Subcontract workers who will obtain a standard (non-Visitor) badge such as a DOE Q, L, Un-cleared; Un-cleared Site-specific LANL; or Cleared/Un-cleared Foreign National badge, shall successfully pass a drug test no more than 60 days before obtaining a standard (non-Visitor) badge.

Subcontract workers who currently hold a standard badge but have not completed a pre-badge drug test, are required to complete the pre-badge drug test prior to working on a LANL subcontract for the first time.

Subcontract workers who currently hold a standard badge and transfer from one LANL subcontract to another without a break in service between subcontracts, are not required to complete a second pre-badge drug test.

Subcontract workers who hold a standard badge and experience a break in service for five (5) or more business days between LANL subcontracts are required to successfully pass a drug test no more than 60 days before re-obtaining a standard badge.

Subcontract workers shall not begin work on this subcontract until a pre-badge drug test is completed and passed, if applicable. The testing will be coordinated and paid for by SUBCONTRACTOR.

A drug testing laboratory used for any LANL required drug test shall be certified by the Department of Health and Human Services under the National Laboratory Certification Program. A current list of approved drug testing laboratories is published in the Federal Register which can be found at: https://www.samhsa.gov/workplace/resources/drug-testing/certified-lab-list

SUBCONTRACTOR shall provide records of pre-badging drug screening to CONTRACTOR upon request.

5.1.3 Random Drug Testing

All Subcontract workers who are issued standard non-Visitor badges from the LANL Badge Office, which include Q, L or Un-cleared badges, are subject to random drug testing while on the LANL site.

Subcontract workers who are subject to random drug testing under another government testing program will not be included in LANL's random testing pool.

5.1.4 Reasonable Suspicion Drug and/or Alcohol Testing

5.1.4.1 When conducting reasonable suspicion testing, CONTRACTOR may test for any drug.

5.1.4.2 Drug and/or Alcohol testing will be required if:

- A Subcontract worker is reasonably suspected of being impaired by either drugs or alcohol.
- LANL Personnel Security, LANL Occupational Medicine or LANL manager or supervisor determines that there is reasonable suspicion that the subcontract worker may have violated this procedure.
- The subcontract worker is the subject of a drug-detection dog alert and/or possesses property that has caused a drug-detection dog alert.
- A LANL manager or supervisor observes worker behavior commonly associated with alcohol or substance abuse such as unexplained chronic tiredness, tardiness, absence patterns, odor of alcohol, slurred speech, unsteady gait, etc. The manager or supervisor shall discuss the observed behavior with the worker as appropriate and make a referral to LANL Occupational Medicine for an evaluation of the worker.

5.1.4.3 Drug and/or alcohol testing may be required if:

- An incident or accident results in a serious injury or had the potential for serious injury occurs at work.
- LANL Occupational Medicine determines that unannounced, periodic testing is medically appropriate as indicated within the context of *Fitness for Duty* or *Human Reliability Program* monitoring.

- It is related to security clearances or applications for security clearances.
- When conducting occurrence testing, CONTRACTOR may test for any drug.

5.1.5 Other Testing

Drug and/or alcohol testing shall be required if:

- A non-vehicular 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 (including motorized equipment) on or off Laboratory property; or while driving any private vehicle (including rental vehicles) within the boundaries of a Laboratory Technical Area (other than downtown Los Alamos). [Note: LANL Personnel Security will determine whether to require testing under these circumstances]
- It is necessary when related to security clearances or applications for security clearances.

5.1.6 Testing Conduct

CONTRACTOR'S Personnel Security organization has oversight of all drug and alcohol testing on-site at LANL for random, reasonable suspicion and other testing. All drug collections and alcohol testing are conducted in accordance with 49 CFR Part 40 and 10 CFR Part 707. All testing (except pre-badge drug testing) will be conducted and paid for by the CONTRACTOR.

5.1.7 Confirmed Positive Drug and/or Alcohol Test

The Requester or STR/AdSTR and LANL manager shall take the following actions if a Subcontract worker has a confirmed positive drug test:

- Immediately stop the worker from performing any additional work on site;
- 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 when a drug test is confirmed positive;
- Ask the worker to call a relative or friend to take him/her home when an alcohol test is confirmed positive;
- Confiscate the worker's badge and return it to Personnel Security;
- Consult with LANL Occupational Medicine to determine whether the worker should have a medical evaluation prior to driving;
- If alcohol related, instruct worker to report to LANL Occupational Medicine the next work day, prior to performing any work duties, for a Fitness for Duty evaluation unless the assignment is terminated.
- Coordinate with the CA/PS to ensure proper notifications are made regarding test results and any changes to the subcontract worker's assignment.

5.1.8 Failure to Show or Refusal of Drug and/or Alcohol Test

- If a Subcontract worker fails to show up for a test after being contacted, such failure shall be treated in the same manner as a confirmed positive.
- If a Subcontract worker refuses to be tested, such 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 worker from the LANL site and work on the subcontract.

5.1.9 Drug Detection Dogs may be used:

- On all Laboratory property (DOE-owned, leased or rented property for LANL) including, but not limited to parking lots.
- In and around worker's privately-owned vehicles parked on Laboratory property.
- In and around work areas.

- In and around desks, lockers and other containers assigned to workers.

5.1.9.1 If illegal drugs are found on a Subcontract worker's person by using drug-detection dogs, the Requester or STR/AdSTR and LANL manager shall take action as outlined in Subsection 5.1.6.

5.1.9.2 If illegal drugs are not found, but the drug-detection dogs alert to the scent of illegal drugs in private property owned by a worker or in a work area, desk, locker or other container assigned to a certain employee and no illegal drugs are actually found, the LANL Physical Security Team shall notify the subcontract worker's LANL manager of a drug-detection dog alert. Additional action may be taken if behavior is observed by the LANL manager that may pose an immediate threat to the health and safety of the worker or others or a potential threat to security.

5.1.10 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, on Laboratory business, or on 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.

5.2 Badges

SUBCONTRACTOR shall ensure compliance with the badge requirements outlined in the following subsections. Any individual performing work under this subcontract shall obtain a DOE or LANL badge. (Subcontract workers, Guests and Affiliates)

All badges issued by the LANL Badge Office are accountable. SUBCONTRACTOR shall ensure that every badge issued under this subcontract is returned to the LANL Badge Office. SUBCONTRACTOR shall also timely report any lost or stolen badges to the LANL Badge Office. Failure to return DOE security and site-specific (LANL) badges will result in denial of future badging services to the badge holder.

5.2.1 General Badging Requirements

5.2.1.1 A Subcontract Worker who is submitted for a standard DOE-Cleared or Uncleared badge or a LANL-Only Site-specific badge shall provide Real ID approved proof of U.S. citizenship to the LANL Badge Office at the time of badging. The following applies regardless of the length of time that a Subcontract Worker will be on site.

5.2.1.2 Proof of citizenship includes an original photo identification card, such as a current and valid state driver's license or passport and an original of one of the following five secondary evidence documents:

- For a Subcontract worker born in the U.S., a birth certificate filed for record shortly after birth and certified with the registrar's signature is required. 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. All documents submitted as evidence shall be original or certified.
- For a Subcontract worker claiming citizenship by naturalization, a Certificate of Naturalization showing the individual's name is required. (*Form N550 or N570*)
- For a Subcontract worker claiming citizenship acquired by birth abroad to a US citizen, one of the following (showing the worker's name) is required: Certificate of Citizenship issued by the Immigration and Naturalization Service; Consular Report of Birth Abroad of a Citizen of the United States of America (*Form FS240*); or Certificate of Birth (*Form FS 545 or DS 1350*).
- A current US passport.

- A record of Military Processing-Armed Forces of the US (*DD Form 1966*) provided it reflects that the worker is a US citizen.

5.2.1.3 A Subcontract Worker who is a US citizen, does not currently hold a DOE badge and meets applicable requirements, shall be issued a DOE Uncleared badge or LANL-Only Site-specific badge.

5.2.1.4 A Subcontract Worker who is either a Cleared or an Uncleared foreign national shall be badged in accordance with current DOE and LANL policies. The Subcontract worker shall wear a photo badge whenever on DOE property (i.e. LANL) or LANL-leased premises.

5.2.1.5 Individuals who falsely certify their citizenship will be removed from the Laboratory and will be denied future access to LANL. This will be reported to the appropriate LANL organizations for investigation and other external organizations as necessary.

5.2.2 Obtaining a Badge

5.2.2.1 Worker (US Citizen) Requirements

- A Subcontract worker shall obtain either a DOE or a LANL badge before performing any work at LANL.
- A Subcontract worker shall present identification as required by the Badge Office before being issued a badge.

5.2.2.2 Official Visitor (US Citizen) Requirements

- An Official Visitor shall obtain a badge in accordance with this document;
- An Official Visitor shall wear a badge issued by the LANL Badge Office whenever on Laboratory Property;
- Uncleared Official Visitors will be required to sign a "*Statement of U.S. Citizenship*" form at the LANL Badge Office affirming their U.S. citizenship;
- Uncleared Official Visitors shall receive a briefing that covers safety and security requirements relevant to the work they will be performing;
- Uncleared Official Visitors who falsely certify their citizenship will be removed from the Laboratory and will be denied future access to LANL. This breach will also be reported to the appropriate LANL organizations.

5.2.2.3 Cleared Foreign National (Worker or Official Visitor) Requirements

A cleared foreign national, in conjunction with his or her Laboratory Host, shall contact the LANL Personnel Security Office to receive a cleared foreign national badge.

5.2.2.4 Uncleared Foreign National (Worker or Official Visitor) Requirements

An Uncleared foreign national, in conjunction with his or her Laboratory Host, shall contact the Foreign Visits & Assignment Team before performing work or other activities at LANL; and contact the LANL Personnel Security Office to receive an Uncleared foreign national badge.

5.2.3 Subcontract Workers shall:

- Complete training required by Personnel Security before receiving a badge (see Section 3.4.2 for training details);
- 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, LANL host, or the Personnel Security Group;
- Not allow other individuals to use their badge under any circumstances;
- Minimize the number of instances of temporary badge issuance and replacement of

lost badges;

- Ensure the badge is never photocopied;
- Return an issued badge to the Badge Office (via the RLM or STR/AdSTR as appropriate) following termination of employment, badge expiration, end of assignment, or completion of a visit. Subcontract Workers are not permitted to retain badges for any reason.
- Failure to return DOE security and LANL site-specific badges will result in denial of future badging services to the badge holder.

5.2.4 Badge Expiration Dates

5.2.4.1 Badges may be issued for the term of the subcontract. However, a SUBCONTRACTOR shall only request a badge for the period of time in which a Subcontract Worker will be utilized on this subcontract.

5.2.4.2 SUBCONTRACTOR shall abide by the following end date requirements:

- When a Subcontract Worker is working multiple subcontracts all outside of Security Areas, the earliest end date among the subcontracts will be the badge end date.
- When a Subcontract Worker holds a clearance (i.e., access authorization) under multiple subcontracts, the badge end date is based on the subcontract that is designated as the "primary" subcontract.
- When a Subcontract Worker holding a clearance (i.e., access authorization) is performing work under multiple subcontracts held by a Subcontractor that has received a favorable FOCI determination, the earliest end-date among those subcontracts is used. A new badge will need to be requested if there is any work to be performed that extends beyond the earliest end-date within a Security Area.

5.2.4.3 If a subcontract is going to be extended, SUBCONTRACTOR shall renew a Subcontract Worker's badge within 30 days prior to its expiration.

5.2.5 Lost or Stolen Badge(s)

5.2.5.1 Lost or stolen badges shall be reported to the LANL Badge Office 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. The individual badge holder shall go to the LANL Badge Office and complete a written affidavit (*Form 1672*) *Notification of Permanent Inactivation of Badge* in order to obtain a replacement badge.

5.2.5.2 In addition to 5.2.5.1, if a badge is stolen, the individual badge holder shall report the theft to the Security Incident Team (SIT) and inform the STR/AdSTR or CA/PS by the next business day of discovery of the loss.

5.3 Clearances (i.e., access authorizations)

SUBCONTRACTOR shall follow all clearance requirements outlined below and shall not permit any individual to have access to classified information; except when access to classified information is determined by proper clearance and the need-to-know.

The requirements for securing eligible personnel and proper personnel security clearances (i.e., access authorizations) for "L" and "Q" work and for complying with other security regulations and procedures shall not be considered cause for an extension of time for performance of the subcontract work or for extra payments under the subcontract. However, the cost of processing DOE "Q" or "L" access authorizations will be borne by the Government.

5.3.1 Requesting an Initial Clearance

SUBCONTRACTOR shall ensure that Subcontract Workers:

- Provide information required to request a clearance, including, but not limited to, proof of citizenship, Personal Identification Verification (PIV) documents, fingerprints, residence, work, education, military history, and personal references, as well as specific information regarding any legal, financial, mental health or loyalty issues;

- Have had a complete a background investigation and testing for illegal drugs;
- Verify the Subcontract Worker's record is active in the system, correct and complete through the RLM or STR/AdSTR, including employer and subcontract number and that the worker is working on a FOCI approved contract;
- Complete a *Clearance Request/Recertification/Suitability Form* (DOE F 472.1C) signed by a LANL RLM.
- Complete an online (e-QIP) *Questionnaire for National Security Positions QNSP* (SF-86) and attendant clearance documents when requested by the Personnel Security Office.
- Meet with Clearance Processing Security Specialist and/or provide written responses to additional requests for information from Clearance Processing.

5.3.2 Clearance Processing Critical Reporting Elements

SUBCONTRACTOR shall ensure that subcontract workers holding a cleared DOE-standard badge, report any of the following events to Clearance Processing, the RLM and STR/AdSTR within **one (1)** working day of the occurrence unless otherwise stated:

- All arrests, criminal charges (including charges that are dismissed) or detentions by Federal, state, or other law enforcement authorities for violations of the law (other than traffic violations for which only a fine of $300 or less was imposed), within or outside of the US, unless the traffic violations were drug or alcohol related;
- Personal or business-related filing for bankruptcy;
- Any use of an illegal drug, or use of a legal drug in a manner that deviates from approved medical direction;
- Garnishment of wages;
- Legal action effected for name change;
- Change in citizenship;
- Employment by, representation of, or other business-related association with a foreign or foreign-owned interest or foreign national;
- Any hospitalization for mental illness; treatment of drug abuse; or treatment for alcohol abuse;
- Any matters of potential counter-intelligence interest, including but not limited to approaches by individuals seeking unauthorized access to classified information or matter or SNM. If such an approach or contact is made while on foreign travel, workers should notify a Department of State official at the local US Embassy or Consulate;
- Termination of employment - also notify the RLM and STR/AdSTR;
- When the clearance holder or applicant is transferred from one company subcontract to another company's subcontract with LANL;
- Change in duties resulting in a clearance no longer being required;
- Leave of absence or extended leave not requiring access to classified information or matter, or SNM for 90 consecutive working days;
- Leave for foreign travel, employment, assignment, education, or residence for more than three months, not involving official US Government business even if employment continues with the subcontractor.

5.3.3 Security Termination Requirements for Departing Subcontract Workers

Cleared Subcontract workers who are terminating work under a LANL Subcontract at the Laboratory for any reason shall meet all the federal and local requirements for departing workers.

Subcontract workers shall complete all clearance-related departure requirements. Some termination procedures are mandated by federal law. Failing to comply with the requirements can hinder or prevent a worker's future efforts to obtain a security clearance or badging services at LANL. Failure of a Cleared worker to follow proper termination procedures is also reported to NNSA/DOE by LANL Personnel Security.

Clearance-related requirements for departing Subcontract workers include the following:

- **Termination Briefing** - the Subcontract worker shall attend a termination briefing conducted by LANL Personnel Security or SUBCONTRACTOR management; and submit a completed *Safeguards and Security Clearance Termination Briefing Form* to Personnel Security.
- **Security Termination Statement** - the Subcontract worker shall sign and submit a *Security Termination Statement (*DOE Form 5631.29) to LANL Personnel Security.
- **Surrender DOE Access Credentials** - the Subcontract Worker shall surrender his or her security badge to the LANL Badge Office, while coordinating with the RLM and STR/AdSTR.

For each event listed below, the required action shall be carried out within **two (2**) **working days** of the Event described in the first column of the table.

| Event | Do Termination Briefing & Form, and Submit DOE Form 5631.29 | Return These Badges |
|---|---|---|
| Subcontract Worker's employment terminated | Individual Subcontract Worker | Subcontract Worker's badge, whether Cleared or Uncleared, including expired |
| Subcontract Worker transferred from subcontract | Individual Subcontract Worker | Subcontract Worker's badge, whether Cleared or Uncleared, including expired |
| Clearance no longer required | All Subcontract Workers | All Cleared "L" or "Q" badges, including expired |
| Subcontractor's FOCI approval withdrawn or terminated | All Subcontract Workers | All Cleared "L" or "Q" badges, including expired |
| Subcontract completed or terminated | All Subcontract Workers | All badges, whether Cleared or Uncleared, including expired |

- SUBCONTRACTOR shall ensure that any Subcontract Worker who holds a clearance and is no longer working on this subcontract, follows the security clearance termination process outlined above.
- SUBCONTRACTOR shall notify Personnel Security, the RLM, STR/AdSTR and CA/PS of any Event that changes the status of a worker's need for a badge.

5.3.4 Clearance Renewals or Reinvestigations

SUBCONTRACTOR shall ensure that a Subcontract Worker whose clearance is being renewed or reinvestigated:

- Completes the reinvestigation e-QIP package every 5 years for Q clearance holders or every 10 years for L clearance holders.
- Completes the LANL Annual Security Refresher Training before the effective date of the training expiring and access is therefore denied.

5.4 Foreign Ownership, Control or Influence (FOCI)

FOCI determinations are required for a SUBCONTRACTOR, its owners, and lower-tier subcontractors, if a subcontract requires Q or L-cleared access authorizations. Before a Subcontract Worker may be Q or L-cleared, his/her company shall undergo a FOCI certification. A separate FOCI determination is required for a prime subcontractor and any lower-tier subcontractor.

SUBCONTRACTOR'S Key Management Personnel shall have an active clearance or a clearance request in process before a favorable FOCI determination can be returned. As a part of the FOCI determination process, SUBCONTRACTOR'S Facility Security Officer (FSO) and any additional workers with security responsibilities shall complete the self-study course indicated under Section 3.4.2.

SUBCONTRACTOR shall submit their FOCI packages / information online at this website: https://foci.anl.gov/. A favorable FOCI determination shall be rendered prior to LANL granting a

facility clearance requiring access authorizations. Questions related to FOCI should be addressed through the RLM or STR/AdSTR to the Personnel Security POC.

5.4.1 SUBCONTRACTOR shall ensure that the following notifications are immediately provided to the Personnel Security POC and the RLM or STR/AdSTR.

- Written notification of a change in the extent and nature of FOCI that affects the information in the FOCI determination;
- Immediately provide written notification and supporting documentation relevant to changes that would affect the information in a subcontractor's or any tier parents' most recent DOE FOCI submission(s).

5.4.2 SUBCONTRACTOR shall complete and submit a new FOCI package at least every five years or at the request of CONTRACTOR, to the Personnel Security POC.

5.4.3 SUBCONTRACTOR shall certify annually to the Personnel Security POC and inform the RLM or STR/AdSTR and the CA/PS that:

- No significant changes have occurred in the extent and nature of FOCI that would affect the answers to the questions provided in it's FOCI representations;
- No changes have occurred in the organization's ownership;
- No changes have occurred in the organization's officers, directors, and executive personnel.

5.4.4 CONTRACTOR may terminate this subcontract for default if SUBCONTRACTOR either fails to meet obligations imposed by this section, or creates a FOCI situation in order to avoid performance or a termination for default. CONTRACTOR may terminate this subcontract for convenience if SUBCONTRACTOR becomes subject to FOCI and for reasons other than avoidance of performance of the subcontract, cannot, or chooses not to avoid or mitigate the FOCI problem.

5.5 Human Reliability Program **[Not Applicable]**

5.6 Foreign Visits and Assignments **[Not Applicable]**

**G6.0 Information Security (Oct 2018)**

Subcontract Workers shall not disclose LANL data collected, created, processed, transmitted, stored or disseminated by SUBCONTRACTOR in performance of this subcontract, unless each case of such disclosure is specifically approved by the LANL Data Owner and the CA/PS.

Subcontract Workers shall ensure LANL data utilized in the performance of this subcontract is not used for any other purpose that has not been specifically approved by the LANL Data Owner.

6.1 Official Use Only (OUO) and CONTRACTOR Proprietary (CPI) Information

OUO and CPI 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. CPI includes any information relating to the business, operations and programs of LANL not generally known by persons not employed at LANL.

Personal Identifiable Information (PII) is a type of OUO. PII is any information collected or maintained by DOE or CONTRACTOR about an individual, including but not limited to education, medical history, financial transactions and employment history; and information that can be used to distinguish an individual's identity.

SUBCONTRACTOR shall protect OUO and CPI information from unauthorized dissemination (e.g. to persons who do not require the information to perform work under this subcontract) and shall follow all requirements for OUO and CPI documents specified below.

CONTRACTOR shall impose an administrative penalty under this subcontract if:

- OUO information from a document marked as containing OUO information is intentionally released to a person who does not need to know the information to perform their job

- A document marked as containing OUO information is intentionally or negligently release to a person who does not need to know the information to perform their job
- A document that is known to contain OUO information is intentionally not marked
- A document that is known to not contain OUO information is intentionally marked as containing such information

6.1.1 Access

No security clearance is required for access to OUO or CPI. Access to OUO and CPI information shall only be provided to those persons who have a need to know.

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.

6.1.2 Storing

OUO and CPI information shall be stored in a locked room or locked receptacle (e.g. desk, file cabinet, safe). OUO and CPI information stored on a computer shall meet all LANL password, authentication, encryption, or file access control requirements to protect the files from unauthorized access.

6.1.3 Reproduction / Printing

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

6.1.4 Transmitting

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

PII information that is disseminated over networks outside of LANL shall be encrypted with NIST-validated encryption software.

In the case of hard copies being sent outside of LANL - OUO or CPI 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, OUO or CPI 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.

6.1.5 Destroying

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

6.1.6 Export Controlled Information Restrictions

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.). Violations of these laws may result in severe administrative, civil, or criminal penalties. Further dissemination must be pre-approved by Los Alamos National Laboratory.

6.2 Unclassified Controlled Nuclear Information (UCNI)

UCNI is certain unclassified but sensitive government information where unauthorized dissemination is prohibited. UCNI is intended to be viewed only by those individuals with a need-to-

know to perform their official duties or DOE-authorized activities. SUBCONTRACTOR shall protect such information from unauthorized dissemination and shall follow all requirements for UCNI documents specified below.

6.2.1 Access

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

6.2.2 Storing

When 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 meet all LANL password, authentication, encryption or file access control requirements.

6.2.3 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.

6.2.4 Transmitting

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

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

If 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®.

6.2.5 Destroying

Users are not required to destroy electronic media that contain UCNI. Disks should be overwritten using approved software before they are discarded. Hard copy UCNI documents are to be destroyed by shredding in an approved shredder (cross-cut particles no larger than ¼ inch wide and 2 inches long). SUBCONTRACTOR shall coordinate with the LANL Classified Matter Protection & Control Team through the RLM or STR/AdSTR to properly destroy UCNI information.

6.2.6 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.

6.3 Classified Matter and Material **[Not Applicable]**

**G7.0 Controlled Portable Electronic Devices / Wireless Technology (Oct 2018)**

LANL's level of control on wireless computing devices and on other controlled portable articles depends on the type of device, who owns it (Government or non-Government), where it will be located and how it will be used. Microphone, camera, storage and transmit/wireless capabilities restrict where a device may be carried or used without additional approval or authorization.

7.1 Controlled Portable Electronic Devices (PEDs)

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

Controlled PEDs are not permitted in Security Areas without prior authorization. SUBCONTRACTOR shall ensure that controlled PEDs are not brought into a Security Area without prior written approval from the Cyber Information Security Office with concurrence by the RLM or STR/AdSTR. 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 watch, 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) or other wireless transmission capabilities;
- 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;
- All types of Cameras - video, still, digital, film, tablet computers 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 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)

7.2 Approvals Required Before Commencement of Work

7.2.1 Prior to the introduction of any controlled PEDs into a Limited Area or connected to a LANL-owned system, approval shall be obtained from the Cyber Information Security Office. The RLM or STR/AdSTR shall also be informed.

7.2.2 Prior to any wireless operation on wireless projects (unclassified or classified) approval shall be obtained from LANL's Cyber Information Security Office. The RLM or STR/AdSTR shall also be informed. 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.

7.2.3 Subcontractors using wireless technology, including construction sites, need to obtain certification and approval from the Cyber Information Security Office prior to engaging wireless technology. A LANL "Wireless System Security Plan" may also be required.

7.3 Rules for Using Authorized Controlled PEDs in Security Areas

Authorized controlled PEDs with audio recording or data transmitting capabilities in Security Areas shall be turned off (for UCNI), batteries removed (for classified) or placed in an approved Radio Frequency container whenever:

- A classified or UCNI discussion or phone call is taking place within audible range;
- Classified or UCNI computer processing is taking place in the immediate area of the device;
- Classified or UCNI faxing is taking place within the immediate area of the device; and
- Classified or UCNI copying is taking place on a digital copier in the immediate area of the device.

It is the responsibility of subcontract workers to be cognizant of classified or UCNI activities that may be occurring in adjacent work areas. Workers shall confirm that no classified or UCNI activities area taking place in the immediate vicinity prior to using the authorized controlled article.

7.4 Wireless Device Requirements

7.4.1 The use of devices with wireless connectivity such as computing, cellular and printing devices with "Bluetooth" technology, or wireless networking protocol is prohibited anywhere at LANL, including all LANL property and leased space except for certain defined areas. Wireless devices cannot be connected to LANL computing assets or networks. Such capabilities shall be disabled unless the activity has been approved by the LANL Cyber Information 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.

7.4.2 The use of wireless networking, Bluetooth and cell phone technologies is allowed in public areas of the Bradbury Science Museum, the Otowi Cafeteria and public access areas outside buildings such as roadways, sidewalks and parking lots.

7.4.3 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.

7.4.4 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.

7.4.5 Active wireless devices that have prior approval to be in a PPA and/or Limited Area shall be labeled (company sticker, owner's name) to identify Subcontractor ownership.

7.5 LANL and Other Government-owned Wireless Devices

7.5.1 Government-owned cell or satellite phones shall be disabled when inside a Limited Area or higher Security Areas.

7.5.2 All LANL and government-issued cellular devices including smart phones such as Blackberries shall be turned off completely when in proximity to UCNI activity. Batteries must be removed when in proximity to classified activity.

7.5.3 Only LANL-issued Blackberry devices, applications and accessories may be carried in Limited Areas. No Blackberry devices are allowed in Vault Type Rooms, SCIFs or SAPFs.

7.5.4 Government-owned computing controlled articles (e.g. laptops, palmtop computers and PDAs) shall follow access control requirements such as username and password.

7.5.5 Government-owned computing controlled articles shall use anti-virus software to detect malicious activity where the capability exists.

7.5.6 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.

7.6 Non-government Owned Controlled PEDs

7.6.1 Non-government owned controlled PEDs are prohibited in Limited Areas and higher security areas.

7.6.2 All non-government owned cellular devices including smart phones such as Blackberries shall be turned off completely when in proximity to UCNI activity. Batteries must be removed when in proximity to classified activity.

7.6.3 Non-government owned controlled PEDs may not be connected to any LANL-owned information system or network (classified or unclassified) without written approval and may not be used to store any sensitive or classified government information without written approval. *(Form 1897)*

7.6.4 Non-government owned controlled PEDs shall not store or process government controlled unclassified information; unless formal approval has been granted and full disc encryption is utilized.

7.6.5 When privately-owned vehicles are allowed to enter a Limited Area, controlled PEDs that are attached to the vehicle (i.e. built-in cell phones, On Star and CB 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.

7.7 Non-government Wireless Computing Devices

7.7.1 LANL management approval may be required before bringing a non-government computing device (e.g. laptop, Tablet computer, iPhones, iPad) into a Property Protection Area based on local security requirements. *(Form 1897)*

7.7.2 LANL Cyber Information Security Office approval is required if computing devices will be in a Security Area or connected to the LANL network. *(Form 1897)*

7.7.3 LANL management approval is required before connecting a non-government computing device to a LANL network. *(Form 1897)*

7.7.4 Non-government owned wireless computing devices shall be authorized prior to connecting to any LANL wireless computing resource.

7.8 Connecting to Presentation Systems and Using Equipment Remote Controls

7.8.1 Non-government owned controlled PEDs may be connected to stand-alone presentation equipment and stand-alone systems in PPAs provided:

7.8.1.1 The information system has virus detection software active, automatically scanning for malicious code and using the most current definition file and,

7.8.1.2 The information system shall not contain any sensitive information that the controlled article owner does not have authorization to access.

7.8.2 LANL prohibits Radio Frequency (RF) keyboards everywhere.

7.8.3 LANL allows RF and Infrared (IR) remote controls on unclassified presentation equipment (audio, video, etc.) in unclassified workspace without restrictions.

7.8.4 LANL does not allow RF and IR remote controls on classified computers.

7.8.5 IR and RF remote controls are permitted to control projectors.

**G8.0 Contacts (Oct 2018)**

| Name | Telephone | Email |
|---|---|---|
| Security After-hours On-call Officer cell phone | 505-699-4094 | |
| Security After-hours On-call Duty Officer pager | 505-949-0156 | |
| Badge Office | 505-667-6901 | badge@lanl.gov |
| Chief Information Office (CIO) | 505-606-2263 | |
| Chief Information Office on-call pager | 505-664-6282 | |
| Classification Group | 505-667-5011 | |
| Classified Matter Protection & Control | 505-665-1802 | cmpc@lanl.gov |
| Clearance Processing | 505-667-7253 | clearance@lanl.gov |
| Counterintelligence Program | 505-665-6090 | ocihelp@lanl.gov |
| (Cyber) Information Security Help Desk | 505-665-1795 | cybersecurity@lanl.gov |

| Name | Telephone | Email |
|---|---|---|
| Emergency Management & Response | 505-667-6211 | |
| Export Control | 505-665-2194 | export@lanl.gov |
| Fire, Bomb Threat, etc. | 911 | |
| Foreign Ownership Control & Influence | 505-665-1624 | |
| Foreign Visits and Assignments | 505-665-1572 | foreignvisits@lanl.gov |
| Fraud, Waste and Abuse | 505-665-6159 | |
| Immigration Services | 505-667-8650 | |
| Info Security Operations Center (iSOC) Coordinator Pager | 505-949-4762 | |
| Lock Shop | 505-667-4911 | |
| Material Control & Accountability Group | 505-667-5886 | |
| Network Operations Center (NOC) | 505-667-7423 | noc@lanl.gov |
| Personnel Security | 505-665-6565 | |
| Physical Security Team | 505-667-2510 | |
| Protective Force | 505-667-4437 | |
| Protective Force After Hours Reporting (Central Alarm Station) | 505-665-7708 | |
| Protective Force After Hours Shift Commander | 505-665-1279 | |
| Safety Help Desk | 505-665-7233 | safety@lanl.gov |
| Security Help Desk | 505-665-2002 | security@lanl.gov |
| Security Incident Team (SIT) | 505-665-3505 | |
| Wireless Point of Contact | | wirelesssecurity@lanl.gov |

**G9.0 Required Notifications (May 2015)**

SUBCONTRACTOR shall notify the Requester, STR/AdSTR and the Contract Administrator /Procurement Specialist immediately, whenever a change in the scope of the work to be performed has been identified or requested. The Requester or STR/AdSTR shall then notify the appropriate security expert so that any security modifications can be made to the approved Exhibit G in response to the change in the scope of work.

**G10.0 Additional Requirements (Mar 2017)**

10.1 SUBCONTRACTOR shall comply with safeguards and security requirements for TA-55 as outlined below and instructed by the LANL Host.

The following items are not permitted at TA-55 Areas without prior written authorization from the TA-55 Security Team and concurrence by the RLM or STR/AdSTR. These items include:

- Media (e.g. CDs, DVDs, USB flash drives, external hard drives, etc);
- Personal or Non-LANL electronic devices (e.g. cellular phones, Blackberrys, iPhones, iPads, Android devices, smart phones, cordless phones, iPods, Kindles, MP3 Players, etc.);
- Recording equipment (audio, video, optical or data);
- Radio frequency, Infrared or Bluetooth transmitting equipment (e.g. two-way radios, two-way pagers, etc.)
- Electronic equipment with a data exchange port capable of being connected to information system equipment (e.g. iPods, USB flash drive, etc.)
- Non-LANL computers (e.g. palm-tops, laptops, PDAs, etc.)
- Cameras (film or digital, video or still, tablet computers or in cellular phones). If the use of cameras, either inside or outside of a security area is deemed mission essential, it must be authorized via coordination among the STR/AdSTR, the RLM, the TA-55 Security Team, and the Physical Security Team prior to the use of such cameras.

TA-55 does not issue Generic Visitor Badges. All individuals who enter TA-55 workspace must have a LANL or DOE issued badge.

Escorts shall maintain visual contact with all escorted personnel at all times. One individual may escort no more than five persons, except in PF-4 where the ration is four individuals to one escort. While in PF-4, Subcontract workers must also comply with the Safeguards two-person rule.

When entry to PF-4 is required, each escort shall accompany Subcontract workers to the TA-55 Access Control Office where a PF-4 specific entry ticket will be issued.

Vehicle Access:

- With proper authorization, only Government and Subcontractor vehicles are allowed entry into the TA-55 Protected Area (PA);
- Private vehicles are not allowed entry;
- Vehicles requiring entry through the West Vehicle Access (WVA) shall be approved prior to entering;
- Only the driver and LANL escort are allowed to enter the PA inside a vehicle. All other personnel shall enter the PA via the East Control Facility (ECF).

10.2 SUBCONTRACT workers shall comply with the following site-specific requirements for TA-15 and TA-16 while working in those areas.

- Report to either the TA-15 or TA-16 Access Control Office to check in prior to beginning work and to check out after work in those areas;
- Lock personal or company vehicles when left unattended;
- Report all suspected thefts to the LANL Deployed Security Representative for the organization where the work is being performed

10.3 If any of the following activities or situations are tied to the scope of work for a specific Release under this Basic Agreement, additional security provisions will be added to the Release against this Agreement:

- Work in a SCIF or SAPF: LANL Host will provide required additional training requirements and instructions.
- Work in a Vault Type Room: additional training listed under 3.4.2, as well as instructions from LANL Host.
- Access to Classified data, information or discussions: LANL host will provide additional instructions and training requirements.

# Attachment G1

**EXHIBIT G PHYSICAL SECURITY**
**SECURITY REQUIREMENTS**
**Vendor Name (if Applicable): TBD**
**P.R. No. MTOA RFP 1698656**
**Ex. G dated: 09/04/2019**

## REQUIRED REVIEWS AND APPROVALS

**Reviewed By:**

| Stephan Maestas | STEPHAN MAESTAS (Affiliate) Digitally signed by STEPHAN MAESTAS (Affiliate) Date: 2019.09.04 07:41:39 -06'00' | 09/04/2019 |
|---|---|---|
| Name of DSO or SPL | Signature | Date |