LAWRENCE LIVERMORE NATIONAL LABORATORY

CYBER SECURITY PROVISIONS

NON-PUBLICLY RELEASABLE LLNS OR THIRD-PARTY DATA

The following provisions shall apply to any work and other activities performed by the Subcontractor or its lower-tier subcontractor under this Subcontract involving the storage and processing of Lawrence Livermore National Security, LLC (LLNS) or Third-Party (Non-Federal) data or information on information systems and networks not owned or managed by LLNS. LLNS or Third-Party data or information may include information that qualifies as confidential, proprietary or business sensitive information, including Official Use Only, Export Controlled, or Privacy information (to include Personally Identifiable Information [PII] and Protected Health Information [PHI]) which is defined as information that is associated with any individual ("LLNS or Third-Party Data"). As used herein, the term "Subcontractor" shall also mean "Seller" and the term "Subcontract" shall also mean "Agreement" or "Purchase Order."

A. Security Controls

The Subcontractor shall provide the following security controls:

1. The Subcontractor shall use reasonable precautions, including but not limited to, physical, software and network security measures, employee screening, training and supervision and appropriate agreements with employees to prevent anyone other than LLNS from gaining unauthorized access to LLNS data.
2. Logically separate LLNS data from other customers.
3. Ensure encryption in transit and at rest meets Federal Information Processing Standard (FIPS) 140-2 level 2 compliance as approved by the National Institute of Standards and Technology (NIST).
4. Ensure all LLNS data resides in a U.S. data center for both primary and secondary locations.
5. Provide support for external SAML-based authentication solutions.
6. Provide ability to display a login banner.
7. Ensure segregation of duties for data access as described in the current version of NIST 800-53 control AC-5 are implemented. Provide description of implementation model upon request.
8. Adhere to the following data backup requirements:
    a. Full and differential backups are run to non-directly connected storage, and be able to be restored within 48 hours to a minimum of the last transaction of the prior business day.
    b. Able to restore backups to a specified time period for a prior period up to thirty days.
    c. Backup integrity and testing checks are run at least annually.

d. Backups meet FIPS 140-2 level 2 standard.

e. Backup data provided to LLNS on media meets the FIPS 140-2 level 2 standard.

9. Provide log files for forensic and investigative purposes.
10. Provide support for LLNS-directed Electronic Discovery (e-Discovery) investigations.
11. Ensure cloud service uptime as described in the Service Level Agreement or Statement of Services.
12. Ensure that Subcontractor employees who have, or will have, access to LLNS Export Controlled data are U.S. persons.
13. Ensure that Subcontractor employees who have, or will have, access to LLNS High Level PII data are working in the U.S. under U.S. laws and regulations

B. Security Audits

The Subcontractor shall conduct site audits of the information technology and information security controls for all facilities used in complying with its obligations under this Subcontract, including but not limited to, obtaining a network-level vulnerability assessment performed by a recognized third-party audit firm based on recognized industry best practices. Upon LLNS' request, the Subcontractor shall submit the following:

1. Security plan and associated documents (e.g., Breach Response Plan, Media Destruction Process, Disaster Recovery Plans, Evidence of Penetration Tests, etc.) If the Subcontractor updates its security plan and associated documents, it shall provide a copy of such documents to the LLNS Contract Analyst.
2. Statement of Standards for Attestation Engagements (SSAE) No. 18 Audit Reports for Reporting on Controls at Service Organization Controls (SOC) Type 2 or 3 Audit Reports.
3. ISO/IEC 27001 Certifications.
4. Health Insurance Portability and Accountability Act (HIPAA) Compliance Audit Reports or HITRUST CSF Assurance Report (if the subcontract involves the Subcontractor having access to LLNS or Third-Party Data subject to HIPAA).
5. Payment Card Industry (PCI) Compliance Report (if the Subcontract involves processing credit card payments).

The Subcontractor shall promptly address any exceptions noted on the SOC reports or other audit reports, with the development and implementation of a corrective action plan by the Subcontractor.

LLNS shall have the right to periodically audit Subcontractor's security practices to ensure compliance with the requirements identified herein. Subcontractor shall provide all reasonable assistance necessary for LLNS to conduct security audits.

C. Data Breach Response

The Subcontractor shall maintain a cyber incident breach response plan, in accordance with accepted industry standards and will implement the procedures required under such plan on the occurrence of a data breach or security incident involving LLNS or Third-Party Data. In the event of a confirmed or reasonably suspected incidents of security concern involving any LLNS or Third-Party Data ("Security Breach"), the Subcontractor shall comply with the following requirements:

1. Provide immediate notification, and within 24 hours, upon discovery of a confirmed or reasonably suspected incidents of a Security Breach by the Subcontractor or its lower-tier subcontractor to the LLNL Security Operations Center at 925-422-4655 (Monday through Friday, 8:00 a.m. – 5:00 p.m. Pacific) or 925-403-4552 (after hours) or via email at cybersecurity@llnl.gov. Also notify the LLNS Privacy Officer (925-422-1100) of a confirmed or reasonably suspected incident of a Security Breach by the Subcontractor or its lower-tier subcontractor involving PII or HIPAA.

2. Notify the LLNS Contract Analyst within 24-hours of notifying the Security Operations Center of any such security incidents.

3. Notifications shall include (to the extent known) information on the extent of the data breach, specific parties impacted, and remedial actions to be taken. Subcontractor shall provide ongoing updates as additional information regarding the compromised data becomes known.

4. Immediately following Subcontractor's notification to LLNS of a Security Breach, the parties shall coordinate with each other to investigate the Security Breach and prevent any further actual or potential unauthorized disclosure of LLNS or Third-Party Data. Subcontractor agrees to fully cooperate with LLNS in its handling of the matter, including, without limitation: (i) assisting with any investigation; (ii) providing LLNS with physical access to the facilities and operations affected; (iii) facilitating interviews with Subcontractor's employees and others involved in the matter; and (iv) making available all relevant records, logs, files, data reporting, and other materials required to comply with applicable law, regulation, industry standards, or as otherwise reasonably required by LLNS.

5. The Subcontractor shall at its own expense take reasonable steps to immediately contain and remedy the Security Breach and prevent any further Security Breach, including, but not limited to taking any action necessary to comply with applicable privacy laws, regulations and standards. The Subcontractor shall provide free credit monitoring for a minimum period of one year for any LLNS personnel, independent contractors, visitors, and guests for whom personal data was compromised as a

result of the Subcontractor's application and/or data center being compromised. Such credit monitoring is cumulative and in addition to any rights or remedies otherwise available to LLNS or the individuals for whom such personal data is compromised.

6. The Subcontractor agrees to maintain and preserve all documents, records, and other data related to any Security Breach.

D. Data Ownership, Access, Usage, Protection and Destruction

1. LLNS retains all rights to any LLNS provided data. The Subcontractor may not utilize LLNS or Third-Party Data for other than what is identified in the Subcontract.

2. The Subcontractor shall not provide access to LLNS or Third-Party Data to third parties without the LLNS Contract Analyst's prior written approval.

3. The Subcontractor shall maintain all LLNS or Third-Party Data obtained during performance of the Subcontract and protect it from any unauthorized disclosure consistent with the requirements of the GENERAL PROVISIONS Clause "Use and Release Restrictions for Protected Information".

4. The Subcontractor shall return (or at LLNS' option destroy) any LLNS or Third-Party Data, including backups, upon cancellation, termination, or expiration of the Subcontract. If the Subcontractor is not reasonably able to return or securely dispose of LLNS or Third-Party Data, including data stored on backup media, the Subcontractor shall continue to protect such data in accordance with the terms of this Subcontract until such time it can reasonably return or securely dispose of such LLNS or Third-Party Data.

E. Subcontracting

1. The Subcontractor shall flow down these Cyber Security Provisions to all lower-tier subcontractors as necessary to ensure compliance with the terms contained herein.

2. The Subcontractor shall obtain written approval from the LLNS Contract Analyst prior to subcontracting any portion of the work that involves access to LLNS or Third-Party Data by the lower-tier subcontractor(s).

3. LLNS' consent to any such lower-tier subcontractor shall not relieve the Subcontractor of its representations, warranties, or obligations under this Subcontract.

4. The Subcontractor shall remain responsible and liable for any and all (i) performance required under the Subcontract, including proper supervision, coordination and performance of services; and (ii) acts and omissions of the Subcontractor's lower-tier subcontractors (including, such subcontractor's employees and agents, who, to the extent they are involved in performing under the Subcontract) to the same extent as if such acts or omissions were by the Subcontractor.

F. Indemnification

The Subcontractor shall indemnify, hold harmless, and defend Lawrence Livermore National Security, LLC and its members and affiliates and the U.S. Government, their officers, employees and agents from and against all claims, losses, damages and expenses of whatever kind including reasonable attorney's fees, incurred by LLNS arising from or relating to (A) any third party claims, suit or proceeding ("Third Party Claim") that arise out of these services or use of these services provided under this Subcontract ("Services") infringes or misappropriate such third party's intellectual property rights (patents, copyright, trade secret, trademark or other proprietary rights) or (B) any breach of confidentiality or data security arising from the Subcontractor's negligence in providing Services under this Subcontract.

If such Third Party claim is made or either party anticipates such a Third Party Claim will be made regarding potential infringement, LLNS agrees to permit the Subcontractor, when applicable and pursuant to mutual agreement between the parties, to (a) modify or replace the Services, or component or part thereof, to make it non-infringing, or (b) obtain the right for LLNS to continue use, or (c) in the event that the Subcontractor is unable or determines, in its reasonable judgment, that it is commercially unreasonable to do either of the aforementioned, Subcontractor shall refund to LLNS any prepaid fees for Services that have yet to be performed.

(END OF PROVISIONS)