Introduction

FedRAMP security control baselines specify control parameter requirements and organizational parameters specific to the provider's control implementation. Since certain controls may be required to govern agency user interaction, control organizational parameters may need to be included in the task order and specified. As an example, if a system needs to utilize SAML 2.0 architecture to integrate with an existing agency directory service for agency user account management and authentication, the contract clause should specify the required architecture from a consumer's perspective. However, the contract clauses should not govern how the provider's administrative end user accounts are managed or authenticated. The FedRAMP office suggests that agencies review the FedRAMP security control baseline, and that agencies do not contractually specify parameters for controls in the FedRAMP baseline, except from the perspective of a consumer's implementation of a control.

Additionally, Continuous Monitoring artifacts are identified within the FedRAMP Continuous Monitoring Strategy and Guide; and agencies should reference this guide when identifying any periodicity to their ongoing deliverable requirements.

Agencies should place agency specific requirements in the yellow highlighted portions of the sample template language provided below.

Specific Areas of Concern That Might Need Additional Contract Clauses

Data Jurisdiction

No FedRAMP controls govern data location; providers may describe boundaries that include foreign data centers. Agencies with specific data location requirements must include contractual requirements identifying where data-at-rest (primary and replicated storage) shall be stored.

> **Sample Template Language for Technical Requirements:**
> The vendor shall identify all data centers that the data at rest or data backup will reside. All data centers will be guaranteed to reside within [defined boundary / country / jurisdiction].
>
> The vendor shall provide a Wide Area Network (WAN), with a minimum of [#] data center facilities at [#] different geographic locations with at least [#] Internet Exchange Point (IXP) for each price offering. The vendor shall provide Internet bandwidth at the minimum of [#] GB.

FIPS 140-2 Validated Cryptography for Secure Communications

The FedRAMP security control baseline includes IA-7, SC-8(1), SC-9(1), SC-13, and SC-13(1) all of which require cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures. If agency requirements stipulate FIPS 140-2 validated cryptography be used from the agency to the cloud service provider, that should be specified.

> **Sample Template Language for Technical Requirements:**
> All deliverables shall be labeled [appropriate label such as "Controlled Unclassified Information" (CUI) or other agency selected designation per document sensitivity]. External transmission/dissemination

of [labeled deliverables] to or from a Government computer must be encrypted. Certified encryption modules must be used in accordance with [standard, such as FIPS PUB 140 (as amended), "Security requirements for Cryptographic Modules."]

AU-10(5): Non-Repudiation

The organizational parameter requires that cloud service providers implement FIPS 140-2 validated cryptography for digital signatures. If the agency has a requirement for integration with specific digital signature technologies, that should be included within the contract requirements.

Sample Template Language for Technical Requirements:

The vendor shall provide a system that implements [encryption standard] that provides for origin authentication, data integrity, and signer non-repudiation.

AU-11: Audit Record Retention

Agencies should consider the length of time they require Cloud Service Providers to retain audit records as part of their contracts with the CSP. The FedRAMP requirement is that the service provider retains audit records on-line for at least ninety days and further preserves audit records off-line for a period that is in accordance with NARA requirements.

Sample Template Language for Technical Requirements:

The vendor shall support a system in accordance with the requirement for Federal agencies to manage their electronic records in accordance with 36 CFR § 1236.20 & 1236.22 (ref. a), including **but not limited to** capabilities such as those identified in:

- DoD STD-5015.2 V3 (ref. b), Electronic Records Management Software Applications Design Criteria Standard,
- NARA Bulletin 2008-05, July 31, 2008, Guidance concerning the use of e-mail archiving applications to store e-mail (ref. c),
- NARA Bulletin 2010-05 September 08, 2010, Guidance on Managing Records in Cloud Computing Environments (ref 8).

These provide requirements for maintaining records to retain functionality and integrity throughout the records' full lifecycle including:

- Maintenance of links between records and metadata, and
- Categorization of records to manage retention and disposal, either through transfer of permanent records to NARA or deletion of temporary records in accordance with NARA-approved retention schedules.

IA-2(1), (2), (3) and (8): Identification and Authentication (Organizational Users) Multi-Factor Authentication

Cloud Service Providers pursuing a FedRAMP authorization will have to provide a mechanism for Government consuming end-users to utilize two-factor authentication. However, Agencies requiring a specific method of authentication, or integration with an existing agency system (such as a SAML 2.0 authentication to the agency's Identity Provider) must specify this requirement in their contract.

Sample Template Language for Technical Requirements:

The vendor shall support a secure, dual factor method of remote authentication and authorization to identified Government Administrators that will allow Government designated personnel the ability to perform management duties on the system.

The vendor shall support dual factor authentication including [specific method of authentication].

IA-8: Identification and Authentication (Non-Organizational Users)

Cloud Service Providers pursuing a FedRAMP authorization will have to provide multi-factor authentication for Provider's administrators.

Sample Template Language for Technical Requirements:

The vendor shall support a secure, dual factor method of remote authentication and authorization to identified Vendor Administrators that will allow vendor designated personnel the ability to perform management duties on the system.

IR-6: Incident Reporting Timeframes

FedRAMP parameters set compliance for Incident Reporting at the levels stipulated in NIST SP 800-61; and the JAB will require an Incident Reporting plan that complies with those requirements. Agency contracts should stipulate any specific incident reporting requirements including who and how to notify the agency.

Sample Template Language for Technical Requirements:

Cloud Service Providers are required to report all computer security incidents to the United States Computer Emergency Readiness Team (US-CERT) in accordance with US-CERT "Incident Categories and Reporting Timeframes" in , Appendix J, Table J-1 of NIST SP 800-61 (as amended), "Computer Security Incident Handling Guide." Any Category (CAT) 1, CAT 2, or CAT 3 incident, must be reported immediately to their Information Systems Security Officer (ISSO) and the Senior Agency Information Security Officer (SAISO). Any incident that involves compromised Personally Identifiable Information (PII) must be reported to US-CERT within 1 hour of detection regardless of the incident category reporting timeframe.

For further information, NIST published SP800-86 Guide to Integrating Forensic Techniques into Incident Response. SP800-86 defines in a much more precise and specific way the procedures, issues and technologies required to move an incident from the point of discovery all the way through to resolution.

MP-5(2) and (4): Media Transport

Sample Template Language for Technical Requirements:

The vendor shall document activities associated with the transport of Federal agency information stored on digital and non-digital media and employ cryptographic mechanisms to protect the confidentiality and integrity of this information during transport outside of controlled areas.

Digital media, containing Federal agency information, that is transported outside of controlled areas must be encrypted using a [encryption mode]; non-digital media including but not limited to CD-ROM, floppy disks, etc., must be secured using the same policies and procedures as paper.

Media, containing Federal Agency information that is transported outside of controlled areas must ensure accountability. This can be accomplished through [appropriate actions such as logging and a documented chain of custody form].

Federal Agency data that resides on mobile/portable devices (e.g., USB flash drives, external hard drives, and SD cards) must be encrypted using [encryption mode]. All Federal Agency data residing on laptop computing devices must be protected with approved encryption software.

PS-3: Personnel Screening

Since Joint Authorization Board (JAB) member agencies may not have contracts with CSP's achieving Provisional Authorizations, agencies should specify the level of Background Investigations that should be conducted, in accordance with OPM and OMB requirements. Agencies leveraging FedRAMP Provisional Authorizations will be responsible for conducting their own Background Investigations and or accepting reciprocity from other agencies that have implemented Cloud Service Provider systems. FedRAMP parameters set reinvestigation parameters as follows: moderate risk law enforcement and high impact public trust level, a reinvestigation is required during the 5th year. There is no reinvestigation for other moderate risk positions or any low risk positions. Agencies are responsible for the screening process, and may want to stipulate additional screening requirements.

Sample Template Language for Technical Requirements:

The vendor shall provide support personnel maintaining a NACI clearance or greater in accordance with OMB memorandum M-05-24, Section C (http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-24.pdf).

Vendor shall furnish documentation reflecting favorable adjudication of background investigations for all personnel supporting the system. Vendor shall comply with [agency directive on personnel screening]. [Agency] separates the risk levels for personnel working on Federal computer systems into [#] categories: [category descriptions]. In accordance with [agency directive on personnel screening], the cost of meeting all security requirements and maintaining assessment and authorization shall be [method of meeting cost].

- Those vendor personnel (hereafter known as "Applicant") determined to be in a [category of risk] will require a [level of clearance] investigation.
- [repeat for each category of risk]

The Contracting Officer, through the Contracting Officer's Technical Representative or Program Manager will ensure that all required information is forwarded to the Federal Protective Service (FPS) in accordance with the [Agency processes]. FPS will then contact each Applicant with instructions for completing required forms and releases for the particular type of personnel investigation requested.

Optional Additional Sample Template Language for Technical Requirements:
Applicants will not be reinvestigated if a prior favorable adjudication is on file with FPS or [agency], there has been less than a one year break in service, and the position is identified at the same or lower risk level.

Once a favorable FBI Criminal History Check (Fingerprint Check) has been returned, Applicants may receive an [agency] identity credential (if required) and initial access to [agency] information systems. The HSPD-12 Handbook contains procedures for obtaining identity credentials and access to [agency] information systems as well as procedures to be followed in case of unfavorable adjudications.

SC-7(1) - Boundary Protection (TIC)

Cloud Service Providers pursuing a FedRAMP authorization will have to provide boundary protection in accordance with SC-7; however, if the Agency data assets require utilization of a Trusted Internet Connection, the Agency must include requirements for data routing within their contract.

Sample Template Language for Technical Requirements:
The vendor shall ensure that Federal information, other than unrestricted information, being transmitted from Federal government entities to external entities using cloud services is inspected by Trusted Internet Connections (TIC) processes.

Or

The vendor shall route all external connections through a Trusted Internet Connection (TIC).

SC-28 - Protection of Information At Rest

Cloud Service Providers pursuing a FedRAMP authorization will have to support the capability to encrypt data-at-rest; however, contract clauses should indicate any specific agency requirements for data encryption.

Sample Template Language for Technical Requirements:
The Quoter shall provide security mechanisms for handling data at rest and in transit in accordance with [encryption standard].

SI-5 - Security Alerts, Advisories, and Directives

Cloud Service Providers are required to include FedRAMP personnel in the list of personnel required to receive alerts, advisories and directives; if an agency elects to include their own SOC or security personnel in alerts, an agency should include a contract clause.

Sample Template Language for Technical Requirements:

The vendor shall provide a list of their personnel, identified by name and role, with system administration, monitoring, and/or security responsibilities that are to receive security alerts, advisories, and directives. This list shall include [designated government personnel].