FedRAMP Policy for Cryptographic Module Selection and Use

APPROVED BY THE FEDRAMP BOARD

January 16, 2025

APPLICABILITY

This policy defines requirements and recommendations for the following parties:

- **Cloud service providers (CSPs)** who participate or want to participate in the FedRAMP marketplace
- **Independent assessors (IAs)** perform third-party cybersecurity assessments for cloud service offerings (CSOs) through their FedRAMP packages. IAs conduct both initial and periodic evaluations of CSOs to ensure they comply with federal security requirements. IAs are also known as *third-party assessment organizations (3PAOs)*.
- **FedRAMP designated leads** are federal agencies responsible for sponsoring CSPs for FedRAMP authorization. A designated lead can be:
    - An authorizing official at a federal agency; or
    - The FedRAMP Director at GSA in the case of a program-sponsored authorization.
- **Reviewers of FedRAMP packages** may include FedRAMP's own reviewers and/or package review teams from FedRAMP designated leads.

Section 3 of this policy is normative. The rest of this policy is informative. This policy is effective immediately.

FEEDBACK

Suggestions for improving the policy are welcome anytime through the feedback form at https://www.fedramp.gov/documents-templates/.

1. Policy Overview

When protecting federal information systems ("systems") and information ("data")[1], Federal agencies are required[2] to use cryptographic modules that have been validated by NIST's Cryptographic Algorithm Validation Program (CAVP) as complying with the Federal Information Processing Standard (FIPS) 140.

Federal agencies are also required to patch or update their software in order to protect federal systems and information. Sources of these requirements include Cybersecurity Directives from the Cybersecurity and Infrastructure Security Agency (CISA), and FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems* from NIST.

FedRAMP works primarily with commercially operated cloud service providers (CSPs) and is responsible for reviewing the security of those providers' cloud service offerings (CSOs) to meet the expectations of federal agencies. As a result, the FedRAMP process is responsible for applying the goals and requirements of the federal government into environments that are often operated very differently from those of many federal agencies.

This policy uses two terms related to acquiring patches and updates. These streams are used in practice to deliver updated software cryptographic modules:

- An ***update stream*** contains the latest patches and updates to be applied to software, regardless of the FIPS-validation status of the changed software.
- A ***validation module stream*** contains the latest FIPS-validated patches and updates to be applied to software, whether or not more recent, unvalidated patches or updates exist.

Sometimes it is not possible to meet requirements for both using FIPS-validated modules and using software without known vulnerabilities at the same time. In such situations, FedRAMP generally prefers the elimination of known vulnerabilities through patches or updates (update stream usage) over continuing to use known-vulnerable software that is FIPS-validated (validated module stream usage).

The presence of known vulnerabilities can create risks that outweigh the assurance value provided through validation, especially if the modules being patched or updated were FIPS-validated. This policy sets the expectation that CSPs will choose to use either update streams or validated module streams since switching between these approaches is difficult and costly.

For this reason, update streams are encouraged by this policy to ensure that remedies for known vulnerabilities are deployed quickly and that use of effective cryptography is encouraged where it is needed.

[1] OMB Circular A-130, "Managing Information as a Strategic Resource" defines *federal information system* as "an information system used or operated by an agency or by a contractor of an agency or by another organization on behalf of an agency" and *federal information* as "information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government, in any medium or form."

[2] https://csrc.nist.gov/projects/fips-140-3-transition-effort

2. Background

Cryptography is the science of information hiding and verification. It includes the protocols, algorithms, and methodologies to securely and consistently prevent unauthorized access to sensitive information and enable verifiability of the information. The main goals include ensuring confidentiality and integrity. Cryptography is critical to protecting cloud-based information systems and their information. Cryptographic algorithms are the basis of technologies that provide foundational security and privacy guarantees in modern systems, including encryption, digital signing, one-way hashing, privacy-enhancing technologies, and other security capabilities.

Cryptographic modules are hardware and software (including firmware) that implement security functions, including cryptographic algorithms and key generation, which are contained within a cryptographic boundary[3]. The cryptographic boundary differentiates functionality that is contained within the module and functionality that is provided outside the module. Cryptographic modules can be, or be part of, open-source and proprietary software libraries, hardware security modules, on-device secure enclaves, or any other form of software or special-purpose hardware that can execute cryptographic algorithms.

FedRAMP is focused on the effective and transparent management of risk. Considering only the FIPS-validation status of a cryptographic module used by a product or service fails to take into account the larger risk picture based on how the module is used within the system (such as for an identity provider service or a cloud storage system versus a user endpoint), what functions it performs, what data is involved (including its sensitivity and the amount of data), and what known vulnerabilities exist in the module. For example, new vulnerabilities are discovered in software with FIPS-validated cryptographic modules from time to time. Federal agencies would need to patch or update the software to a FIPS-validated version – but such a version might not exist yet.

FedRAMP needs to have a dedicated policy for how cryptographic module requirements will be applied in the context of managing and maintaining a system, as:

- Many CSPs operate their software and security architecture using DevSecOps-based approaches that prioritize rapid patching and security feature development. These are security practices with positive security outcomes that are in federal agencies' interest to enable and incentivize in the services on which they rely and FedRAMP should not discourage them. FedRAMP should especially avoid unintentionally creating pressures on CSPs and agencies to rely on known-vulnerable software.

- Most commercially operated CSPs in the FedRAMP marketplace serve a mix of government and non-government customers. Even when a CSP operates a government-focused instance of their service, this instance may share much of the same underlying software and hardware as other commercially-focused instances. This introduces complexity when different cryptographic modules, security functions, and algorithms are needed for different customer types. FedRAMP needs to enforce federal cryptographic standards in a way that does not require more complexity than is

[3] Federal Information Processing Standard (FIPS) 140 refers to ISO/IEC 19790:2012, "Information technology – Security techniques – Security requirements for cryptographic modules" for more information on cryptographic boundaries. ISO/IEC 19790 defines a cryptographic boundary as an "explicitly defined continuous perimeter that establishes the physical and/or logical bounds of a cryptographic module and contains all the hardware, software, and/or firmware components of a cryptographic module."

necessary and that will reduce the need for government-focused cloud instances to the greatest degree possible.

- CSPs typically need to rely on server-side enforcement of cryptographic requirements to protect communications because requirement enforcement on the client/user side is difficult or impossible in many cases. For example, all U.S. citizens may be eligible to use a federal agency service or application that houses sensitive information, but the CSP and the federal agency can't control the security of the citizens' computers and mobile devices.

FedRAMP's goal for system security is to manage, mitigate, or resolve risks that are identified. To maximize security outcomes, FedRAMP, in consultation with NIST and the Office of Management and Budget, has developed this FedRAMP-specific policy for selecting and using cryptographic modules.

This policy provides guidance and requirements for selecting and using cryptographic modules for cloud-based systems in a way that is informed by risk and focused on strengthening federal security overall. Note that selection and use of cryptographic modules is only one aspect of implementing, managing, and maintaining cryptography, and that using a validated module is not by itself sufficient.

FedRAMP has several goals for this policy:

1. Ensure that the approved cryptographic algorithms and functions used to protect the integrity or confidentiality of federal systems and information[4].

2. Avoid unintentionally incentivizing CSPs to leave federal systems or information unprotected by omitting encryption and other applications of cryptography.

3. Promote the patching of cryptographic modules to ensure that modules in use are free of known vulnerabilities and that operating systems and applications are using up-to-date software dependencies, which can improve overall system security.

4. Ensure that CSOs using unvalidated cryptographic modules document the rationale for doing so and the CSOs are managed through the use of Plans of Actions and Milestones (POA&Ms) providing a management framework and process for the ongoing assessment of their use in a way that is clearly visible to relying agencies, other CSPs, and other stakeholders. Ensure that modules are eventually validated and that use of unvalidated modules is periodically reevaluated.

5. Ensure that IAs consistently evaluate the cryptographic module-related aspects of packages in support of the presumption of adequacy.

To achieve these goals, this policy sets expectations for CSPs, independent assessors, agencies, and reviewers related to the assessment, review, and acceptance of given implementations. FedRAMP expects this policy to facilitate decisions necessary to keep federal systems and information secure.

2.1. Cases Where a Validated Module Is Not Necessary

There are some cases where a CSP does not need to use a validated cryptographic module because the module is not necessary for protecting federal systems and information. Here are a few examples:

[4] Approved cryptographic algorithms and functions are listed on the Cryptographic Algorithm Validation Program site.

- **Cryptography may not be the only way or the most effective way of protecting the systems or information.** For example, cryptographically signing information is one way of verifying data integrity, but there are other options that may be preferable in certain situations.

- **Services are being provided to entities that do not support, cannot use, or cannot reasonably enforce the use of validated modules.** For example, the CSP may be interacting with non-federal entities that cannot consistently support validated modules. Another example is certificate authorities that issue publicly trusted certificates as part of the Web PKI. The CSP has no means of enforcing or controlling the cryptographic modules used, where an attacker's options for obtaining a fraudulent certificate are not impacted by the CSP's choice of certificate authority.

- **Another layer of cryptography is already present and uses a validated module to achieve the security requirements.** When multiple layers of cryptography are used to protect federal systems or information, it may be sufficient for only one of those layers to use a validated module. For example, if an inner encryption layer uses a validated module, an outer encryption layer (like a VPN tunnel or a mesh) might not need to use a validated module. If a CSP elects to use a second encryption layer that goes beyond what is needed to meet the SC-8(1) and SC-28(1) controls, the additional layer could use unvalidated modules. Additional layers of cryptography should be documented within the relevant controls, clearly stating that they exceed the requirement.

- **Cryptography is not needed to protect federal systems or information.** FedRAMP does not require CSPs to use validated modules where federal systems or information are not involved, nor does it require their use where the cryptographic function is not used to provide security guarantees. CSPs still need to use cryptography to protect sensitive systems and information, and the use of validated modules without known vulnerabilities is encouraged, and can even be useful to support similar requirements in other regions.

These examples are not exhaustive. They illustrate some common reasons why the use of validated cryptographic modules might not be needed.

2.2. Risks of Using Validated Modules with Known Vulnerabilities

The management and implementation of cryptography is a critical part of the system development life cycle. CSPs need to apply a risk-informed approach when addressing vulnerabilities in systems and cryptographic modules. As explained earlier in this section, FedRAMP generally prefers use of an unvalidated module with no known vulnerabilities over the use of a known-vulnerable validated module.

However, there are situations where the latter may pose less risk than the former – for example, when the known vulnerabilities in the software are already being effectively mitigated through other means. In such cases, the CSP needs to take into consideration the relevant factors. Examples of possible factors include:

- The risk inherent in the software, including:
    - the risk from known vulnerabilities
    - weakness in the cryptographic implementation that may be discovered by the FIPS 140 conformance testing processes
    - any mitigations in place to address these risks

- The potential impact to agency missions if there is a degradation of confidentiality, integrity, or availability for the system or information. This may already be reflected in the FIPS 199[5] level assigned to the system.
- The maturity of the software, the degree to which the update is based on the source code used in a validated module, and the software provider's history with navigating the module validation process. This can help in estimating the likelihood that a new or updated module will become validated.

A cryptographic module may change for a number of reasons, including:

- to add new functionality
- to fix a defect in existing functionality
- to address a change required for a software dependency
- to port the software to a new architecture or environment.

In many of these situations, the cryptographic functionality tested under CMVP is not changed, so updating the vulnerable software with FIPS-validated modules is likely to increase overall assurance, even though the new software version might not yet be FIPS validated.

If FIPS-validated cryptographic functionality tested under CMVP is changed in the new software version, the use of that update is generally preferable than continuing to use the validated module with known defects. Using modules with CAVP-validated algorithms is strongly preferred over unvalidated algorithms because of the increased assurance that CAVP validation provides.

The CAVP Automated Cryptographic Validation Testing System (ACVTS) supports automated testing. Once algorithm testing has been initially set up[6] with the ACVTS server, this process can be automated for each release

3. Requirements and Recommendations

This section defines requirements and recommendations related to cryptographic module selection for four types of stakeholders: CSPs, independent assessors, FedRAMP designated leads, and reviewers of FedRAMP packages. Requirements use "shall" language, while recommendations use "should" language.

Each requirement and recommendation has an identifier that is unique across FedRAMP policies. This identification approach enables referencing specific requirements and recommendations in this and other resources.

3.1. Cloud Service Providers

The FedRAMP marketplace facilitates effective risk-based decisions by both agencies and CSPs. Agency authorizing officials (AOs) need to be able to know and understand the risks in any cloud service offering they authorize. CSPs working toward a FedRAMP authorization also need the confidence and visibility to leverage or build on another FedRAMP authorized cloud service offering as part of their own offering.

[5] https://doi.org/10.6028/NIST.FIPS.199
[6] See how to access ACVTS for more information on use of the ACVTS. Usage guidelines are also available.

CSPs play the most important role in ensuring the adequacy of cryptographic protections in cloud services, and in providing the information necessary to facilitate decision making by the CSP community and agencies.

The following requirements apply to all CSPs:

- **FRR1:** CSPs **shall** note in their System Security Plan (SSP) in SI-2 control responses whether their default position is to use update streams or validated module streams, as defined in Section 1.

  CSPs **shall** determine their default position by performing a risk evaluation that takes into consideration the module's use in the system and the likelihood and potential impact of vulnerability exploitation, as well as mitigations to prevent such exploitation.

- **FRR2:** For cryptographic modules in use that are inherited from a FedRAMP authorized service, CSPs **shall** accurately document in Appendix Q of their SSP the cryptographic use cases, module names, and module versions.

  This documentation **shall** also note that these modules are inherited and if the leveraged services are configured properly based on applicable customer responsibilities, such as configuring FIPS mode. In Appendix Q, the FedRAMP system identifier for the inherited system would be provided in place of the CMVP identifier, since the CMVP identifier might not be known to the leveraging system. Additionally, the module vendor and name should reference the inherited service providing the cryptographic capabilities.

- **FRR3:** For cryptographic modules in use that are not inherited from a FedRAMP authorized service, CSPs **shall** accurately document in Appendix Q of their SSP the cryptographic use cases, module names, and module versions.

  Use of unvalidated modules **shall** be documented at the CSO, component, and cryptographic function level(s) in use as well as potential federal system or information impact(s), facilitating assessment and transparency to agency AOs**.**

- **FRR4:** CSPs **shall** provide a mechanism to appropriately use secure modules by default and **shall** document in the Customer Responsibility Matrix (CRM) any customer-required configuration necessary to securely utilize a module used in the system, including modules inherited and used from another cloud service, to protect federal information and to ensure that only approved algorithms are used.

  This documentation **shall** consider differences between cryptographic modes of operation (e.g., FIPS mode) that may change as a result of a module update. For example, there may be a need to technologically prevent functionality that would be otherwise allowed if operated in a different mode, such as use of unapproved cryptographic algorithms.

- **FRR5:** CSPs **shall** align their Security Assessment Plans (SAPs) to the requirements captured within this policy, which need to be assessed according to the requirements for independent assessors in Section 3.2.

- **FRR6:** CSPs using any unvalidated modules that are not derived from an update stream of an existing validated module **shall** document in their POA&M a plan for transitioning to validated

modules or update streams of validated modules. The plan outlined in the POA&M will help inform AOs' ongoing authorization decisions.

CSPs **shall** provide regular updates[7] within the POA&M on their progress toward using validated modules.

- **FRR7:** CSPs **shall** provide complete visibility into cryptographic module use (including versions) in continuous monitoring data provided to FedRAMP and agencies. No exceptions can be made; this ensures that FedRAMP and agency AOs can monitor any ongoing risk related to the use of cryptographic module versions.

  CSPs using update streams of validated modules **shall** retain artifacts demonstrating that updated major versions are submitted to the CMVP within 6 months of release.

- **FRR8:** CSPs **shall** represent their FIPS module validation status and any related claims within publicly available documentation for their FedRAMP cloud service offerings transparently and accurately. To be accurate, these representations must use terminology approved by NIST[8]. CSPs must not use ambiguous or CSP-defined terms such as "FIPS compliant" in their representations to FedRAMP.

The following requirements involve situations where new vulnerabilities are discovered in software in use that contains cryptographic modules and the modules are not inherited from a FedRAMP authorized service:

- **FRR9:** CSPs **shall** determine if updating to a newer version of the software, whether or not its cryptographic modules are FIPS validated, would eliminate the vulnerabilities; if it would, CSPs **shall** promptly update if that is feasible.

- **FRR10:** If updating the software to eliminate known vulnerabilities is not currently an option, CSPs **shall** create or update their POA&M based on the criticality of the vulnerabilities[9] to communicate their plan for remediating or mitigating the vulnerabilities. The plan outlined in the POA&M will help inform AOs' ongoing authorization decisions.

The following recommendations apply to all CSPs in regards to the providers that implement cryptographic modules used in their CSOs:

- **FRR11:** CSPs **should** ask their providers that implement cryptographic modules to be transparent about changes they make in their software in regards to cryptographic modules.

  For example, their change logs should include information if cryptographic modules were changed and the nature and extent of any changes. This will help organizations using the cryptographic modules to better estimate the risk associated with those changes.

---

[7] For frequency requirements, see Section 3 of the FedRAMP Plan of Actions and Milestones (POA&M) Template Completion Guide.

[8] See use of FIPS 140 logos and phrases on the CMVP website for specific phrase and logo requirements.

[9] This is consistent with vulnerability management requirements defined in the FedRAMP Plan of Actions and Milestones (POA&M) Template Completion Guide, Section 3 of FedRAMP Vulnerability Scanning Requirements, and the FedRAMP Vulnerability Deviation Request Form.

- **FRR12:** CSPs **should** ask their providers that implement cryptographic modules to promote the use of update streams over the use of validated module streams.

  Pinning to validated modules often has a negative net effect on software dependencies that can result in the use of outdated, vulnerable versions of other software components in the operating system. This can increase the overall number of severe vulnerabilities in libraries and other software across the operating system, making it less secure overall.

- **FRR13:** CSPs **should** ask their providers that implement cryptographic algorithms to ensure that these algorithms are tested and meet NIST requirements using the CAVP Automated Cryptographic Validation Testing System (ACVTS).

- **FRR14:** CSPs **should** ask their providers that implement cryptographic modules to resubmit their software for FIPS validation when its cryptographic modules have been modified to maintain a high level of cryptographic module assurance.

  FIPS validation increases the level of assurance for software cryptographic modules, so FIPS validation should continue to occur.

3.2. Independent Assessors

The following requirements specific to cryptographic modules apply to all independent assessors. The activities help ensure that CSPs are managing the selection and use of their cryptographic modules according to the requirements of Section 3.1.

- **FRR15:** IAs **shall** perform a comprehensive examination[10] where unvalidated modules that are not derived from an update stream of an existing validated module are used to meet a control requirement (i.e., when FRR6 applies).

  IAs **shall** ensure that such modules and mitigations are operating as intended and producing the documented security and risk management outcome.

- **FRR16:** IAs **shall** verify that all cryptographic use cases and use of modules are accurately documented in Appendix Q of the SSP as specified in FRR2 and FRR3.

  IAs shall verify CMVP submission artifacts to ensure modules are validated in accordance with FFR7

- **FRR17:** IAs **shall** verify that POA&Ms related to cryptographic modules are created by the CSP when required, are updated regularly, and are not overdue.

3.3. FedRAMP Designated Leads

The following requirements specific to cryptographic modules apply to FedRAMP designated leads. They help ensure that CSPs are managing the selection and use of their cryptographic modules according to the requirements of Section 3.1.

[10] SP 800-53A Rev. 5, Assessing Security and Privacy Controls in Information Systems and Organizations

- **FRR18:** FedRAMP designated leads **shall** review documentation that captures the cryptographic module provider's approach to managing cryptographic module validation as part of the provider's system development life cycle to ensure the approach meets the requirements in this policy.

- **FRR19:** FedRAMP designated leads **shall** review SC-13 findings in the POA&M and related risk identification and mitigation documentation provided within the CSO repository and ensure that the required milestones are met on schedule.

3.4. Package Reviewers

The following requirements apply to FedRAMP reviewers and designated lead package review teams. Package reviewers help ensure that CSPs are managing the selection and use of their cryptographic modules according to the requirements of Section 3.1, which are a requirement for all FedRAMP authorizations.

- **FRR20:** Package reviewers **shall** verify that all cryptographic use cases and modules are accurately and comprehensively documented as specified in FRR2 and FRR3 and that IAs have reviewed this information as specified in FRR16, including the specific modules and versions in use.

- **FRR21:** Package reviewers **shall** validate that the assessment artifacts represent a thorough evaluation where unvalidated modules are used to meet a control requirement.

DOCUMENT REVISION HISTORY

FedRAMP will review this policy on a yearly basis and will issue revisions as needed.

Date	Version	Description
08/10/2024	1.0	Initial Public Draft
01/16/2025	1.1	Approved by FedRAMP Board