EXHIBIT G OFF-SITE LOW RISK CLOUD COMPUTING SERVICES SECURITY REQUIREMENTS

G1.0 Definitions and Acronyms (Feb 2014)

Definitions and acronyms may be accessed electronically at

http://www.lanl.gov/resources/_assets/docs/Exhibit-G/exhibit-g-definitions-acronyms-green.pdf

G2.0 Statements Applicable To Scope of Work (Oct. 2013)

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

2.1 Work under this subcontract will not be performed at any DOE owned or leased facilities including LANL, LANS' leased facilities, or on DOE property.

2.2 Subcontract workers will not require access to DOE owned or leased facilities including LANL, LANS' leased facilities or DOE property for meetings, presentations, activities or any other reason.

2.3 Subcontract workers will not require any LANL security training to perform work under the subcontract.

2.4 Subcontract workers will not require DOE or LANL badges. DOE or LANL uncleared or cleared badges will not need to be issued to Subcontract workers to perform this subcontract.

2.5 All data, information or research involved with this subcontract is considered open, non-sensitive and routinely published in the public domain.

2.6 Subcontract workers will not have access to or process any LANL Controlled Unclassified Information such as OUO, LPI, PII, UCI, UCNI, or any other sensitive unclassified data that needs to be protected in accordance with U.S. Government policy.

2.7 Subcontract workers will not have access to or process any LANL classified information or data.

2.7 Subcontract workers will not have access to LANL networks or systems requiring authentication.

G3.0 Security Requirements (Feb. 2014)

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

3.1 DEAR Clauses Incorporated By Reference

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

3.1.2 Full text of the referenced clauses may be accessed electronically at http://farsite.hill.af.mil/VFDOE1.HTM

3.1.3 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.

3.1.4 The following clauses apply as stated in the Instructions:

Clause Number	Title and Date	Instructions
DEAR 952.204-77	Computer Security (Aug 2006)	Applies when Subcontractor has access to computers owned, leased or operated on behalf of the DOE.
FAR 52.204-9	Personal Identity Verification of Contractor Personnel (Jan 2011)	Applies when Subcontractor has routine physical access to a Federally-controlled facility and/or routine access to a Federally-controlled information system.

3.2 DOE Directives Incorporated By Reference

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

Directive Number	Title	Instructions
DOE O 142.3A	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.
NAP 14.1C Chpt. VII	NNSA Baseline Cyber Security Program, Chapter VII Incident Management	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.
NAP 14.1D	Baseline Cyber Security	Applies if contract involves National Security Systems that collect, process, store, display, create, disseminate, or transmit information.
DOE O 205.1B Chg 1	Department of Energy Cyber Security Program	Applies if contract includes access to DOE unclassified or classified information and information systems used or operated by CONTRACTOR.
DOE O 471.6 Chg 1	Information Security	Applies if contract includes access to unclassified or classified information and matter controlled by statues, regulation or NNSA policies.
DOE O 471.1B	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 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.

G4.0 Cloud Computing Services (Feb 2014)

SUBCONTRACTOR shall comply with cloud computing services requirements outlined in the following subsections for the use of cloud services. A cloud service denotes any connection that involves delivering host services over the Internet.

4.1 Qualification and Validation

SUBCONTRACTORS shall comply with the following regulations and requirements:

- National Institute of Science Technology (NIST 800-53) found at http://csrc.nist.gov/publications/PubsSPs.html or equivalent approved by the CSSM
- Federal Information Processing Standard (FIPS) Publication 199 found at http://csrc.nist.gov/publications/PubsFIPS.html
- A Cloud Computing Security Plan may be required prior to services beginning

Compliance with these requirements shall be verified by LANL Cyber Information Security prior to SUBCONTRACTOR submitting a formal response to a Request for Proposal.

SUBCONTRACTOR shall complete a Cloud Service Security Requirement Questionnaire as part of the review and approval process which can be found at http://www.lanl.gov/resources/_assets/docs/Exhibit-G/cloud-services-security-requirements-questionnaire-rev2.pdf.

Only those subcontractors who meet the minimum qualifications shall be authorized to provide service.

4.2 Certification and Accreditation

SUBCONTRACTOR shall develop, with the assistance of the LANL Information Cyber Security Office, the following plans prior to the use of a cloud service. These plans must be approved by LANL Cyber Information Security before an Approval to Operate notice is issued.

If SUBCONTRACTOR is already federally authorized or industry tested and authorized, additional certification or accreditation is not required. Supporting documentation will still be required.

- Configuration Management Plan
- Contingency Plan
- System Security Plan or equivalent
- Privacy Impact Assessment (if LANL PII is going to be stored)

SUBCONTRACTOR shall provide results of bi-annual and annual security control test results to the LANL Information Cyber Security Office. A list of the control tests required can be found at http://www.lanl.gov/resources/_assets/docs/Exhibit-G/nist-800-53.pdf

G5.0 Foreign Visits and Assignments (Feb 2014)

Approval for a foreign national to work off-site on a LANL project is not required if the following conditions are met: 1) all work is conducted entirely off-site; 2) work involves ONLY information that is open, non-sensitive and routinely published in the public domain.

If any of the above criteria are not met, approval for a foreign national to work on a LANL project off-site must be obtained from the LANL Foreign Visits and Assignments office PRIOR to commencing work on the Subcontract. The individual who is hosting a foreign national shall be a CONTRACTOR employee and a US citizen.

G6.0 CONTRACTOR Reviews and Approvals

The undersigned CONTRACTOR representative has reviewed the SOW for the proposed Purchase Request, referenced in the footer of this document and believe that all statements listed in Section G2.0 are factually correct.

Name of DSO or SPL	Signature	Date
Name Cyber Security Designee	Signature	Date