

**EXHIBIT G
SECURITY REQUIREMENTS
CAPACITY CLUSTER TLCC2
UNLOAD UNPACK INSTALL
B590550
TABLE OF CONTENTS**

<u>No.</u>	<u>Clause Title</u>	<u>Page</u>
G1.0	Definitions and Acronyms (May 2009)	2
G2.0	Security Requirements (May 2009)	2
2.1	DEAR Clauses Incorporated By Reference.....	2
2.2	DOE Directives Incorporated by Reference	2
2.3	Goal of Zero Security Incidents	5
G3.0	General Security (May 2009)	5
3.1	Work site, Security Area, Badge and Data Information	5
3.2	Integrated Safeguards and Security Management (ISSM).....	6
3.3	Safeguards, Security and Counterintelligence Awareness.....	6
3.4	Security Training N/A	6
3.5	Security Stop Work.....	6
3.6	Reporting Security Incidents	7
G4.0	Physical Security (May 2009)	7
4.1	Prohibited Articles	7
4.2	Escorting	7
4.3	Security Areas	9
4.4	Acknowledgement / Control of Vehicles On-Site.....	9
4.5	Enhanced Security Areas	9
4.6	Security Fences and Barriers	9
G5.0	Personnel Security (May 2009)	10
5.1	Substance Abuse	10
5.2	Badges	12
5.3	Clearances (i.e., access authorizations) N/A	14
5.4	Foreign Ownership, Control or Influence (FOCI) N/A	14
5.5	Human Reliability Program N/A	14
5.6	Foreign Visits and Assignments N/A	14
G6.0	Information Security (May 2009) N/A	14
G7.0	Cyber Information Security (May 2009) N/A	14
G8.0	Portable Electronic Devices / Wireless Technology (May 2009)	14
8.1	Controlled Articles	15
8.3	Approvals Required Before Commencement Of Work.....	15
8.4	Unallowable Technology on LANL property	15
8.5	General Wireless Device Requirements.....	16
8.6	LANL and Government-owned Wireless Devices	16
8.7	Non-government Owned PEDs in LANL Security Areas	16
8.8	Non-government Wireless Computing Devices.....	16
8.9	Connecting to Presentation Systems and Using Equipment Remote Controls... 16	16
G9.0	Contacts (May 2009)	17
G10.0	Required Notifications (Dec 2007)	17

G1.0 Definitions and Acronyms (May 2009)

Definitions and acronyms may be accessed electronically at http://www.lanl.gov/orgs/adss/ExG/docs/definitions_acronyms.pdf

G2.0 Security Requirements (May 2009)

SUBCONTRACTOR shall ensure compliance with all requirements specified in this exhibit, and those additional specific security requirements not listed herein that CONTRACTOR determines to be necessary to perform the subcontract in a secure manner. 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.

2.1 DEAR Clauses Incorporated By Reference

2.1.1 The Department of Energy Acquisition Regulation (DEAR) clauses which are incorporated by reference herein shall have the same force and effect as if printed in full text.

2.1.2 Full text of the referenced clauses may be accessed electronically at <http://www.management.energy.gov/DEAR.htm>.

2.1.3 The following alterations apply only to FAR and DEAR clauses and do not apply to DOE or NNSA Directives. Wherever necessary to make the context of the unmodified DEAR clauses applicable to this subcontract:

- The term "Contractor" shall mean "SUBCONTRACTOR;"
- The term "Contract" shall mean this subcontract; and
- The term "DOE", "Government," "Contracting Officer" and equivalent phrases shall mean CONTRACTOR and/or CONTRACTOR'S representative, except the terms "Government" and "Contracting Officer" do not change when a right, act, authorization or obligation can be granted or performed only by the Government or the prime contract Contracting Officer or his duly authorized representative; or where specifically modified herein.

2.1.4 The following clauses apply as stated in the Instructions.

Clause Number	Title and Date	Instructions
DEAR 952.204-2	Security (May 2002)	Applies when work involves or may involve classified information, access to special nuclear materials or the provision of protective services.
DEAR 952.204-70	Classification / Declassification (Sep 1997)	Applies when work involves or may involve access to classified information.
DEAR 952.204-73	Facility Clearance (May 2002)	Applies when Subcontractor employees/workers are required to possess access authorizations.
DEAR 952.247-70	Foreign Travel (Dec 2000)	Applies if foreign travel may be required in order to perform subcontract work. If applicable, authorization is required from DOE prior to traveling.
DEAR 952.204-77	Computer Security (Aug 2006)	Applies when Subcontractor has access to computers owned, leased or operated on behalf of the DOE.
DEAR 970.5204-1	Counterintelligence (Dec 2000)	Applies when DEAR 952.204-2 Security and DEAR 952.204-70 Classification / Declassification are applicable.

2.2 DOE Directives Incorporated by Reference

When requested by CONTRACTOR, SUBCONTRACTOR shall provide such information, assistance and support as necessary to ensure CONTRACTOR'S compliance with the following DOE/NNSA Directives, as applicable to the scope of work. 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/directives/read.html>. Applicable NNSA NAP documents may be provided to SUBCONTRACTOR by the Contract Administrator / Procurement Specialist (CA/PS) upon request.

Clause Number	Title	Instructions
DOE O 142.1	Classified Visits Involving Foreign Nationals	Applies if contract involves access by foreign nationals to classified information.
DOE O 142.2A	Voluntary Offer Safeguards Agreement and Additional Protocol with the International Atomic Energy Agency	Applies to contracts which involve activities potentially subject to application of safeguards by the International Atomic Energy Agency (IAEA)
DOE M 142.2-1	Manual for Implementation of the Voluntary Offer Safeguards Agreement and Additional Protocol with the IAEA.	Applies if contract involves activities associated with the IAEA Safeguards Agreement.
DOE O 142.3 Chg 1	Unclassified Foreign Visits and Assignment	Applies if contract involves foreign national access to DOE-owned or leased sites/facilities. Applies if contract involves off-site foreign national access to DOE information or technologies that are not releasable to the public.
DOE M 205.1-4	National Security System Manual	Applies if contract involves National Security Systems that collect, process, store, display, create, disseminate, or transmit information.
DOE M 205.1-8	Cyber Security Incident Management Manual	Applies if contract work involves information systems used on behalf of DOE/NNSA to collect, process, store, display, create, disseminate or transmit national security or unclassified DOE / government information.
DOE O 205.1A	Department of Energy Cyber Security Management Program	Applies if contract includes access to DOE unclassified or classified information and information systems used or operated by CONTRACTOR.
DOE M 452.4-1A	Protection of Use Control Vulnerabilities and Designs	Applies if contract work involves access to Sigma 14 and 15 nuclear weapon data.
DOE O 452.4A	Security and Control of Nuclear Explosives and Nuclear Weapons	Applies if contract includes work in support of the Nuclear Explosive and Weapon Security and Control Program.
DOE O 457.1	Nuclear Counterterrorism	Applies if contract involves or could potentially involve accessing or generating nuclear weapon design information.
DOE M 457.1-1	Control of Improvised Nuclear Device Information	Applies if contract involves or could potentially involve accessing or generating improvised nuclear device information.
DOE O 460.2A	Departmental Materials Transportation & Packaging Management	Applies if contract involves transportation and packaging of hazardous or nonhazardous material.
DOE M 460.2-1A	Radioactive Material Transportation Practices Manual	Applies if contract involves transportation and packaging of radioactive material or radioactive waste.
DOE O 461.1A	Packaging and Transfer or Transportation of Materials of National Security Interest	Applies if contract includes packaging and shipment off-site of materials of national security interest.
DOE P 470.1	Integrated Safeguards and Security Management (ISSM) Policy	Applies to all work performed for CONTRACTOR.

Clause Number	Title	Instructions
DOE M 470.4-1 Chg 1	Safeguards and Security Program Planning and Management	Applies when contract requires security training and/or requires a FOCI determination for access authorizations (clearances).
DOE M 470.4-2, Chg 1	Physical Protection	Applies if contract includes responsibilities for operating, administering, and/or protecting DOE safeguards and security interests.
DOE M 470.4-4A	Information Security	Applies if contract includes access to unclassified or classified information and matter controlled by statutes, regulation or DOE directives.
DOE M 470.4-5	Personnel Security	Applies if contract work requires employees to hold a clearance and/or when official duties require access to classified information or matter, or special nuclear material or data.
DOE M 470.4-6 Chg 1	Nuclear Material Control and Accountability	Applies if contract includes access to nuclear or special nuclear material or data.
DOE O 471.1A	Identification and Protection of Unclassified Controlled Nuclear Information	Applies to work activities that may generate, possess, or have access to information or matter containing UCNI.
DOE M 471.1-1 Chg 1	Identification and Protection of Unclassified Controlled Nuclear Information Manual	Applies to work activities that may generate, possess, or have access to information or matter containing UCNI.
DOE O 471.3	Identifying Official Use Only Information	Applies if contract involves activities where Official Use Only (OUO) information and documents will be handled, used or generated.
DOE M 471.3-1	Manual for Identifying and Protecting Official Use Only Information	Applies if contract involves activities where Official Use Only (OUO) information and documents will be handled, used or generated.
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.
DOE M 475.1-1B	Identifying Classified Information Manual	Applies if contract work includes access to classified information, documents, or material.
DOE O 475.2	Identifying Classified Information	Applies if contract work includes access to classified information, documents, or material.
DOE O 551.1C	Official Foreign Travel	Applies if contract work involves or could potentially involve official foreign travel.
DOE 1450.4	Consensual Listening-in to or Recording Telephone/Radio conversations	Applies if contract includes the use of, or access to, a telephone system of the Federal Government.
DOE O 5639.8A	Security of Foreign Intelligence Information and Sensitive Compartmented Information Facilities	Applies if contract work requires access, receipt, storage, processing and/or handling of Foreign Intelligence Information.
NAP 14.1C	NNSA Baseline Cyber Security Program	Applies if contract work involves the collection, creation, processing, transmission, storage or dissemination of DOE or NNSA unclassified or classified information on automated information systems.

Clause Number	Title	Instructions
NAP 14.2C	NNSA Certification and Accreditation Process for Information Systems	Applies if contract requires CONTRACTOR to maintain information systems that collect, create, process, transmit, store or disseminate unclassified or classified DOE or NNSA data.
NAP 14.3B	Transmission of Restricted Data Over Secret Internet Protocol Router Network (SIPRNet)	Applies if contract involves the collection, creation, processing, transmission, storage or dissemination of classified DOE or NNSA information on SIPRNet.

2.3 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.

G3.0 General Security (May 2009)

3.1 Work site, Security Area, Badge and Data Information

WORK SITE TA-3 SM 1498 SM 2327	
<input checked="" type="checkbox"/>	DOE owned/leased (LANL) or LANS' owned/leased facility or property
<input type="checkbox"/>	Subcontractor owned/leased <u>and</u> DOE Owned / Leased (LANL) facility or property
<input type="checkbox"/>	Subcontractor owned/leased only

TYPE / CATEGORY	
<input type="checkbox"/>	Subcontract
<input type="checkbox"/>	Subcontract Master Task Order
<input type="checkbox"/>	Subcontract Task Order / Release
<input type="checkbox"/>	Purchase Order (will not become a Subcontract)

ON-SITE WORK AREA DESIGNATION	
<input type="checkbox"/>	Open Area
<input type="checkbox"/>	Property Protection Area (PPA)
<input checked="" type="checkbox"/>	Limited Area (LA)
<input type="checkbox"/>	Protection Area (PA)
<input type="checkbox"/>	Material Access Area (MAA)
<input checked="" type="checkbox"/>	SCIF, SAPF or VTR

BADGE TYPE / CLEARANCE LEVEL	
<input type="checkbox"/>	LANL Generic Uncleared US Visitor
<input checked="" type="checkbox"/>	LANL Generic Uncleared US Visitor Escort Required
<input type="checkbox"/>	LANL Uncleared Foreign National badge
<input type="checkbox"/>	LANL Cleared Foreign National badge
<input type="checkbox"/>	Uncleared DOE badge
<input type="checkbox"/>	L-Cleared DOE badge
<input type="checkbox"/>	Q-Cleared DOE badge
<input type="checkbox"/>	HRP

DATA CLASSIFICATION N/A No Data accessed	
<input type="checkbox"/>	Classified
<input type="checkbox"/>	UCNI
<input type="checkbox"/>	Unclassified Sensitive
<input type="checkbox"/>	Unclassified

DATA CLASSIFICATION N/A No Data accessed	
	Unclassified / Public Release

3.2 Integrated Safeguards and Security Management (ISSM)

ISSM uses a five-step process 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 ISSM five-step 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.

3.3 Safeguards, Security and Counterintelligence Awareness

3.3.1 Operations Security (OPSEC) Plan **N/A**

SUBCONTRACTOR shall develop, with assistance from CONTRACTOR'S Operations Security Program Office, implement and sustain a DOE OPSEC Plan using the template provided by the Contract Administrator / Procurement Specialist. SUBCONTRACTOR'S OPSEC Plan shall be approved by CONTRACTOR'S Office of Counterintelligence, Operations Security Program Office before work may begin at LANL. A link to the OPSEC Plan template is <http://www.lanl.gov/orgs/adss/ExG.shtml>

3.3.2 SUBCONTRACT workers shall report all of the following situations to the Office of Counterintelligence and inform the RLM or STR and CA / PS. Situations may range from pointed questions to subtle elicitation.

- Professional contacts and relationships with sensitive country foreign nationals, whether they occur at one's worksite or abroad.
- All unofficial travel to any sensitive country.
- Any suspicious or provocative actions encountered while on travel.
- 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)

3.3.3 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;
- unusual foreign travel patterns of workers; and
- personal problems of workers that could affect security or fitness for duty.

3.4 Security Training **N/A**

3.5 Security Stop Work

When any Subcontract Worker observes a security related hazard or unmitigated risk, the worker has the authority and responsibility to inform any worker engaged in the security related hazard or unmitigated risk of his/her concern and request that the work be stopped.

3.6 Reporting Security Incidents

This subsection contains requirements for identifying and reporting known and potential incidents of security concern. Such incidents may involve issues associated with Personally Identifiable Information (PII), classified matter, computer systems, nuclear materials, secure communications, personnel security, and physical security occurring on LANL property, Laboratory-leased property or SUBCONTRACTOR-owned property. Subcontract workers shall comply with the following requirements.

3.6.1 Immediately upon discovery of a potential incident of security concern, report such concern to the Security Inquiry Team (SIT) (505-665-3505) and then inform the RLM, STR, and SPL or DSO. During normal business hours, notifications shall be made only in person or through secure communications (STU or STE) as required below. 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.

3.6.1.1 The potential compromise of PII shall be reported *immediately* upon discovery to the SIT. A potential compromise of PII is considered a serious information security incident because of the possibility of significant adverse consequences to the individuals whose data has been compromised.

3.6.1.2 *Immediately* report all security incidents and potential threats and vulnerabilities involving LANL data utilized by the SUBCONTRACTOR to the SIT and notify the appropriate CSSO or OCSR, RLM and STR.

3.6.1.3 After discovery of any incident involving the loss, compromise, or unauthorized disclosure of classified matter, report the incident *immediately* to the SIT and then inform the assigned OCSR, RLM and STR.

3.6.1.4 After discovery of any incident involving the loss, theft, diversion, or unauthorized use of nuclear material, report the incident *immediately* to Material Control & Accountability Group or the SIT.

3.6.2 Contact Requirements Outside of Normal Business Hours

For all incidents contact the ADSS on-call duty officer through the Protective Force central alarm station at 505-667-4437, *immediately* after discovery of a potential incident of security concern. The ADSS on-call duty officer may be asked to meet with the SUBCONTRACTOR in person so that SUBCONTRACTOR may report such known or potential incidents of security concern, if secure communications are not available.

G4.0 Physical Security (May 2009)

4.1 Prohibited Articles

Prohibited Articles are those not permitted on DOE property (e.g., LANL) including parking lots. SUBCONTRACTOR shall ensure that prohibited articles are not brought on to DOE property. 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;
- alcoholic beverages, including unopened bottles or cans;
- controlled substances such as illegal drugs and associated paraphernalia, but not prescription medicine; and
- items prohibited by local, state or federal law.

4.2 Escorting

In addition to any facility-specific escorting requirements, SUBCONTRACTOR shall ensure that all LANL escorting requirements listed below are complied with while in a Security Area - whether escorting individuals or being escorted by another individual.

4.2.1 Uncleared foreign nationals are allowed unescorted in publicly-accessible Laboratory property only. Uncleared foreign nationals are not permitted in Security Areas, and only

under extraordinary circumstances should an exception be requested. Uncleared foreign nationals may only be escorted into a security area if prior approval has been obtained from DOE/HQ and local security officials. This process takes a minimum of eight (8) weeks.

- 4.2.2 An Uncleared US citizen may be authorized for escorted access into a Security Area only if such individual:
- is entering an area to conduct official LANL business that can be accomplished only in a Security Area, or
 - has a skill or ability that is required and cannot be provided by another person who has the required clearance (i.e., access authorization) level.
- 4.2.3 The following individuals shall be escorted in a Security Area:
- Uncleared US citizens;
 - US citizen visitors who do not have a cleared DOE-standard badge; and
 - L-cleared US citizens in a Q-Only Security Area.
- 4.2.4 All US citizens escorted into a Security Area shall wear one of the following:
- An Uncleared DOE standard badge;
 - A LANL Generic Uncleared US Citizen Visitor Badge or;
 - A LANL Generic Uncleared US Citizen ESCORT REQUIRED Visitor Badge.
- 4.2.5 Subcontract workers who are being escorted shall:
- State country of citizenship for their escort before entering a security area;
 - Log in, pursuant to the manner required by the LANL owning / tenant organization, before entering a security area;
 - Physically remain with his/her escort upon entry, during the visit and upon exit of a security area.
 - Comply with all requirements outlined by the escort.
- 4.2.6 Subcontract Workers serving as escorts have the following responsibilities:
- Complete "Escort Responsibilities" training course prior to escorting individuals;
 - Be a US Citizen and possess a valid DOE badge and clearance level for the Security Area being accessed;
 - Ensure the Visitor being escorted has a valid photo ID prior to issuing any badge;
 - Ensure each individual being escorted is a US citizen through their statement of such status;
 - Provide Visitor with clear instructions on the rules of behavior and consequences for failure to comply, before granting access to facilities and/or information systems;
 - Confirm that each Visitor displays their assigned badge whenever in a Security Area;
 - Review prohibited and controlled article restrictions with each Visitor prior to escorting such visitor;
 - Protect classified and unclassified controlled matter, information or discussions from unauthorized access by a Visitor;
 - Log in each Visitor by whatever method is provided at the facility being accessed;
 - Notify area occupants of the presence of an Uncleared Visitor;
 - Maintain control of each Visitor at all times;
 - Implement any facility-specific escorting requirements as required;
 - Immediately notify the Requester/RLM and STR of any incident of security concern;
 - Escort each Visitor safely to the organization's designated muster area in the case of an emergency evacuation.
- 4.2.7 An escort shall not escort more than five (5) individuals at any one time, unless otherwise approved by CONTRACTOR in writing.

4.2.8 In cases where an individual without proper security clearance is discovered unescorted in a Security Area, SUBCONTRACTOR shall immediately place such individual under escort by an authorized escort and report the situation to the RLM and STR as soon as possible.

4.3 Security Areas

SUBCONTRACTOR shall comply with all requirements for designated Security Areas. In addition, SUBCONTRACTOR shall ensure that all Subcontract Workers:

- Have the appropriate clearance (i.e., access authorization) for the Security Area or be properly escorted within the Security Area;
- Adhere to the posted requirements for entering any Security Area (clearance status, badge, access status, training and inspections);
- Immediately report physical security and access control discrepancies to the SIT and RLM. Inform the STR. (e.g. breaches of fences or walls or attempts to circumvent security barriers);
- Use a valid badge to enter a Security Area and display the valid badge at all times photo side out, above the waist and in front of the body while in that area;
- Not introduce prohibited articles into Security Areas;
- Obtain authorization before introducing controlled articles into a Security Area;
- Cooperate with Protective Force personnel during badge checks;
- Cooperate with Protective Force personnel during searches of vehicles, persons, and/or hand-carried items being brought into or out of a Security Area;
- Store and protect all keys issued;
- Return all issued keys to the responsible organization Key Custodian when no longer required and inform the RLM and STR of the same;
- Immediately report lost or stolen keys in person to the Key Custodian who issued the keys and inform the RLM and STR of the same;
- Adhere to all requirements for escorting individuals who are not authorized to be in a Security Area unescorted. (See Escorting, Section 4.2);
- Do not tailgate, piggyback, or vouch, nor allow another person to do so.

4.4 Acknowledgement / Control of Vehicles On-Site

- If requested, SUBCONTRACTOR shall submit to the STR or RLM the make, year and license number of all vehicles that will be used on site.
- Vehicles driven by Uncleared drivers delivering construction materials or other supplies will be permitted to enter unsecured areas provided they are under escort by personnel possessing a Q or L access authorization as appropriate for the delivery site.
- All non-government owned heavy duty vehicles (F350 or larger) making deliveries at LANL shall proceed to Post 10 (east end of the Truck Route Road, East Jemez Rd.) for a search conducted by the Protective Force. If the search does not disclose anything of concern, the driver will receive an appropriate pass that will allow entry into their LANL destination.

4.5 Enhanced Security Areas

Subcontract Workers authorized to enter a Sensitive Compartmented Information Facility (SCIF), a Special Access Program Facility (SAPF), a Vault or Vault-type room (VTR), a Material Access Area (MAA), a Protected Area (PA), an Exclusion Area (EA), or a Vital Area shall comply with all training and other security requirements as directed by the LANL host organization and identified in the training matrix. These areas have rigid physical security standards and robust access controls that shall be adhered to.

4.6 Security Fences and Barriers

4.6.1 SUBCONTRACTOR shall make arrangements through the RLM or STR to ensure that adequate access control is maintained at any temporary openings or penetrations of Security Area boundaries. Such work shall be arranged through the RLM or STR and inspected/approved by the Physical Security Team or Deployed Security Officer to ensure there are adequate access controls in place during the temporary opening and that at the end of the work day the temporary openings are repaired / replaced. The CA shall be kept informed of compliance with this requirement by the RLM or STR.

- 4.6.2 At the end of each work day or sooner if required, SUBCONTRACTOR shall repair, replace or provide adequate barriers to preclude unauthorized entry into any Security Area through temporary openings, penetrations, holes dug or cuts in security fences, or through modified gates or other alterations of security perimeters. The repairs shall be inspected / approved by the Physical Security Team or Deployed Security Officer at the end of the work day to ensure the temporary openings are repaired / replaced properly.
- 4.6.3 SUBCONTRACTOR shall make arrangements through the RLM or STR to ensure that any planned placement and proximity of equipment and vehicles to security fences and security boundaries does not create an unintended bridge to a Security Area.

G5.0 Personnel Security (May 2009)

5.1 Substance Abuse

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 Los Alamos National Laboratory as a subcontract worker, guest scientist, visitor, student or other type of worker as it relates to ensuring a work environment that is free from unauthorized or illegal use, possession or distribution of alcohol or controlled substances.

Drugs currently used in CONTRACTOR'S pre-badging and random testing panel include marijuana, cocaine, opiates, phencyclidine and amphetamines.

SUBCONTRACTOR shall ensure that Subcontract workers comply with all requirements of LANL's Substance Abuse Policy (SAP) which may be accessed electronically at <http://www.lanl.gov/orgs/adss/ExG.shtml>. For the purposes of this Exhibit, the term manager as used in the SAP means any or all of the following: STR, LANL manager or staff with oversight of this Subcontract, or on-site Subcontract personnel.

SUBCONTRACTOR shall ensure that all lower-tier subcontractors meet the requirements of this section. Failure at any tier, of a SUBCONTRACTOR to comply with the requirements of this section, shall be grounds for the CONTRACTOR to bar the worker of a SUBCONTRACTOR at any tier, from work on DOE/LANL property or on the subcontract.

5.1.1 Subcontract Workers shall:

- Be fit for duty and avoid behavior that compromises the health or safety of others or the security of the Lab;
- Notify Personnel Security, the RLM, STR and CA/PS immediately if cited, arrested or convicted of a drug or alcohol statute violation;
- Notify Personnel Security, the RLM, STR and CA/PS immediately if they are cited, arrested or convicted of any alcohol-related incident such as (e.g.) DUI, DWI, public intoxication, open container, minor in possession;
- Notify Personnel Security, the RLM, STR, and CA/PS immediately after any initiation of treatment for any drug or alcohol-related disorder (only required of workers with security clearances);
- Meet with Personnel Security or Occupational Medicine promptly when asked to perform a drug and/or alcohol test and fully cooperate with their instructions;
- Provide true and accurate records relating to their use of drugs and alcohol;
- Immediately report accidental ingestion of illegal drugs to Personnel Security, the RLM, and STR so the appropriate action can be taken.

5.1.2 Pre-badging Drug Testing **N/A**

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.

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, 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 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-badging drug testing) will be conducted and paid for by the CONTRACTOR.

5.1.6 Confirmed Positive Drug and/or Alcohol Test

The Requester or STR, 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 OM-MS to determine whether the worker should have a medical evaluation prior to driving;
- If alcohol related, instruct worker to report to OM-MS 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.

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

- If a 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 the 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.

5.1.8 Drug Detection Dogs may be used:

- On all Laboratory property, 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.

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

5.1.8.2 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, 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.

5.1.9 Off-site Behavior

Additionally, the use of illegal drugs or other violations of this substance abuse policy is considered connected to work with or at LANL and may result in the termination of a Subcontractor 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. Therefore, 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 badge or LANL-Only Uncleared badge shall provide proof of U.S. citizenship to the LANL Badge Office at the time of badging. The foregoing 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 and an original of one of the following five documents:

- For a 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 worker claiming citizenship by naturalization, a certificate of naturalization showing the individual's name is required.
- For a 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 US passport, current or expired.
- 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 Uncleared 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 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 worker shall obtain either a DOE badge or a LANL badge before performing any work at LANL.
- A 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, in conjunction with his or her Laboratory Host, shall obtain a badge, in accordance with this document;
- 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 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;
- 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 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;
- Wear the badge, photo-side out, above the waist, on the front side of the body, at all times while on DOE-owned property (i.e., 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, their LANL host, or the Personnel Security Group;

- 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 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.

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 work 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 Badge Office within 24 hours or the next business day after discovery of the loss, whichever is soonest. The RLM or STR 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 the above, if a badge is stolen, the individual badge holder shall report the theft to the Security Inquiry Team (SIT) and inform the STR or CA/PS by the next business day of discovery of the loss.

5.3 Clearances (i.e., access authorizations) **N/A**

5.4 Foreign Ownership, Control or Influence (FOCI) **N/A**

5.5 Human Reliability Program **N/A**

5.6 Foreign Visits and Assignments **N/A**

G6.0 Information Security (May 2009) N/A

G7.0 Cyber Information Security (May 2009) N/A

These requirements apply to any information system or network that SUBCONTRACTOR may use to collect, create, process, transmit, store or disseminate information for CONTRACTOR. Unless specifically waived, CONTRACTOR retains ownership of the data that SUBCONTRACTOR may utilize in performance of this subcontract. Regardless of the performer of the work, SUBCONTRACTOR shall ensure compliance with the provisions of this section.

G8.0 Portable Electronic Devices / Wireless Technology (May 2009)

LANL's level of control on wireless computing devices and on portable electronic devices (PEDs) depends on the type of device, who owns it (Government or non-Government) where it will be located and how it will be used. PEDs include Controlled Articles and Portable Electronic Storage Devices (PESDs)

8.1 Controlled Articles

Controlled Articles are stand-alone devices that can record or transmit data. Controlled articles are not permitted in Security Areas without prior authorization. SUBCONTRACTOR shall ensure that controlled articles are not brought into a Security Area without prior written approval from the Cyber Information Security Office with concurrence by the RLM or STR. Additional LANL site-specific requirements may exist and shall be followed as appropriate.

Controlled articles include:

- Cell phones, cordless phones, two-way pagers, two-way radios;
- Recording equipment (audio, video, optical, or data);
- 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 such as laptops, personal digital assistant (PDAs), palm-top computers, Blackberrys or iPods;
- 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, 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 and must be escorted by a badged LANL Media Relations worker.

8.2 Portable Electronic Storage Devices (PESDs)

PESDs can store, read and/or write nonvolatile information and plug into a computer. They are not stand-alone devices like Controlled Articles. Examples of PESDs include:

- 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)

8.3 Approvals Required Before Commencement Of Work

- 8.3.1 Prior to the introduction of any controlled portable electronic device (PED), including portable electronic storage devices and other controlled articles, 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 shall also be informed.
- 8.3.2 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 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.
- 8.3.3 Subcontractors using wireless technology, including construction sites, need to obtain certification and approval from the Cyber Information Security Office prior to engaging the wireless technology. A LANL "Wireless System Security Plan" may also be required.

8.4 Unallowable Technology on LANL property

- 8.4.1 The use of wireless computing and printing devices such as "Bluetooth" technology or wireless networking protocol is prohibited anywhere at LANL, including all LANL property and leased space except for certain defined areas. 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.

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.

- 8.4.2 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.
- 8.5 General Wireless Device Requirements
 - 8.5.1 For non-government owned unclassified devices with wireless capability, Subcontract workers shall have all wireless networking and Bluetooth disabled while in a PPA unless approved by the LANL Cyber Information Security Office. Software or hardware disablement is permitted.
 - 8.5.2 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.
 - 8.5.3 Active wireless devices that have prior approval to be in a PPA and/or Limited Area shall be labeled to identify Subcontractor ownership.
- 8.6 LANL and Government-owned Wireless Devices
 - 8.6.1 Government-owned cell or satellite phones shall be disabled when inside a LA or above.
 - 8.6.2 Government-owned computing PEDs (laptops, palmtop computers and PDAs) shall follow access control requirements such as username and password.
 - 8.6.3 Government-owned computing PEDs shall use anti-virus software to detect malicious activity where the capability exists.
 - 8.6.4 Government-owned unclassified PEDs are not permitted to connect to any LANL computer or network or store LANL sensitive data without approval from LANL management. (*Form 1865*)
- 8.7 Non-government Owned PEDs in LANL Security Areas
 - 8.7.1 Non-government owned PEDs are prohibited in Limited Areas and above.
 - 8.7.2 Non-government owned 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*)
 - 8.7.3 When privately-owned vehicles are allowed to enter a Limited Area, 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.
- 8.8 Non-government Wireless Computing Devices
 - 8.8.1 LANL management approval may be required before bringing a non-government laptop to a Property Protection Area based on local security requirements. (*Form 1897*)
 - 8.8.2 LANL Cyber Information Security Office approval is required if the laptop will be in a Security Area or connected to the LANL network. (*Form 1897*)
 - 8.8.3 LANL management approval is required before connecting a non-government laptop to a LANL network. (*Form 1897*)
 - 8.8.4 Non-government owned wireless computing devices shall be authorized before connecting to any LANL wireless computing resource.
- 8.9 Connecting to Presentation Systems and Using Equipment Remote Controls
 - 8.9.1 Non-government owned PEDs may be connected to stand-alone presentation equipment and stand-alone systems in PPAs provided:
 - 8.9.1.1 The information system has virus detection software active, automatically scanning for malicious code and using the most current definition file and,
 - 8.9.1.2 The information system shall not contain any sensitive information that the PED owner does not have authorization to access.
 - 8.9.2 LANL prohibits Radio Frequency (RF) keyboards everywhere.

- 8.9.3 LANL allows RF and Infrared (IR) remote controls on unclassified presentation equipment (audio, video, etc.) in unclassified workspace without restrictions.
- 8.9.4 LANL does not allow RF and IR remote controls on classified computers.
- 8.9.5 IR and RF remote controls are permitted to control projectors.

G9.0 Contacts (May 2009)

Name	Telephone	Email
Badge Office	505-667-6901	badge@lanl.gov
Chief Information Office	505-667-0961	
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
(Cyber) Information Security Help Desk	505-665-1795	cybersecurity@lanl.gov
Emergency Management & Response	505-667-6211	
Fire, Bomb Threat, etc.	911	
Foreign Ownership Control & Influence	505-665-1624	
Foreign Visits and Assignments	505-665-1572	
Fraud, Waste and Abuse	505-665-6159	
Immigration Services	505-667-8650	
Info Security Operations Center (iSOC)	505-665-7492	cpc@lanl.gov
Lock Shop	505-667-4911	
Material Control & Accountability Group	505-667-5886	
Network Operations Center (NOC)	505-667-7423	noc@lanl.gov
Operations Security Program Office (OPSEC)	505-665-4843 or 505-667-0002	
Personnel Security POC	505-665-1624	
Personnel Security	505-665-6565	
Physical Security Team	505-667-2510	
Protective Force	505-665-1279	
Protective Force after hours	505-667-4437	
Safety Help Desk	505-665-7233	
Security Help Desk	505-665-2002	security@lanl.gov
Security Inquiry Team (SIT)	505-665-3505	
Wireless Point of Contact		wirelesssecurity@lanl.gov

G10.0 Required Notifications (Dec 2007)

SUBCONTRACTOR shall notify the Requester, STR 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 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.

Attachment G1

EXHIBIT "G"
SECURITY REQUIREMENTS
Vendor Name (if Applicable):
Subcontract / P.O. No. B590550
Ex. G dated: 07/08/10
Rev. No.: 1

REQUIRED REVIEWS AND APPROVALS

Submitted By:		
_____	_____	_____
Name of Requester	Signature	Date
_____	_____	_____
Name of STR	Signature	Date

Sections G1 - G6 & G9 & G10 Reviewed By:		
_____	_____	_____
Name of DSO	Signature	Date
OR		
Bud Shultz	_____	_____
Name of SPL	Signature	Date

Section G7 & G8 Reviewed and Approved By:		
N/A	_____	_____
Name (Cyber) Information Security	Signature	Date

Approved By:		
_____	_____	_____
Name of RLM or Designee	Signature	Date