

EXHIBIT G

Security Requirements for Subcontractors

May 2009

LA-UR 09-03201

Background of Exhibit G

- **Replaces security requirements outlined under former “General Provisions” within your contract**
- **More detailed security requirements necessitated by DOE Compliance Order (7/2007)**
 - Flow comprehensive security requirements to subcontractors
 - Present requirements clearly
 - Requirements are the same as those to be followed by LANL employees
- **Provide clear guidance to subcontractors**
 - Enhance ability to develop bids closely aligned with actual security requirements
 - To mitigate occurrence of future security incidents
- **Flow-down of 6 DEARS (DOE Acquisition Requirements), 20+ DOE Directives & 3 NAPS (NNSA Administrative Policies) required by LANS’ Prime Contract**
 - Translates to ~ 7,000 pages of DOE / NNSA security requirements
 - Includes ~ 600 pages of internal LANL security procedure documents

Goal of Exhibit G

- **Exhibit G consolidates these requirements into 27 pages or less for subcontractor / vendor applicability**
- **Exhibit G “long-form” is tailored (shortened) for each procurement, after security subject matter expert (SME) analysis of the scope of work**
- **Certain low-risk security activities may incorporate short versions of Exhibit G after SME analysis**
- **Exhibit G is required for the procurement of *services*, not goods.**
- **There may be instances where a request for goods & services (e.g. installation) are combined, requiring the inclusion of an Exhibit G**
- **Key to success is a valid, usable, biddable & legally binding Exhibit G**

Content of Exhibit G Long-Form

■ Ten Sections

- *Definitions & Acronyms* (via link)
- *DEAR Clauses, DOE Directives, NAPS* (conditional applicability)
- *General Security* (OPSEC, Training, Stop Work, Reporting Security Incidents)
- *Physical Security* (Prohibited Articles, Escorting, Security Areas)
- *Personnel Security* (Substance Abuse, Badges, Clearances, Foreign visits)
- *Information Security* (OUO, UCNI, & Classified information)
- *Cyber Security* (Training, Reporting, On-site access, Off-site access)
- *Controlled Articles / Wireless Technology* (Approvals, Un-allowed technology)
- *Contacts* (LANL phone numbers, e-mail addresses)
- *Required Notifications* (with a SOW change)

Operations Security (OPSEC)

- **A process designed to disrupt and/or defeat the ability of adversaries to exploit activities and information.**
- **OPSEC process**
 - Identification of critical program activities & information
 - Analysis of threats
 - Analysis of vulnerabilities
 - Assessment of risk
 - Application of appropriate countermeasures to the threats & vulnerabilities
- **Subcontractor and LANS shall jointly perform and document (in an OPSEC Plan) the 5 step OPSEC process.**
- **Certain activities may not require an OPSEC Plan**

Prohibited Articles

- **Definition:**

- Items never permitted on DOE property (e.g. at LANL), including parking lots

- **Items include:**

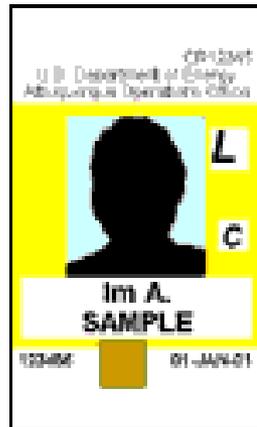
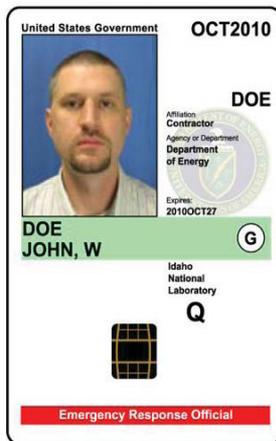
- Dangerous weapons (e.g. guns, knives, explosives)
- Alcoholic beverages, including unopened bottles or cans
- Illegal drugs and associated paraphernalia
- Other items prohibited by law

Substance Abuse

- **Prohibited on LANL site**
 - Unauthorized use of alcohol and/or illegal drugs
 - Being under influence of alcohol and/or illegal drugs
- **Pre-employment testing required for DOE badge – Uncleared, L or Q-cleared**
- **Random drug and alcohol testing for workers with DOE badge**
- **“For-cause” testing for anyone on LANL site, no badge required**
- **Link to approved drug testing laboratories**
http://dwp.samhsa.gov/DrugTesting/Level_1_Pages/CertifiedLabs.aspx

Badge Return Policy

- All subcontractors of LANL shall obtain a LANL or DOE badge.
- All LANL & DOE badges are government property and accountable.
- Every badge under a subcontract must be returned.
- Subcontractor must timely report any lost or stolen badges.
- Failure to return LANL or DOE badges will result in the denial of future badging services to the badge holder.



Foreign Ownership, Control or Influence (FOCI)

- **Company must be FOCI-certified before workers may be “Q” or “L”-cleared**
- **Initial determination + five-year renewal required**
- **Annual certification required**
 - FOCI is suspended if yearly update not received
- **FOCI terminated when company has no active FOCI DOE contracts**

Cyber Security

■ Training

- Less than 10 days on-site receive verbal training
- More than 10 days on-site requires formal training (mostly on-line)

■ On-site system and data access requirements

- Protect all data from those without a “need-to-know”
- Do not share passwords or log on for someone else
- Only workers with appropriate clearance level may have access to classified data

■ Off-site access; storage of LANL sensitive data

- Must receive prior approval to access LANL networks from off-site
- Must use token card for passcode access
- Off-site storage requires prior approval through documented Contractor Cyber Security Plan (CCSP)
- System protections must be identified in the CCSP and in place

Controlled Articles / Wireless Technology

- **Controlled Personal Electronic Devices (PEDs) examples include**
 - Cell phones, thumb drives, recording equipment, laptops, PDAs, Blackberrys, iPods, cameras, RF transmitting equipment, two-way radios or pagers.
- **PEDs are not permitted in LANL Security Areas without prior authorization**
- **Technology prohibited anywhere at LANL, including leased space**
 - Wireless computing, networking, cell phones with “Bluetooth” technology
 - Capabilities must be disabled unless activity is approved

Exhibit G Execution

■ Exhibit G “long-form” tailorable

- Used to address medium & high security risk for on-site work and possibly off-site work
- Will be tailored to include security requirements directly associated with a specific scope of work; 27 pages or less

■ Exhibit G Off-site

- Used to address low security risks; 3 pages

■ Exhibit G On-Site Meetings

- Addresses certain training, presentations, deliveries and equipment installation or repair
- Used to address low security risks; 9 pages

■ Exhibit G Task Order / Release

- Ties to Master Task Order Agreement “long-form” Exhibit G; 4 pages

Exhibit G Resources

- **Link to Exhibit G templates:** <http://www.lanl.gov/orgs/adss/ExG.shtml>
- **LANL Acquisition Services Management Contract Administrators / Procurement Specialists**
- **LANL Subcontract Technical Representative (STR)**
- **LANL Security Program Leads & Deployed Security Officers (provide support to LANL technical organizations)**
- **LANL Exhibit G Project Lead**
- **LANL Cyber Security contacts**
- **LANL OPSEC Plan contacts**