FedRAMP CONTROL SPECIFIC CONTRACT CLAUSES

Version 3.0

December 8, 2017

FedRAMP

EXECUTIVE SUMMARY

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.

DOCUMENT REVISION HISTORY

DATE	VERSION	PAGE(S)	DESCRIPTION	AUTHOR
06/06/2014	1.0	All	Major revision for SP800-53 Revision 4. Includes new template and formatting changes.	FedRAMP PMO
06/06/2017	2.0	All	Updated logo	FedRAMP PMO
12/08/2017	3.0	All	Updated to newest template	FedRAMP PMO

ABOUT THIS DOCUMENT

This document provides guidance on contractual language that might be used for FedRAMP cloud computing projects.

WHO SHOULD USE THIS DOCUMENT?

This document is directed at acquisition and contracting personnel who might need to negotiate specific contractual language for contracts involving cloud computing

HOW THIS DOCUMENT IS ORGANIZED

This document has one primary section:

Section 1 – Specific areas of concern that might need additional contract clauses.

Appendix A – Table of Acronyms.

HOW TO CONTACT US

Questions about FedRAMP or this document should be directed to info@fedramp.gov.

For more information about FedRAMP, visit the website at http://www.fedramp.gov.

TABLE OF CONTENTS

I. INTRODUCTION AND PURPOSE

1.1. PURPOSE

1.2. APPLICABLE LAWS AND REGULATIONS

- Computer Fraud and Abuse Act [PL 99-474, 18 USC 1030]
- E-Authentication Guidance for Federal Agencies [OMB M-04-04]
- Federal Information Security Management Act (FISMA) of 2002 [Title III, PL 107-347]
- Freedom of Information Act As Amended in 2002 [PL 104-232, 5 USC 552]
- Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy [OMB M-01-05]
- Homeland Security Presidential Directive-7, Critical Infrastructure Identification, Prioritization and Protection [HSPD-7]
- Internal Control Systems [OMB Circular A-123]
- Management of Federal Information Resources [OMB Circular A-130]
- Management's Responsibility for Internal Control [OMB Circular A-123, Revised 12/21/2004]
- Privacy Act of 1974 as amended [5 USC 552a]
- Protection of Sensitive Agency Information [OMB M-06-16]
- Records Management by Federal Agencies [44 USC 31]
- Responsibilities for the Maintenance of Records About Individuals by Federal Agencies [OMB Circular A-108, as amended]
- Security of Federal Automated Information Systems [OMB Circular A-130, Appendix III]

1.3. APPLICABLE STANDARDS AND GUIDANCE

- A NIST Definition of Cloud Computing [NIST SP 800-145]
- Computer Security Incident Handling Guide [NIST SP 800—61, Revision 2]
- Contingency Planning Guide for Federal Information Systems [NIST SP 800-34, Revision 1]
- Engineering Principles for Information Technology Security (A Baseline for Achieving Security) [NIST SP 800-27, Revision A]
- Guide for Assessing the Security Controls in Federal Information Systems [NIST SP 800-53A]
- Guide for Developing Security Plans for Federal Information Systems [NIST SP 800-18, Guide to Understanding FedRAMP Version 1.2, April 22, 2013 Page 12 Revision 1]
- Guide for Developing the Risk Management Framework to Federal Information Systems:
- A Security Life Cycle Approach [NIST SP 800-37, Revision 1] Guide for Mapping Types of Information and Information Systems to Security Categories [NIST SP 800-60, Revision 1]
- Guide for Security-Focused Configuration Management of Information Systems [NIST SP 800-128]
- Information Security Continuous Monitoring for Federal Information Systems and Organizations [NIST SP 800-137]
- Managing Information Security Risk [NIST SP 800-39]
- Minimum Security Requirements for Federal Information and Information Systems [FIPS Publication 200]

- Personal Identity Verification (PIV) of Federal Employees and Contractors [FIPS Publication 201-1]
- Recommended Security Controls for Federal Information Systems [NIST SP 800-53, Revision 4]
- Risk Management Guide for Information Technology Systems [NIST SP 800-30]
- Security Considerations in the System Development Life Cycle [NIST SP 800-64, Revision 2]
- Security Requirements for Cryptographic Modules [FIPS Publication 140-2]
- Standards for Security Categorization of Federal Information and Information Systems [FIPS Publication 199]
- Technical Guide to Information Security Testing and Assessment [NIST SP 800-115]

1.4. FEDRAMP REQUIREMENTS AND GUIDANCE

All FedRAMP documents are available at www.fedramp.gov

- FedRAMP Incident Communications Procedure
- FedRAMP Continuous Monitoring Strategy and Guide
- Guide to Understanding FedRAMP

2. SPECIFIC AREAS OF CONCERN THAT MIGHT NEED ADDITIONAL CONTRACT CLAUSES

2.1. DATA JURISDICTION

No NIST SP 800-53 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.

2.2. 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, including which level (1-4) of FIPS 140-2 validation is required.

Sample Template Language for Technical Requirements:

The vendor shall use only cryptographic mechanisms that comply with [FIPS 140-2 level # or other approved mechanism]

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 140-2 (as amended), "Security requirements for Cryptographic Modules."]

2.3. 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. If the agency has a requirement for FIPS 140-2 encryption, that should be specified, including which level (1-4) of FIPS 140-2 encryption is required.

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.

2.4. AU-11: AUDIT RECORD RETENTION

Agencies should consider the length of time they require Cloud Service Providers (CSP) 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.

2.5. 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 use multi-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. In accordance with Homeland Security Presidential Directive 12 (HSPD-12), agencies should consider specific requirements to support PIV/CAC cards.

Sample Template Language for Technical Requirements:

The vendor shall support a secure, multi-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 multi-factor authentication including [specific method of authentication].

2.6. 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, multi-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.

2.7. IR-6: INCIDENT REPORTING TIMEFRAMES

FedRAMP parameters set compliance for Incident Reporting at the levels stipulated in NIST SP 800-61; and the Authorizing Officials (AO) 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), 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.

2.8. 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 FIPS 140-2 level 2 [or other approved 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 NIST-approved encryption software.

2.9. PS-3: PERSONNEL SCREENING

Federal agencies are responsible for the level of Background Investigations that should be conducted in accordance with OPM and OMB requirements. As a note, the Joint Authorization Board (JAB) does not have contracts with CSP's achieving Provisional Authorizations and therefore does not provide background investigations for CSPs seeking a Provisional Authorization. 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 who are U.S. persons 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.

2.10. 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).

2.11. 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].

2.12. 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].

APPENDIX A: FedRAMP ACRONYMS

The master list of FedRAMP acronym and glossary definitions for all FedRAMP templates is available on the FedRAMP website Documents page under Program Overview Documents.

(https://www.fedramp.gov/resources/documents-2016/)

Please send suggestions about corrections, additions, or deletions to info@fedramp.gov.