identification and Protection of Unclassified Controlled Nuclear Information	Applies if contract involves activities that may generate, possess or have access to information or matter containing UCNI.
DOE O 471.3, Admin Chg 1	Identifying Official Use Only Information	Applies if contract involves activities where Official Use Only (OOU) information and documents will be handled, used or generated.
DOE M 471.3-1, Admin Chg 1	Manual for Identifying and Protecting Official Use Only Information	Applies if contract involves activities where Official Use Only (OOU) information and documents will be handled, used or generated.
DOE O 471.6, Chg 3	Information Security	Applies if contract includes access to unclassified information and matter controlled by statutes, regulation or NNSA policies.
DOE O 473.3A, Chg 1 (MinChg)	Protection Program Operations	Applies if contract includes responsibilities for operating, administering, and/or protecting DOE & NNSA safeguards & security interests.
DOE O 475.1	Counterintelligence Program	Applies if contract work involves access to or use of DOE facilities, technology, personnel, unclassified sensitive information and classified matter.

3.2 Goal of Zero Security Incidents

SUBCONTRACTOR and any lower-tier subcontractors shall strive to eliminate all security events, incidents, and adverse impacts to national security.

G4.0 General Security (Oct 2020)

4.1 Work Location and Badge Information **PN: Check the appropriate box for location and type of badge required to perform the work; not the type of badge currently held by a Subcontract worker, since some workers may hold clearances even though the SOW doesn't require it.**

LOCATION	BADGE REQUIRED FOR THE WORK
<input type="checkbox"/> General Access Area	<input type="checkbox"/> No Badge Required
<input type="checkbox"/> Property Protection Area	<input type="checkbox"/> Generic Uncleared US Visitor
<input type="checkbox"/> Limited Area	<input type="checkbox"/> Generic Uncleared US Visitor Escort Required
	<input type="checkbox"/> LANL Uncleared Site-Specific Badge

4.2 Integrated Safeguards and Security Management (ISSM)

ISSM utilizes a five-step process that LANL incorporates to ensure that security expectations are established, implemented, measured and reinforced in every work activity. The following five-step process defines a systematic approach to actions taken before, during, and after work is performed. SUBCONTRACTOR shall ensure that the five-step ISSM process or an equivalent process is followed by all Subcontract Workers.

- (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

4.3 Counterintelligence Awareness

4.3.1 SUBCONTRACT Workers shall report all of the following situations to the LANL Office of Counterintelligence and inform the RLM or STR/AdSTR and CA/PS.

- Professional contacts and relationships with sensitive country foreign nationals, whether they occur at one's worksite or abroad.
- Suspicious or provocative actions or behaviors on the part of foreign nationals visiting or assigned to LANL.
- Substantive personal relationships with sensitive country foreign nationals (who are not lawful permanent residents), other than family members.
- Business transactions including financial transactions, partnerships, or other business interests or investments with citizens of sensitive countries who are not lawful permanent residents, whether they involve one-time interactions or ongoing financial relationships. (Small payments for things such as house cleaning or other such personal services or financial support provided to family members are not included).
- Any attempts by unauthorized persons to gain access to classified information. (Not limited to sensitive country foreign nationals or foreign nationals; includes US and non-US citizens)

4.3.2 SUBCONTRACTOR shall be alert to and report any of the following to the RLM and STR:

- attempts by unauthorized persons to obtain information;
- unexplained / excessive use of copiers by workers;

- workers living beyond their means;
- unreported contacts with foreign nationals;
- unauthorized downloads of information;
- attempts to encourage others to violate laws or security policies;
- unusual foreign travel patterns of workers; and
- personal problems of workers that could affect security or fitness for duty.

4.4 Security Stop Work

When a Subcontract worker observes a security related hazard or unmitigated risk, the worker has the authority and responsibility to inform any worker engaged in the work that the work should be stopped to address the hazard or risk.

4.5 Reporting Security Incidents

This subsection contains requirements for identifying and reporting known and/or potential incidents of security concern. Such incidents may involve issues associated with OOU, ECI, UCNI, secure communications, and personnel security occurring off-site or on-site; and physical security occurring on LANL property, DOE/LANL-leased property or SUBCONTRACTOR-owned property. Subcontract workers shall comply with the following requirements.

4.5.1 *Immediately* upon discovery of a potential incident of security concern, report such concern to the Security Inquiry Team (SIT) (505-665-3505) or a SPL / DSO; then inform the LANL RLM and STR/AdSTR. During normal business hours, notifications shall be made only in person or through secure communications (STU or STE). A non-secure telephone, non-secure fax, non-secure voice mail, or non-secure electronic mail shall not be used to report a potential incident of security concern.

4.5.2 Contact Requirements Outside of Normal Business Hours

For all incidents contact the Security on-call duty officer through the Protective Force at 505-665-7708, *immediately* after discovery of a potential incident of security concern. If secure communications are not available, the Security on-call duty officer may ask the SUBCONTRACTOR to meet in person so SUBCONTRACTOR can report known or potential incidents of security concern.

4.6 Workplace Violence

LANL maintains a work environment that is free from violent behavior and threats of violence. Violent behavior and threats of violence are unacceptable conduct and are prohibited. Any subcontract worker who participates in workplace violence will be barred from the LANL worksite and their employer shall be notified. Workplace violence is behavior that involves:

- hostile or aggressive physical contact with another person;
- a statement or body gesture that threatens harm to another person; or
- a course of conduct that would cause a reasonable person to believe that they are under threat of harm.

G5.0 Physical Security (Oct 2020)

5.1 Prohibited Articles

Prohibited Articles are items never permitted on DOE property (e.g. LANL) which includes leased facilities and parking lots. SUBCONTRACTOR shall ensure that prohibited articles are not brought on to DOE property. Introducing an unauthorized prohibited article onto DOE property is a reportable security incident that may result in legal action. Prohibited articles include:

- Dangerous weapons (e.g., guns and knives), explosives, or other instruments or

material likely to cause substantial injury or damage to persons or property; includes pocket, hunting or other sharp knives with blades longer than 2.5 inches;

- Non-government-owned firearms;
- Alcoholic beverages, including unopened bottles or cans;
- Controlled substances such as illegal drugs and associated paraphernalia, including medical & recreational marijuana – but not other prescription medicine;
- Pepper spray and/or mace;
- Privately owned Unmanned Aerial Vehicles (UAVs), drones, unmanned aircraft systems and remotely piloted aircrafts, etc; and
- Items prohibited by local, state or federal law;
- Other items that may pose a safety, security or environmental hazard; as determined by LANL security professionals.

5.2 Escorting

In addition to any facility-specific escorting requirements, SUBCONTRACT Workers shall ensure that all LANL escorting requirements listed below are complied with while on DOE/LANL property or LANL-leased property.

An Un-cleared US Citizen shall be authorized for escorted access into a Security Area (e.g. a Limited Area) only if such individual is entering an area to conduct official LANL business that can be accomplished only in that Security Area.

Subcontract Workers shall be escorted into a LANL area where they are not permitted unescorted access. A Subcontract worker shall not escort another Subcontract worker or an Un-cleared individual. The Subcontract worker shall:

- Provide a valid photo ID;
- State country of citizenship for their LANL escort before entering a security area;
- Log in, pursuant to the manner required by the LANL-owning / tenant organization before entering an area where he/she is being escorted;
- Wear their badge in plain sight at all times while on-site at LANL;
- Return the badge to the issuing LANL host when the escorted visit is over;
- Physically remain with his/her escort at all times;
- Comply with all requirements outlined by the LANL escort and host organization;
- No more than five (5) individuals shall be escorted at any one time.

5.3 Escorting Vehicles

When vehicles are escorted through manned security posts, the escort shall be in the same vehicle or a separate vehicle as the subcontract worker(s). The escort ratio for vehicles is 1:3 - one escort vehicle to three escorted vehicles.

5.4 Parking on LANL Premises

- Subcontract Workers shall park vehicles in designated parking areas only.
- Subcontract Workers shall obey all posted designations and park in a safe and courteous manner.
- Failure to park in designated areas and to obey posted signage shall result in a parking violation. Vehicles that are abandoned or present a safety or security concern are subject to removal at the owner's expense.

G6.0 Personnel Security (Jan 2020)

6.1 Substance Abuse Policy

- 6.1.1 The unauthorized use of alcohol and/or illegal drugs or being under the influence of alcohol and/or illegal drugs is prohibited on the LANL site. LANL's substance abuse policy applies to all who perform work at or for LANL; calls for drug and/or alcohol testing on the basis of reasonable suspicion that the policy has been violated; and drug and/or alcohol testing due to an incident or accident that results in a serious injury or has the potential to cause serious injury. All drug collections and alcohol testing are conducted in accordance with 49 CFR Part 40.
- 6.1.2 If a Subcontract worker is reasonably suspected of being impaired by either drugs or alcohol, CONTRACTOR will require Subcontract worker to submit to drug / alcohol testing. The testing will be conducted and paid for by the CONTRACTOR.
- 6.1.3 Drugs currently used in CONTRACTOR'S random testing panel include marijuana, cocaine, opiates, heroine, phencyclidine and amphetamines. The use of medical and recreational marijuana is illegal under federal law and therefore is prohibited in accordance with these substance abuse requirements. When conducting reasonable suspicion or occurrence testing, CONTRACTOR may test for any drug listed in Schedules I or II of the Controlled Substances Act.
- 6.1.4 SUBCONTRACTOR shall ensure that Subcontract workers comply with all requirements of LANL's Substance Abuse program. Failure to comply with requirements shall result in termination of a Subcontract Worker's permission to work on LANL property or on the subcontract.
- 6.1.5 Subcontract workers shall:
- Be fit for duty and avoid behavior that compromises the health or safety of others and/or the security of the Lab;
 - Notify Personnel Security, the RLM, STR/AdSTR and CA/PS immediately if cited, arrested or convicted of a drug or alcohol statute violation;
 - Notify Personnel Security, the RLM, STR/AdSTR and CA/PS immediately if they are cited, arrested or convicted of any alcohol-related incident such as (e.g.) DUI, DWI, or public intoxication, open container;
 - Meet with LANL Personnel Security or Occupational Medicine promptly when asked to perform a drug and/or alcohol test;
 - Immediately report accidental ingestion of illegal drugs to LANL Personnel Security, the RLM, and the STR/AdSTR so the appropriate action can be taken.
- 6.1.6 Other testing shall be required if
- An incident or accident occurs at work that results in a serious injury or had the potential for serious injury.
 - A vehicle accident that results in or had the potential for injury while driving any government-owned vehicle on or off DOE/LANL property; or while driving any private vehicle within the boundaries of a LANL Technical Area.
- 6.1.7 Failure to Show or Refusal of Drug and/or Alcohol Test
- If a Subcontract worker fails to show up or refuses to be tested, such failure or refusal shall be reported and treated as a confirmed positive.
 - Failure to cooperate and submit to a drug/alcohol test shall be grounds for the CONTRACTOR to bar the Subcontract worker from the LANL site.
- 6.1.8 Confirmed Positive Drug and/or Alcohol Test
- The RLM or STR/AdSTR shall take the following actions if a Subcontract Worker has a confirmed positive drug test:
- Immediately stop the worker from performing any additional work;
 - Immediately notify Subcontract worker's management that the worker's badge is being pulled;
 - Ask the worker to report back to his/her employer because his/her assignment is being terminated;

- Confiscate the worker's badge;
- Consult with LANL OM-MS to determine whether the worker should have a medical evaluation prior to driving;
- Coordinate with the CA/PS to ensure proper notifications are made regarding test results and any changes to the subcontract worker's assignment.

6.1.9 Off-site Behavior

The unlawful manufacture, distribution, dispensing, possession, use, transfer or sale of controlled substances is prohibited regardless of whether this occurs at the workplace, while performing Laboratory business, or during an individual's private time or property. These and other violations of this substance abuse policy are considered connected to work with or at LANL and may result in the termination of a Subcontract worker's permission to work on DOE / LANL property or on the subcontract, regardless of whether or not the misconduct occurs during work hours or on Laboratory premises.

6.2 Badges

SUBCONTRACTOR shall ensure compliance with the badge requirements outlined in the following subsections. Any individual performing work under a contractual agreement with LANL, shall obtain a LANL badge. (E.g. Subcontract workers, Guests and Affiliates)

All badges issued by the LANL Badge Office, including a Generic Un-cleared US Citizen Visitor badge supplied by a LANL host, are accountable. Therefore, SUBCONTRACTOR shall ensure that every badge issued under this subcontract is returned to the issuing LANL Host. Failure to return any badge will result in denial of future badging services to the subcontract worker.

6.2.1 General Badging Requirements

- A Subcontract worker who will be issued a Generic Un-cleared US Citizen Visitor's badge shall provide Real ID-approved proof of U.S. citizenship to the LANL host issuing the badge.
- Proof of citizenship includes a declaration of US Citizenship with presentation of an original photo identification card (such as a current and valid state driver's license) and/or by signing a Generic Visitor / Escort Required Badge Log declaring US citizenship.
- Individuals who falsely certify their citizenship will be removed from the Laboratory and shall be denied future access to LANL. This will be reported to the appropriate LANL organizations for investigation and other external organizations as necessary.

6.2.2 Obtaining a Generic US Citizen Visitor's Badge

- Subcontract worker shall present identification as required by the LANL host;
- Subcontract worker, in conjunction with his or her Laboratory host, shall be issued a Generic Uncleared US Citizen Visitor's Badge before performing any work on-site at LANL;
- Uncleared US Citizens shall be required to sign a "*Statement of U.S. Citizenship*" provided by the LANL host affirming their U.S. citizenship;
- Uncleared US Citizens who are on site six (6) consecutive months or less, shall attend a briefing designed by their Laboratory Host and RLM, covering safety and security requirements relevant to the work they will be performing;

6.2.3 Subcontract workers shall:

- Wear the badge, photo-side out, above the waist, on the front side of the body, at all times while on DOE-owned property (LANL) or on CONTRACTOR leased or rented premises;
- Remove the badge and protect it from public view when leaving DOE-owned

property or CONTRACTOR leased or rented premises;

- Present the badge whenever requested by Protective Force personnel, the LANL host, or LANL Personnel Security Group.

6.2.4 Badge Expiration Dates

A LANL Generic Uncleared US Citizen Visitor badge shall be issued to each SUBCONTRACT worker on the day the worker is actually on-site; the badge shall be collected by the LANL host at the end of each daily visit to DOE/LANL property or facilities or LANL leased facilities.

6.2.5 Lost or Stolen Badge(s)

- Lost or stolen badges shall be reported to the issuing LANL host within 24 hours or the next business day after discovery of the loss, whichever is soonest. The RLM or STR/AdSTR shall also be notified.
- In addition to the above, if a badge is stolen, the individual badge holder shall report the theft to the LANL Security Inquiry Team (SIT), the LANL Badge Office and inform the STR/AdSTR or CA/PS by the next business day of discovery of the loss.

G7.0 Information Security (Oct 2020)

7.1 Official Use Only (OUO) and TRIAD Proprietary Information (TPI)

OUO and TPI information is unclassified with the potential to damage government, commercial or private interests if disseminated to persons who do not have a need-to-know the information to perform their jobs or other DOE-authorized activities. SUBCONTRACTOR shall protect such information from unauthorized dissemination and shall follow all requirements for OUO and TPI documents specified below.

7.1.1 Access

No security clearance is required for access to OUO or TPI.

If OUO information is Export Control Information (ECI), access is restricted to US persons, defined as citizens and Lawful Permanent Residents. Access to ECI (including parts, tools, material and equipment fabricated from ECI specifications and drawings) by non-Permanent Resident Alien foreign nationals is prohibited.

If OUO information is Applied Technology (AT) it is subject to access restrictions established by the DOE Program Office. The associated LANL program manager can determine access authorizations for Laboratory workers.

7.1.2 Storing

OUO and CPI information shall be stored in a locked room or locked receptacle (e.g. desk, file cabinet, safe). OUO and TPI information stored on a computer shall have passwords, authentication, encryption or file access controls in place to protect the files from unauthorized access.

7.1.3 Reproduction / Printing

All copies of LANL OUO and TPI (including 3-D print prototypes) shall be protected, accessed, stored, marked, transmitted and destroyed in the same manner as the originals.

OUO and TPI shall be reproduced to the minimum extent possible.

7.1.4 Transmitting

E-mail messages that contain OUO or TPI information should indicate OUO or TPI in the first line, before the body of the text. OUO or TPI disseminated over networks outside of LANL should be encrypted with NIST-validated encryption software (e.g., Entrust®).

Hard copies of OUO or TPI sent outside of LANL, shall be placed in a sealed, opaque envelope marked with the recipient's name, a return address and the

words "To Be Opened by Addressee Only". For interoffice mail within LANL, OOU or TPI shall be placed in a sealed, opaque envelope with the recipient's address and the words "To be Opened by Addressee Only" on the front of the envelope.

7.1.5 Destroying

Users are not required to destroy electronic media that contains OOU or TPI. However, disks should be overwritten using approved software before the discs are thrown away. Hard copy OOU or TPI documentation shall be destroyed by using an approved shredder (strips no more than ¼ inch wide).

7.1.6 Export Controlled Information Restrictions

If the work to be performed under this subcontract includes LANL technical data; the export of which is restricted by the Arms Export Control Act (22 U.S.C. §2751, et seq.), the Atomic Energy Act of 1954, as amended (42 U.S.C. §2011) or the Export Administration Act of 1979, as amended (50 U.S.C. §2401, et seq.), the data shall be protected as required under these laws. Violations of these laws may result in severe administrative, civil, or criminal penalties. Dissemination must be pre-approved by Los Alamos National Laboratory. The LANL STR/Ad/STR shall provide guidance on marking ECI documents and material.

7.2 Unclassified Controlled Nuclear Information (UCNI)

UCNI is unclassified but sensitive government information whereby unauthorized dissemination is prohibited. UCNI is intended to be viewed only by those individuals with a need-to-know the UCNI to perform their official duties or DOE-authorized activities under this subcontract. SUBCONTRACTOR shall protect such information from unauthorized dissemination and shall follow all requirements for UCNI documents specified below. Subcontract workers with routine access to UCNI shall be briefed periodically on their responsibilities for protecting UCNI.

7.2.1 Access

No security clearance is required for access to UCNI; however, access is permitted to only individuals authorized for routine or special access and who have a need-to-know. UCNI stored on a computer shall be restricted with passwords, authentication, file access control encryption and offline storage, to only individuals who have a need-to-know.

7.2.2 Storing

While using UCNI, physical control shall be maintained over the material to prevent unauthorized access to the information. When not in use, UCNI matter shall be stored in a locked room or receptacle (e.g. desk, file cabinet, bookcase or safe). The locked receptacle shall have controls that limit access to only approved workers. UCNI stored on a computer shall have passwords, authentication, encryption or file access controls in place for protection.

7.2.3 Reproduction / Printing

Reproduced copies of documents or media that contain UCNI (including 3-D print prototypes) must be protected, accessed, stored, marked, transmitted and destroyed in the same manner as required for the originals. Copies shall be kept to the minimum required.

7.2.4 Transmitting

UCNI must be marked correctly prior to transmitting over any media. Only a qualified LANL UCNI Reviewing Official is authorized to identify and mark UCNI. Contact the LANL Classification Group through the RLM or STR/AdSTR for assistance.

When transmitting over telecommunication circuits (including telephone, fax, radio, e-mail or Internet) encryption algorithms that comply with all applicable Federal laws, regulations and standards for the protection of UCNI shall be used.

Transmission over open phone lines is prohibited. A Secure Terminal Equipment

(STE) line is required. All cellular devices, including LANL-issued smart phones such as Blackberries must be turned off completely when in proximity to UCNI discussions.

UCNI documents must be transmitted using a fax machine that employs encryption. When transmitted outside LANL, UCNI shall be encrypted with NIST-validated encryption software. E-mails with UCNI attachments are considered transmittal documents and shall be marked as such.

When mailing outside of LANL, an opaque envelope shall be used and the outer packaging shall not indicate that the content within is UCNI. For interoffice mail, an interoffice envelope shall be used and mailed through standard interoffice mail, but do not indicate that the content is UCNI. When using e-mail, UCNI shall be encrypted with NIST-validated encryption software such as Entrust®.

7.2.5 Destroying

Users are not required to destroy electronic media that contain UCNI. Disks shall be overwritten using approved software before they are discarded. Hard copy UCNI documents are to be destroyed by shredding in an approved shredder.

SUBCONTRACTOR shall coordinate with a LANL Reviewing Official (through the RLM or STR/AdSTR) after destruction to verify that all UCNI has been removed prior to disposing of the material.

7.2.6 Noncompliance Consequences

SUBCONTRACTOR'S failure to comply with the requirements pertaining to UCNI may result in the imposition of a civil and/or criminal penalty for each violation.

G8.0 Controlled Portable Electronic Devices / Wireless Technology (Oct 2020)

LANL's level of control for wireless computing devices and other controlled articles depends on the type of device, who owns it, where it will be located and how it will be used.

8.1 Controlled Portable Electronic Devices (PEDs)

Controlled PEDs are easily portable, stand-alone devices that can store, read, write, record or transmit data. Certain controlled articles can read and/or write nonvolatile information and plug into a computer. They are not considered stand-alone devices like other types of controlled articles.

Controlled PEDs do not require approval for use in General Access Areas (GAAs) and Property Protection Areas (PPAs). Connection to the LANL Visitor Network does not require prior approval.

Controlled PEDs are not permitted in Secure Spaces. SUBCONTRACTOR shall ensure that controlled articles are not brought into a Secure Space. Additional LANL site-specific requirements may exist and shall be followed as appropriate.

Controlled PEDs include:

- Cell phones, smart phones, cordless phones, Blackberry devices, two-way pagers, two-way radios;
 - ✓ *Instant Messaging, including text messages shall not be used for discussion of, or creation of records for official LANL business.*
- Smart watches, fitness trackers with Bluetooth, USB or other connect/transmit capabilities;
- Recording equipment (audio, video, optical, or data);
- Copiers or scanners with hard drives;
- Radio frequency (RF) transmitting equipment (including ankle monitoring devices), Infrared (IR), computers or peripherals with active Bluetooth, or other wireless transmission capabilities, unless disabled;
- Electronic equipment with a data exchange port capable of being connected to automatic information system equipment;

- Portable computers including but not limited to: laptops, tablet computers, personal digital assistant (PDAs), palm-top computers, Blackberry devices, Notebooks, iPhones or iPads and watches;
 - Portable electronic reading, web-browsing and data collection devices with WiFi or USB connectivity, including but not limited to: Kindles, iPads, Nextbook Tablets, Nook eReaders, Sony Digital Readers, or iPods;
 - Any device with a capability to connect to computers or use wireless communications;
 - Cameras - video, still, digital, film or in cell phones. If the use of cameras - either inside or outside of a security area is deemed mission essential - then use of cameras shall be authorized via coordination with the STR/AdSTR, the RLM and the LANL Physical Security Team prior to the use of such cameras. (*Form 1897PA*). A Subcontract worker using a non-government owned camera on Laboratory property shall possess a valid DOE/LANL badge.
 - CD / DVD write drives
 - External hard drives
 - Flash memory (i.e. PC cards, SD memory cards)
 - USB memory devices (i.e. thumb drives, memory sticks, jump drives)
- 8.2 Approvals Required Before Commencement of Work
- 8.2.1 Prior to connecting to a LANL-owned system (other than the Visitor Network), approval shall be obtained from the LANL Cyber Information Security Office. The RLM or STR/AdSTR shall also be informed.
- 8.2.2 Subcontractors using wireless technology in locations that are not designated as a GAA or a PPA, are required to obtain certification and approval from the LANL Cyber Information Security Office prior to engaging the wireless technology.
- Violations of this requirement may constitute a security infraction and may result in administrative actions up to and including exclusion of a Subcontract worker from LANL and/or from working on this subcontract.
- 8.3 Rules for Using Authorized Controlled PEDs in Security Areas
- Authorized controlled articles with audio recording or data transmitting capabilities in a LANL Limited Area shall be turned off (for UCNI) or placed in an approved Radio Frequency container whenever:
- An UCNI discussion or phone call is taking place within audible range;
 - UCNI computer processing is taking place in the immediate area of the device;
 - UCNI faxing is taking place within the immediate area of the device; and
 - UCNI copying is taking place on a digital copier in the immediate area of the device.
- 8.4 Wireless Device Requirements
- 8.4.1 The use of wireless computing and printing devices such as “Bluetooth” technology or wireless networking protocol in locations other than a GAA or PPA is prohibited at LANL, including all LANL property and leased space. Wireless devices cannot be connected to LANL computing assets or networks except for the Visitor’s Network. Such capabilities shall be disabled unless the activity has been approved by the LANL Cyber Security Office. It is the user’s responsibility to know what devices they possess, the capabilities of those devices and to ensure that wireless capabilities have been disabled.
- 8.4.2 The use of wireless networking, Bluetooth and cell phone technologies is allowed in LANL GAAs and PPAs, public areas of the Bradbury Science Museum, the Otowi Cafeteria and public access areas outside buildings such as roadways, sidewalks and parking lots.

- 8.4.3 The use of wireless networking is not restricted in non-LANL occupied areas of LANL-leased properties such as Canyon Complex, White Rock Training Center, the Research Park and Central Park Square.
- 8.4.4 These wireless device requirements do not apply to the wireless computing capability used by Subcontractor delivery and shipping workers in the LANL receiving area outside of a building.
- 8.5 LANL and Other Government-owned Wireless Devices
 - 8.5.1 LANL and government-owned cell or satellite phones are not allowed in Secure Areas or higher Security areas.
 - 8.5.2 LANL and government-owned cellular devices including smart phones such as Blackberries shall be turned off completely when in proximity to UCNI discussions.
 - 8.5.3 LANL-issued Blackberry devices, applications and accessories are not allowed in LANL locations designated as a Secure Space.
 - 8.5.4 Government-owned computing controlled articles (e.g. laptops, palmtop computers and PDAs) shall follow access control requirements such as username and password.
 - 8.5.5 Government-owned computing controlled articles shall use anti-virus software to detect malicious activity where the capability exists.
 - 8.5.6 Government-owned unclassified controlled articles are not permitted to connect to any LANL computer or network or store LANL sensitive data without approval from LANL management.
- 8.6 Privately-owned Owned Controlled PEDs
 - 8.6.1 Privately-owned Controlled PEDs are prohibited in Secure Spaces.
 - 8.6.2 Privately-owned Controlled PEDs may not be connected to any LANL-owned information system or network without written approval; and may not be used to store or process any government controlled unclassified information unless formal approval has been granted and full disc encryption is utilized. (*Form 1897*)
 - 8.6.3 Privately-owned cellular devices, including smart phones such as Blackberries shall be turned off completely when in proximity to UCNI discussions.
 - 8.6.4 When privately-owned vehicles are allowed to enter a LANL Secure Space, controlled articles that are attached to the vehicle (i.e. built-in cell phones, On Star and CD radios) shall be turned off if capable and left in the vehicle. Additional restrictions may apply in some areas and Subcontract workers shall follow local controls.
- 8.7 Privately-owned Wireless Computing Devices
 - 8.7.1 LANL Cyber Information Security Office approval is required if computing devices will be in a LANL Limited Area. (*Form 1897*)
 - 8.7.2 LANL management approval is required before connecting a non-government computing device to a LANL network. (*Form 1897*)
 - 8.7.3 Privately-owned owned wireless computing devices must be authorized before connecting to any LANL wireless computing resource.
- 8.8 Connecting to Presentation Systems and Using Equipment Remote Controls
 - 8.8.1 Privately-owned Controlled PEDs may be connected to stand-alone presentation equipment and stand-alone systems in PPAs provided:
 - 1) The information system has virus detection software active, automatically scanning for malicious code and using the most current definition file and,
 - 2) The information system shall not contain any sensitive information that the controlled article owner does not have authorization to access.
 - 8.8.2 RF and Infrared (IR) remote controls on unclassified presentation equipment (audio, video, etc.) in unclassified workspace are allowed.
 - 8.8.3 IR and RF remote controls are permitted to control projectors.

