FedRAMP Requirements for Validated Cryptographic Modules

A White Paper from SafeLogic and Coalfire

SafeLogic Inc.

530 Lytton Ave, Suite 200

Palo Alto, CA 94301

www.SafeLogic.com

Executive Summary

The U.S. Federal Risk and Authorization Management Program (FedRAMP), like so many other U.S. federal technology governance requirements, is tied directly to the frameworks established by the National Institute of Standards and Technology (NIST). In particular, NIST's Special Publication (SP) 800-53 is relied upon for best practices in federal information systems and organizations. Now in its fourth revision, SP 800-53's security controls and associated assessment procedures are the basis for the Federal Information Security Management Act (FISMA) of 2002 and drive many of the industry's federal prerequisite initiatives. FedRAMP's stated goal of enabling "agencies to rapidly adapt from old, insecure legacy IT to mission-enabling, secure, and cost effective Cloud-based IT" can be more bluntly interpreted as "clarifying 800-53 controls for Cloud deployment."

With that in mind, this document was jointly developed by SafeLogic and Coalfire to answer persistent questions about one niche area - validated encryption as a prerequisite for FedRAMP authorization. We will highlight cryptographic requirements as noted in the FedRAMP Security Controls Baselines, mapped to NIST SP 800-53 (rev. 4), and governed by NIST's FIPS 140-2 standards, an often-misunderstood but key building block of the U.S. federal mandates for deployed technology.

Table of Contents

1 FedRAMP Overview

The U.S. Federal Risk and Authorization Management Program (FedRAMP) was created to provide a standardized approach for assessing, monitoring, and authorizing Cloud computing products and services under the Federal Information Security Management Act (FISMA), and to promote an accelerated adoption of secure Cloud solutions by federal agencies. By standardizing the approach, disparate agencies could reap the benefits of selecting products from a pool of already-vetted Cloud solutions, accelerating deployment and simplifying the process.

FedRAMP authorization requires that the Agencies and Cloud Service Providers supply written technical evidence of security compliance to their selected Third Party Assessment Organizations (3PAO) using a series of program authorized templates. This process is required for the Full Security Assessment (phase 2 of 4) and the Continuous Monitoring (phase 4 of 4) to maintain the FedRAMP authorization for continued operation.

In the document phase of this FedRAMP assessment process, one of the most crucial documents is the system specific instance of the *FedRAMP High/Moderate/Low System Security Plan* or SSP. Each intended FedRAMP product has its own SSP that contains technical details about the specific Agency/CSP system under assessment. The SSP and the supplemental attachments inform the assessors and other FedRAMP entities about the technical security plan for the new system. Current FedRAMP documentation templates may be found at (https://www.fedramp.gov/templates/).

These documentation efforts are all completed upon the baseline controls for the appropriate FedRAMP level – High, Moderate, Low, or Tailored, also known as Low Impact SaaS. We will discuss these baselines – and the encryption requirements contained within them – in the next section.

2 FedRAMP Security Controls Baselines

The security controls, enhancements, parameters, requirements, and guidance listed in the FedRAMP System Security Plan (SSP) templates are for Cloud systems designated at the low, moderate, and high impact information systems as defined in the Federal Information Processing Standards (FIPS) Publication 199 and are then arranged in tiers based upon the four FedRAMP Security Controls Baselines – Tailored, known as Low Impact Software as a Service (LI-SaaS), Low, Moderate, and High.

The security controls and enhancements have been selected from the NIST SP 800-53 Revision 4 catalog of controls by the FedRAMP Joint Authorization Board (JAB) based on the FedRAMP Program Management Office (PMO) analysis. The JAB then layered additional guidance and requirements around these controls. The controls were selected to address the unique risks of Cloud computing environments, including but not limited to: multi-tenancy, visibility, control/responsibility, shared resource pooling, and trust.

Federal Agencies and their providers - Cloud Service Providers (CSPs) and Independent Software Vendors (ISVs) – are mandated to implement these security controls, enhancements, parameters, and requirements to satisfy the unique requirements of Cloud computing for the Federal Government. They are organized into seventeen (17) control families and each increasing level adds to the controls required for from the lower security control baseline. You will note the sheer number of controls that have been mapped from NIST 800-53 to FedRAMP in the table below, organized by control family and FedRAMP baseline level.

Number of Controls Per Family by Security Baseline Level				
Control Family	**LI SaaS**	**Low**	**Moderate**	**High**
Access Control	9	11	43	54
Awareness Training	4	4	5	7
Audit and Accountability	8	10	19	31
Security Assessment and Authorization	8	8	15	16
Configuration Management	6	8	26	36
Contingency Planning	2	6	24	35
Identification and Authentication	15	15	27	31
Incident Response	8	7	18	26
Maintenance	4	4	11	14
Media Protection	4	4	10	12
Physical and Environmental Protection	10	10	20	27
Planning	3	3	6	6
Personnel Security	8	8	9	10
Risk Assessment	4	4	10	12
System and Services Acquisition	7	6	22	26
System and Communications Protection	9	10	32	39
System and Information Integrity	6	7	28	39
Total	**115**	**125**	**325**	**421**

Number of Controls Per Family by Security Baseline Level

3 Encryption Controls in FedRAMP

Limiting our discussion to the cryptographic requirements and other security requirements affected by encryption in FedRAMP, there are three (3) critical controls that have been mapped from NIST 800-53 that are required at every FedRAMP baseline and in which encryption is addressed.

FedRAMP is designed for federal agency procurement streamlining, so the encryption requirements conform to federal mandates. Specifically, NIST controls across their publications always reference the NIST standards written for cryptography – Federal Information Processing Standard 140, now in the second revision, FIPS 140-2. This states that in all cases, if encryption is employed as a mechanism to meet a security requirement, it must be FIPS 140-2 validated under the Cryptographic Module Validation Program (CMVP).

Let's look at these three critical controls, organized by family and including the notes from FedRAMP, before covering FIPS 140-2 in more detail.

3.1 Identification and Authentication

IA-7 Cryptographic Module Authentication

> The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.
>
> Supplemental Guidance: Authentication mechanisms may be required within a cryptographic module to authenticate an operator accessing the module and to verify that the operator is authorized to assume the requested role and perform services within that role.
>
> Related controls: SC-12, SC-13.
>
> Control Enhancements: None.
>
> References: FIPS Publication 140; Web:https://csrc.nist.gov/projects/cryptographic-module-validation-program.

To interpret that, the cryptographic module within the information system must implement authentication mechanisms (i.e., role-based or identity-based) to control access to the cryptographic module. Since this requirement applies to all federal systems with a security categorization of 'Low" or higher, according to FISMA, this requirement applies to all federal systems. Note both the reference to SC-12 and SC-13, the other two critical controls to be covered in this paper, and FIPS Publication 140.

3.2 System and Communications Protection

SC-12 Cryptographic Key Establishment and Management

> The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].
>
> Supplemental Guidance: Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. Organizations define key management requirements in accordance with applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance, specifying appropriate options, levels, and parameters. Organizations manage trust stores to ensure that only approved trust anchors are in such trust stores. This includes certificates with visibility external to organizational information systems and certificates related to the internal operations of systems.
>
> Related controls: SC-13, SC-17.
>
> References: NIST Special Publications 800-56, 800-57.

SC-12 echoes IA-7's demand for "accordance with applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance", which in the public sector includes FIPS 140-2 validation for any cryptography in use. Note also the persisted reference to SC-13.

The "Assignment" caveat in brackets refers to the ability of the organization to select the benchmark for compliance. For FedRAMP Moderate and High baseline levels, SC-12 (2) is invoked, which narrows this election to NIST FIPS-compliant or NSA-approved, but even at the Low or Tailored levels, deploying anything other than FIPS 140-2 validated encryption will trigger additional scrutiny and may impede deployment in federal agencies.

SC-13 Cryptographic Protection

> The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.
>
> Supplemental Guidance: Cryptography can be employed to support a variety of security solutions including, for example, the protection of classified and Controlled Unclassified Information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals. Cryptography can also be used to support random number generation and hash generation. Generally applicable cryptographic standards include FIPS-validated cryptography and

> NSA-approved cryptography. This control does not impose any requirements on organizations to use cryptography. However, if cryptography is required based on the selection of other security controls, organizations define each type of cryptographic use and the type of cryptography required (e.g., protection of classified information: NSA-approved cryptography; provision of digital signatures: FIPS-validated cryptography).
>
> Related controls: AC-2, AC-3, AC-7, AC-17, AC-18, AU-9, AU-10, CM-11, CP-9, IA-3, IA-7, MA-4, MP-2, MP-4, MP-5, SA-4, SC-8, SC-12, SC-28, SI-7.
>
> References: FIPS Publication 140

SC-13 is interesting in that it states explicitly a loophole that has been (unsuccessfully) noticed by many software vendors – "This control does not impose any requirements on organizations to use cryptography." You would not be the first to try to pursue this path to avoid cryptographic module validation, but you would probably be the first to succeed. Federal agencies are not reassured if you insist that the benchmark is not applicable. They want to know how you plan to protect classified and controlled unclassified information (CUI) through proven means other than cryptography.

Note the number of related controls – they all depend on SC-13 to impose the mandate, not to have to use cryptography, but when it is in use, to comply with the required level of cryptography for the use case.

NSA-approved cryptography comes in two flavors. Suite A, which is a classified collection of classified cryptographic algorithms, is not available for vendors. Suite B is the set of algorithms that would be applicable and overlaps with FIPS 140-2. The AES 256 algorithm will be the workhorse in either scheme and should be validated by Cryptographic Algorithm Validation Program (CAVP) in any scenario. It has been strongly discouraged to use any NSA ciphers that are not also included in FIPS 140-2 testing after the criticism of Simon and Speck, two algorithms famously released by the NSA in 2013 and rejected by ISO and other standards. In addition, as mentioned throughout this document, FedRAMP's role in translating SP 800-53 for the Cloud does not change the fact that it was originally written by NIST and they rightfully stack their standards. SP 800-53 was written with every intention to refer cryptography controls to their cryptography standards document. You can never go wrong with FIPS 140-2 validated encryption in federal government deployments or when satisfying NIST requirements.

4 FIPS 140-2 Overview

NIST realized that standards must be written specifically to govern the use of cryptography in order to support the framework of various other publications and standards in use. Originally issued in 1994, FIPS 140 sought to achieve two goals – first, to explicitly mandate the use of validated cryptography in the federal government, and second, to codify the benchmark and methodology for that validation effort. An update, represented by the "-2" suffix, was instituted in 2001 and has remained in active use ever since.

The validation process requires an independently accredited laboratory, similar to the role of the 3PAO in FedRAMP, to test and verify the functionality in the cryptographic module in question. The lab is responsible for algorithm testing, conducted in partnership with the CAVP, then testing and submitting the paperwork on the module to the CMVP office, and coordinating the finalization of the certification. The CAVP and CMVP are operated in a joint effort between NIST and Canada's counterpart, the Communications Security Establishment (CSE). The labs themselves can be located anywhere in the world and are certified for this role via the National Voluntary Laboratory Accreditation Program (NVLAP) to complete the alphabet soup of oversight entities.

One of the more famous tenets of FIPS 140-2 states in very blunt language that the U.S. federal government will treat any encryption that has not been validated by CMVP to be the same as no encryption at all. Essentially, NIST cannot guarantee any efficacy when the module itself is an unknown implementation of unknown strength.

"Cryptographic keys and CSPs[1] encrypted using a non-Approved algorithm or proprietary algorithm or method are considered in plaintext form, within the scope of this standard."

Following the successful implementation of the FIPS 140-2 mandate in U.S. federal government, many sovereign nations have instituted their own requirements, often still referencing or relying upon validation by CMVP. In addition, regulated industries such as finance, utilities, legal, and healthcare have increased their reliance upon the benchmark, as it becomes table stakes for encryption around the world.

[1] Just to make it more complicated, a CSP in FIPS 140-2 is a "Critical Security Parameter", not to be confused with the "Cloud Service Provider" in FedRAMP.

5 Strategic Guidance

5.1 Conclusion

While NIST SP 800-53 includes a variety of controls that include guidance for cryptographic implementations (see matrix below for FISMA categorization, for example), FedRAMP has streamlined the baseline controls to address the unique elements of Cloud computing. In this document, we have focused on the three controls that are explicit and required for all four baseline levels in the FedRAMP program. They are straightforward and consistent, and while Moderate and High FedRAMP levels may mandate more controls, the encryption requirements will always be referenced back to the same FIPS 140-2 validated module that would have been implemented at the Low or Tailored level. Essentially, it is a single checkmark that will be needed for any and all levels of FedRAMP and will be portable if the CSP wishes to undertake an upgrade in baseline level.

Requirement	Security Categorization			
	Low	Moderate	High	Enhanced
Encryption				
IA-7	✓	✓	✓	✓
SC-13	✓	✓	✓	✓
SA-4 (7)				✓
Data at Rest				
SC-28 (1)				✓
AU-9 (3)				✓
MP-4 (1)				✓
Data in Transmission				
MP-5 (4)		✓	✓	✓
SC-8 (1)		✓	✓	✓
SC-9 (1)		✓	✓	✓
AC-17 (2)		✓	✓	✓
Access Control				
AC-3 (6)				✓
MP-2 (2)				✓
Identification & Authentication				
AC-18 (1)		✓	✓	✓
IA-3 (1) (2)				✓
MP-4 (6)				✓
Non-Repudiation				
AU-10 (5)				✓

FISMA Controls Mapped from NIST SP 800-53 Cryptographic Requirements

Keep in mind that it is NIST that wrote both SP 800-53, upon which FedRAMP is based, and FIPS 140-2. It is no great surprise that one relies upon the other. In order to streamline FedRAMP efforts, it is strongly suggested to procure a FIPS 140-2 compliant module and commence immediately with the validation process. By completing both in parallel, overlapping requirements can be addressed and shared resources can contribute to both efforts.

Note that there is push-to-start availability for FIPS 140-2 that offloads both the engineering and documentation overhead, and saves significant time and costs as well. Keep reading for more about this avenue for FIPS 140-2 validation.

In addition, by engaging an expert advisor for FedRAMP, many redundant efforts can be consolidated and costly pitfalls can be avoided. When certification is the only hurdle standing between your product and federal procurement, every minute is extremely valuable. Please contact SafeLogic and Coalfire immediately to learn more about how quickly you can complete these requirements and begin competing for federal contracts!

5.2 About SafeLogic

Any CSP that wishes to deploy in the U.S. public sector needs to receive a FedRAMP ATO. In fact, if other federal technology assurance programs are any indication, FedRAMP will soon be table stakes for Cloud deployments in governments around the world, as well as regulated industries such as utilities, finance, legal, and healthcare. To meet the FedRAMP requirements shown in this document, the CSP must leverage a validated cryptographic module. This is where the layered requirements begin to get challenging for many software vendors.

Luckily, SafeLogic's CryptoComply meets all FIPS 140-2 standards and has already been validated by the CMVP. By extension, CryptoComply meets and surpasses all FedRAMP standards for cryptography. When a CSP implements a SafeLogic cryptographic module, they are immediately satisfying the NIST SP 800-53 controls and meeting both FedRAMP and FISMA minimums. They are also able to leverage the niche expertise of the SafeLogic team to receive their own validation.

FIPS 140-2 validation traditionally took 8-12 months and significant engineering overhead. Furthermore, the validation boundary was typically set too wide, setting the team up for certain failure and required re-validation when patches would inevitably be needed. Re-validation would begin the clock again in another frustrating cycle.

Instead, SafeLogic modules include RapidCert, the industry's only FIPS 140-2 validation service that provides a certificate in the customer's name, while drastically accelerating the timeline, requiring no additional engineering effort, zero interaction with testing labs, and at a fixed cost. By providing the software and service in tandem, SafeLogic is able to reduce the validation timeline down to 8 weeks, often less, and can be completed in parallel with FedRAMP efforts with no internal resources required. SafeLogic then maintains the module and FIPS 140-2 certificate to guarantee perpetual compliance for the client.

SafeLogic was established in 2012 and focused on standards-based cryptographic engines, fully validated to FIPS 140-2 standards and maintained to ensure ongoing compliance. The modules are built to offer drop-in compatibility for the most popular open source modules used in non-FIPS environments and a variety of connectors to accommodate unique product architecture, including Cloud deployments.

Contact SafeLogic directly to learn more and establish compatibility for your solution.

5.3 About Coalfire

Coalfire is the cybersecurity advisor that helps private and public sector organizations avert threats, close gaps, and effectively manage risk. By providing independent and tailored advice, assessments, technical testing, and cyber engineering services, we help clients develop scalable programs that improve their security posture, achieve their business objectives, and fuel their continued success. As the leading FedRAMP 3PAO, Coalfire provides FedRAMP advisory and assessment services to CSPs. Having completed more than 80 assessments for CSPs, Coalfire has helped more systems attain an Authority to Operate (ATO) than any other 3PAO.

Coalfire teams are highly experienced and well versed in NIST 800-53 and Department of Defense requirements and how they relate to commercial cloud environments. To address these requirements, Coalfire has developed services to help CSPs cost-effectively prepare for their pursuit of a FedRAMP ATO:

- FedRAMP Readiness Assessment – By conducting the required Readiness Capabilities Assessment, Coalfire helps CSPs determine their clouds' readiness for the full FedRAMP assessment.
- Advisory services – Our experts advise on system architecture, security control implementations, and documentation, including SSPs, policies, and procedures.
- Assessment – Coalfire develops the required FedRAMP documentation, including a security assessment plan (SAP), security requirements traceability matrix (SRTM), security assessment report (SAR), and recommendations for authorization.
- Continuous monitoring – To help CSPs maintain their ATOs, Coalfire assists with any monthly, quarterly, or annual continuous monitoring.

Contact Coalfire directly to learn more about our FedRAMP advisory and assessment services.

5.4 Contact

SafeLogic Inc.
530 Lytton Ave, Suite 200
Palo Alto, CA 94301

(844) 4-ENCRYPTION

www.SafeLogic.com
www.Twitter.com/SafeLogic

Coalfire
11000 Westmoor Circle, Suite 450
Westminster, CO 80021

(877) 224-8077

www.Coalfire.com
www.Twitter.com/CoalfireSys

5.5 Acronym and Abbreviation Listing

Acronym / Abbreviation	Definition
3PAO	Third Party Assessment Organizations
AES	Advanced Encryption Standard
ATO	Authorization to Operate
CAVP	Cryptographic Algorithm Validation Program
CMVP	Cryptographic Module Validation Program
CSP (used in FedRAMP)	Cloud Service Provider
CSP (used in FIPS 140-2)	Critical Security Parameter
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act of 2002
JAB	Joint Authorization Board
NIST	National Institute of Standards and Technology
SP	Special Publication
SSP	System Security Plan