

EXHIBIT G7.0 Attachment 2

SUBCONTRACTOR CYBER SECURITY PLAN

Vendor Name (if Applicable):

Subcontract No. PR-

Ex. G dated: XX/XX/XX

Rev. No.: 7

Pursuant to the requirements in the LANL Exhibit G, Section 7.5.1, the following sets forth Subcontractor's specific cyber security responsibilities with regard to identifying and protecting LANL sensitive data, including Personally Identifiable Information (PII), as defined in this Subcontract.

The responsible security officials for this Subcontract are:

LANL's Information Security Site Manager (ISSM)

David Belangia

Los Alamos National Laboratory

P.O. Box 1663, MS B289

Los Alamos, NM 87545

505-667-1982

Subcontractor's Cyber Security Site Manager (or similar position)

Name and Title Name, IT Security Officer

Company Name **Company Name**

Phone Number

Email

Activities of participating parties

1. The data sensitivity determination

The LANL Data Owner specifies the data sensitivity and/or classification of all data that will be collected, created, processed, transmitted, stored or disseminated by SUBCONTRACTOR.

Agreed pursuant to Exhibit G, Section 7.2.

SUBCONTRACTOR ensures:

2. Data is used for agreed upon purposes only.

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, including testing of new systems or applications or demonstrations of software or systems for the purpose of marketing the SUBCONTRACTOR'S skills or services to customers other than LANL.

EXHIBIT G7.0 Attachment 2

Agreed pursuant to Exhibit G, Section 7.3.

3. Suspected or known compromise of PII is reported to LANL.

Immediately report any known or suspected compromise of Personally Identifiable Information (PII) upon determination of a statutory security breach by **(Company Name)** General Counsel to the LANL Security Inquiry Team (SIT) at 505-665-3505 and the contract Subcontract Technical Representative (STR)

Agreed pursuant to Exhibit G, Sections 3.6 and 7.4.

4. Loss of other LANL data, non-PII, is reported to LANL.

Upon determination of a statutory security breach by The Company's General Counsel, report all such breaches involving the LANL data utilized by the SUBCONTRACTOR to the SIT at 505-665-3505 and the contract STR at 505-667-8016.

Agreed pursuant to Exhibit G, Sections 3.6 and 7.4

5. Background screening of Subcontract Workers is completed.

If requested by LANL, agree to a background screening of any Subcontract Worker that will be granted access to LANL data SUBCONTRACTOR may utilize in performance of this subcontract.

It is (Company Name) policy to screen all permanent employees during the employment process. Temporary employees are

6. Subcontractor authentication mechanisms are protected.

Authentication mechanisms, including passwords, issued for the control of SUBCONTRACTOR access to information on information systems are not shared, are protected at the same level of protection applied to the information to which they permit access, and that any compromise or suspected compromise of an authenticator is reported to **(Company Name)** Information Protection Department.

All employees are trained to protect their passwords and

7. Subcontractor authentication methods are robust.

Subcontractor's systems utilize robust, preferably two-factor authentication when granting user access to the data SUBCONTRACTOR may utilize in performance of this subcontract. Robust authentication includes: at least 8 character non-dictionary passwords that are encrypted (i.e.,

EXHIBIT G7.0 Attachment 2

SSL, VPN, etc.) or one-time use passwords.

(Company Name) uses the following authentication methods:

8. That access to systems use the principle of Least Privileged.

Grant user access to LANL data using the least privilege principle; which ensures that Subcontract Workers are granted only the access privileges absolutely necessary to accomplish the work specified by this subcontract.

(Company Name) uses the following process to grant access to sensitive information.

9. That files are examined for malicious code.

(Company Name) uses the following anti-virus software to examine files for malicious code.

10. That sensitive information is protected during transmission.

Ensure that sensitive information transmitted between the contractor's network and LANL is encrypted using a product listed in the NIST FIPS 140-2 validated products list.

<http://csrc.nist.gov/cryptval/>

(Company Name) uses the following encryption methods to transit.....

11. Sensitive information is destroyed when no longer needed.

Subcontractor's hard copies of sensitive documents that are no longer needed are to be destroyed by shredding in a cross-cut shredder.

Subcontractor's are not required to destroy electronic media that contain sensitive data. Disks should be overwritten before they are discarded.

(Company Name) has the following process to destroy or overwrite sensitive information.

12. Periodic Assessment:

The parties shall conduct an initial assessment to certify that protections are implemented and performed as stated in the subcontract and this cyber security plan .

EXHIBIT G7.0 Attachment 2

LANL Information Security will perform an annual assessment of the protections described in the contract with the Company's Information Protection Department for purposes of determining SUBCONTRACTOR's compliance with cyber security requirements and whether modifications to the protections are necessary.

The assessments will be conducted via telephone between LANL Information Security and (Company Name) Information Protection Department. If additional information is required, the parties may elect to meet in person.

13. Violating data management protections outlined in this subcontract may result in actions up to and including removal of Subcontract work from this Subcontract or termination of the Subcontract.

Agreed pursuant to Exhibit A, Termination.

14. Failure of SUBCONTRACTOR to comply with the requirements of this Attachment 2, Cyber Security Plan, of Exhibit G may constitute a material breach of contract. Activities on LANL systems are monitored and recorded and subject to audit. Use of LANL systems and data is expressed consent to such monitoring and recording. Any intentional unauthorized access or use of LANL systems and data is prohibited and could subject the SUBCONTRACTOR to criminal and civil penalties.

Agreed pursuant to Exhibit G, Sections G2.0 and G7.9.

LANL Cyber Security Office Approval:

_____ Date: _____

David Belangia, (ISSM) Los Alamos National Laboratory

_____ Date: _____

IT Security Officer