



**Vendor Service Information Security Plan and
Federal/FedRAMP CONOPS**

Vendor Provider and Application
System Name
Evaluation Date:
COL:

Vendor Signature

| | |
|-----------|------------|
| Name | Title/Role |
| Email | Phone |
| Date | |
| Signature | |

LANL RLM

| | |
|-----------|------------|
| Name | Title/Role |
| Email | Phone |
| Date | |
| Signature | |

LANL ISSM

| | |
|-----------|------------|
| Name | Title/Role |
| Email | Phone |
| Date | |
| Signature | |

Optional

| | |
|-----------|------------|
| Name | Title/Role |
| Email | Phone |
| Date | |
| Signature | |

History of Changes

Note: Non-security significant or minor changes are indicated by version revisions, such as x.1, x.2, x.3, etc.
 Security-significant changes are indicated as major versions such as 1.x, 2.x, 3.x, etc.

| Version | Date | Page/Section(s) Changed | Summary of Changes (Table Head) | Responsible Person |
|------------------------|------|-------------------------|---------------------------------|--------------------|
| | | | | |
| | | | | |
| Major Revisions | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Template Revision History
 (to be completed by LANL CIO staff)

| Version | Date | Page/section(s) changed | Summary of changes | Responsible Person |
|---------|--------|-------------------------|--------------------|---------------------------------------|
| 1.0 | 2/2016 | Initial Edit | Initial Edit | Cody Jackson, OCIO, cjackson@lanl.gov |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Table of Contents

ISSM Instructions for Completing this Security Plan 3

Vendor Information (to be completed by LANL Assessor) 4

Application Information (to be completed by LANL Assessor) 4

Security Plan and Controls (to be completed by the Vendor) 6

Operations Controls 8

Attachments (Optional) 8

Appendix 9

ISSM Instructions for Completing this Security Plan

LANL has an obligation to ensure the security of its data. We are also required to ensure that our Federal security requirements “flow down” to vendors that process and/or store our data. This security plan is required for all vendors that have been deemed as having a FIPS 199 Low/Moderate Consequence of Loss by the LANL Information Security Site Manager (ISSM).

The security controls in this template can be traced back to standards such as SSAE-16, NIST SP 800-53 (FedRAMP), etc.

In many cases, LANL is requesting specific documentation as evidence. For example, if the vendor has an SSAE-16 compliant data center, then we will require a SOC Report (Type 1, 2, and/or 3). If you had a penetration test completed by a 3rd party organization, we would like a statement from that 3rd party organization. Note that we are not requesting the vendor to divulge specific information about vulnerabilities. For example, if the penetration test found that application Foo was not patched, which led to a “successful” penetration, we would not want that information. A simple summary stating that a penetration was conducted and that vulnerabilities were addressed and fixed is all we would need.

Likewise, in the security plan we are asking for internal documentation and descriptions of security functions. If the vendor already has these documented, then simply point to the documentation and include that documentation as an attachment to the plan. Many vendors have white papers or web pages devoted to explaining their security practices. If the vendor describes their data center security and disaster recovery plans on a web page, simply attach a PDF of that web page and reference it in the security plan.

If there is no control in place, it is appropriate to answer with “none,” which may not be a disqualifier. Some controls may not be applicable to your business or the manner in which LANL utilizes your service. However, if we see a critical control missing, this could imply that you are not able to meet our minimal standards for security. For example, if you store or process LANL personally identifiable information (PII) but do not protect it with complex passwords or encrypt it in transit, your ability to meet our security requirements would be questioned.

Lastly, each assessment has a LANL point of contact assigned to it. Please do not hesitate in reaching out to that person with questions or concerns. You may also reach out to the LANL Risk Assessment Team at RATeam@lanl.gov.

Vendor Information
(to be completed by LANL Assessor)

| |
|------------------|
| Vendor Name |
| Point of Contact |
| Email |
| Phone Number |
| URL |

Application Information
(to be completed by LANL Assessor)

| |
|--|
| Application |
| Description of service |
| LANL Customer and Organization |
| Purchase/IT Request Number |
| Data Owner Federal <input type="checkbox"/> LANS <input type="checkbox"/> WFO <input type="checkbox"/> Who? |
| Data Type LAUR <input type="checkbox"/> LACC <input type="checkbox"/> TSPA <input type="checkbox"/> Unclassified <input type="checkbox"/> CUI <input type="checkbox"/> ECI <input type="checkbox"/> OUO <input type="checkbox"/> UONI <input type="checkbox"/> NNPI <input type="checkbox"/> RSI <input type="checkbox"/> AT <input type="checkbox"/> LPI <input type="checkbox"/> |
| Is PII collected? Yes <input type="checkbox"/> No <input type="checkbox"/> If yes, What is collected? |

Privacy Threshold Analysis

| |
|---|
| <p>If any of the following statements are checked (yes), a Privacy Impact Assessment (PIA) is required:</p> <p><input type="checkbox"/> The system contains (collects and/or maintains), or plan to contain any information about individuals?</p> <p><input type="checkbox"/> The information is in an identifiable form.</p> <p><input type="checkbox"/> The information is about individual Members of the Public?</p> <p><input type="checkbox"/> The information is about DOE or contractor employees?</p> <p><input type="checkbox"/> PIA (Privacy Impact Analysis) Completion Date:</p> |
| <p>Privacy Health Information (PHI): Any information, whether oral or recorded in any form or medium, that</p> <ul style="list-style-type: none"> is created or received by a health care provider, health plan, public health authority, employer, life insurer, or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of any individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual. <p>PHI Yes <input type="checkbox"/> No <input type="checkbox"/></p> |
| <p>COL (Please refer to 1.0 COL Table)</p> |
| <p>Confidentiality L <input type="checkbox"/> M <input type="checkbox"/> H <input type="checkbox"/> Why?</p> |
| <p>Integrity L <input type="checkbox"/> M <input type="checkbox"/> H <input type="checkbox"/> Why?</p> |
| <p>Availability L <input type="checkbox"/> M <input type="checkbox"/> H <input type="checkbox"/> Why?</p> |

Exempt Yes No

Why?

- This is a posting of publicly-released information on web sites, wikis, databases, or Box-like systems?
Examples: Box, project wikis.
- This is a paid subscription or membership to commercial information feeds and services (including publishers, recruiting sites)
Examples: Newsfeeds, research feeds, one-way push of data to LANS – no data going out of LANS
- This is a text, audio, and/or video conferencing service used for non-CUI information
Example: WebEx
- This is an off-premises processing service for publicly released information for research or testing purposes
Example: Posting publicly available environmental data on a web site, using a cloud service to manipulate data from a public data source
- This is a data transmission service that includes telecommunications circuits & virtual circuits and message delivery services (e-mail and text messages). The internal systems that connect to these services and circuits have traditional ATO's that control the use of these connections, but the commercial transmission service is considered to be outside the perimeter and not part of a federal information system. Existing data transmission encryption requirements will continue to limit the exposure of information to these service providers.
Examples: email, VOIP, text messaging
- This service uses HPC resources and storage at other government-funded HPC sites

STOP—If it is exempt and Integrity and Availability are of no issue, the process is complete.

Is this an IT service? Yes No

STOP- If this is not an IT service this is the end of the form.

Is this service a cloud? (NIST 800-145 Cloud Characteristics) Yes No

Why?

What type of service

Infrastructure as a Service Platform as a Service Software as a Service

Other Describe:

Subject Matter Experts Consulted:

List Other DOE sites or Federal Agencies using this tool:

Is this service accredited in a Federal Manner? Yes No

If Yes: FedRAMP <https://www.fedramp.gov/>

GSA <http://www.digitalgov.gov/resources/negotiated-terms-of-service-agreements/>

Other? (SSAE-16, ISO/IEC 27001, etc.) Yes No

List:

If Yes, Categorization Level: Low Medium High

If No, is there a FedRAMP provider that offers this service? Yes No

If No, justification for not using a FedRAMP provider:

LANL Assessor Name and Contact Information:

Date of Assessment:

Security Plan and Controls
(to be completed by the Vendor)

In order to maintain compliance with Federal oversight and internal policies, LANL requires providers to provide security documentation to ensure a base level of security. If you have any documentation that covers the following questions please reference the documentation and attach it where applicable. This could include security white papers, reports, FAQs, etc.

| Data and Data Center Controls |
|--|
| Does the company maintain its own data center? Yes <input type="checkbox"/> No <input type="checkbox"/> If No, please provide the name of the company that does: |
| Where is the data center located (Country or US State)? |
| Is the data center a cloud provider (IaaS or PaaS such as AWS), comingled or unique? Yes <input type="checkbox"/> No <input type="checkbox"/> If yes please describe: |
| If the data center is provided by a third party do you have an SLA? Yes <input type="checkbox"/> No <input type="checkbox"/> If yes please describe: |
| Describe the Physical Access Control and Security of the Data Center (for example, badges, CCTV, security guards, etc.) |
| Is the data center SOC II/SAE 16 accredited? Yes <input type="checkbox"/> No <input type="checkbox"/> |
| Does it have any other security certifications? Yes <input type="checkbox"/> No <input type="checkbox"/> If yes please list: |
| Can LANL review any of the certifications or security documentation for the data center (for example, SOC reports, etc.)? |
| Does the data center conduct any penetration or vulnerability assessments either internal or external? Yes <input type="checkbox"/> No <input type="checkbox"/> If yes how often? Please share a brief overview of the results. (Specifics are not required. A general number of findings and/or verifications of corrective actions will suffice.) |
| Does the data center have a disaster recovery plan? Yes <input type="checkbox"/> No <input type="checkbox"/> If Yes, please describe it. If possible, please provide a copy of your DRP. If no, please describe any other compensatory measure. |
| How often do you exercise your contingency/ disaster recovery plan? |
| What types of data backup are performed and how often (tapes, D2D, hot mirroring, etc.)? |
| What is the guaranteed availability of the data center? |

Data Control

Describe the controls that will be used to segregate and protect LANL data.

Is the data encrypted at rest on the data center? Yes No
If yes what type of encryption? Is it FIPS 140-2 compliant?

Does LANL retain ownership of the data? Yes No

Describe media disposal, replacement and reuse policy.

Describe actions taken by provider, data center, and application tier manager to protect LANL data when the service is no longer offered or supported by provider.

Have there been any reportable incidents of data leakage, breach or other situations in the past 4 years?

Application Control

Describe the application level controls. (e.g., website is Verisign SSL HTTP secured, encrypted, security scans run daily, access controls defined by user groups, etc.)

Have there been any security assessments performed on the applications? Yes No
If yes can LANL review a summary of the results (Specifics are not required; a general number of findings and/or verifications of corrective actions will suffice.)

If no, can LANL perform a security assessment?

Has there been any penetration testing performed? Yes No
If yes, can LANL review a summary of the results? (Specifics are not required; a general number of findings and/or verifications of corrective actions will suffice.)

What type of security products does the Vendor utilize (e.g., IDS, IPS, firewall type, network captures, flow data, etc.)?

Does the provider have its own Security Operations Center (SOC)? Yes No
If no, who monitors, identifies, and investigates cyber security threats and vulnerabilities?

Describe the Incident Response procedure and alerting methodology:

How are security logs files generated, analyzed and used?

| Application Control (continued) |
|--|
| Is there any type of continuous monitoring plan? Yes <input type="checkbox"/> No <input type="checkbox"/> If yes, please describe. |
| What types of application testing and scanning are performed? |
| Do you have a formal code review for security? |
| What type of password policy can be enforced via application control for users? |
| Do you utilize multi factor authentication? Yes <input type="checkbox"/> No <input type="checkbox"/> If yes please describe |
| How do you protect against the OWASP Top 10 (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project)? |
| Do you have any other additional security practices or documentation that would be helpful? |

| Operations Controls |
|--|
| What is your internal password policy? |
| Do you perform background checks on your personnel? Yes <input type="checkbox"/> No <input type="checkbox"/> |
| How do you maintain least privileges amongst staff? |
| How do you handle separation of duties amongst staff? |
| Are there any customer security requirements that might flow down to LANL? (i.e., FedRAMP Customer Requirements Document, etc.) Yes <input type="checkbox"/> No <input type="checkbox"/> |

| Attachments (Optional) |
|--|
| Please list any attachments that might be addressed in the body of this plan. Examples include SOC Reports, Disaster Recovery Plans, 3rd Party Assessments, etc. |
| Attachment A |
| Attachment B |
| Attachment C |

Appendix

1. COL Table

| Security Objective | Potential Impact | | |
|---|--|---|---|
| | Low | Moderate | High |
| <p>Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.</p> | <p>The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</p> <p>Unclassified, non-sensitive information, publicly releasable information, etc.</p> | <p>The unauthorized disclosure of information could be expected to have a serious effect on organizational operations, organizational assets, or individuals.</p> <p>Unclassified but sensitive information, CUI, mandatory protected information, PII, UCNI, export controlled, etc.</p> | <p>The unauthorized disclosure of information could be expected to have a severe or catastrophic effect on organizational operations, organizational assets, or individuals.</p> <p>Any classified information</p> |
| <p>Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.</p> | <p>The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</p> <p>Generally the same as for confidentiality</p> | <p>The unauthorized modification or destruction of information could be expected to have a serious effect on organizational operations, organizational assets, or individuals.</p> <p>Generally the same as for confidentiality</p> | <p>The unauthorized modification or destruction of information could be expected to have a severe or catastrophic effect on organizational operations, organizational assets, or individuals.</p> <p>Generally the same as for confidentiality</p> |
| <p>Availability Ensuring timely and reliable access to and user of information.</p> | <p>The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</p> <p>The service or information can be unavailable for greater than 24 hours</p> | <p>The disruption of access to or use of information or an information system could be expected to have a serious effect on organizational operations, organizational assets, or individuals.</p> <p>The service or information can be unavailable for hours but beyond 24 hours impact to mission becomes an issue</p> | <p>The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic effect on organizational operations, organizational assets, or individuals.</p> <p>No tolerance for delay. Impact to mission occurs within seconds to minutes.</p> |

2. NIST 800-145 Cloud Characteristics

Found at <https://ocio.lanl.gov/RIA/RMFRIA/Cloud%20Repository/nistspecialpublication800-145.pdf>

Essential Characteristics:

- On-demand self-service.* A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
- Broad network access.* Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
- Resource pooling.* The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.
- Rapid elasticity.* Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
- Measured service.* Cloud systems automatically control and optimize resource use by leveraging a metering capability¹ at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.