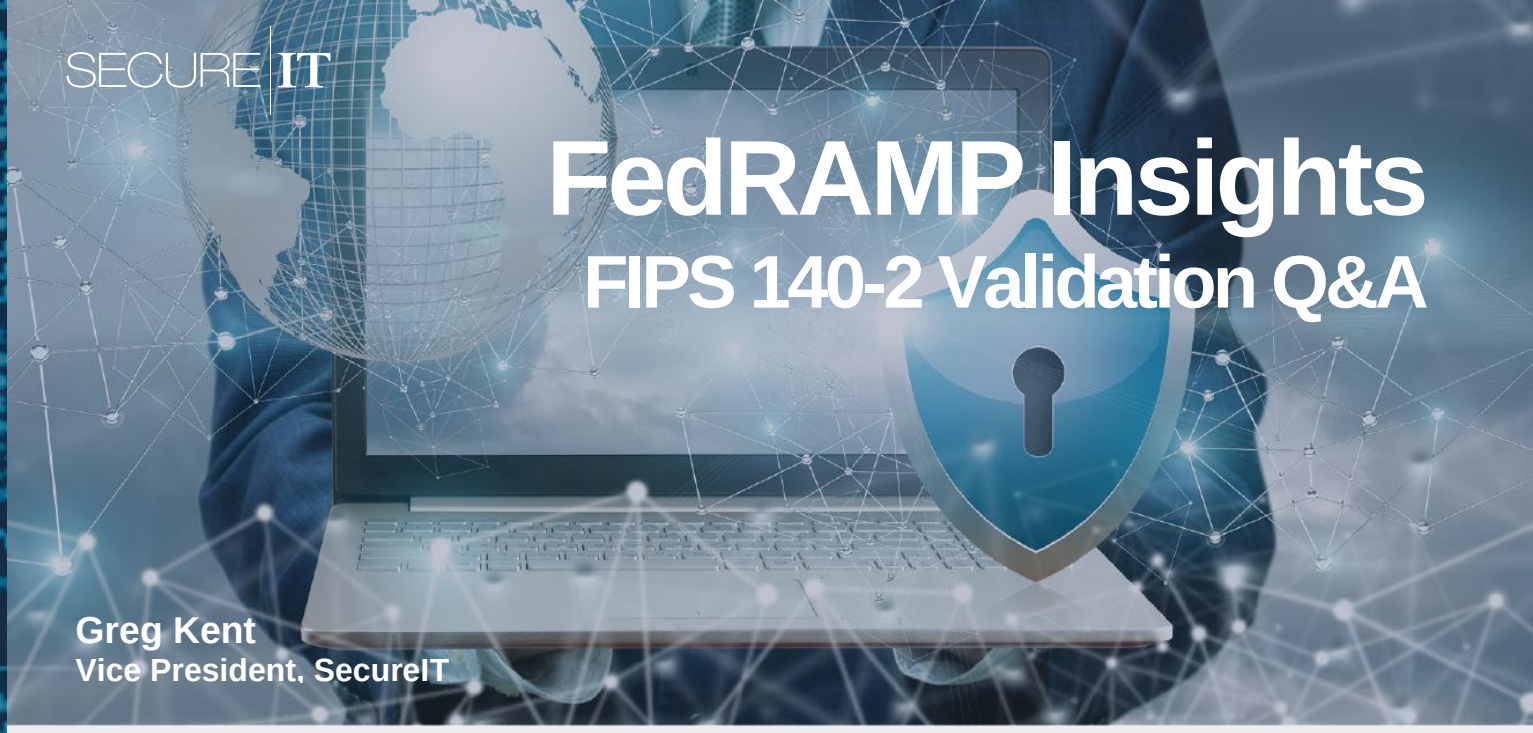
SECURE IT

FedRAMP Insights
FIPS 140-2 Validation Q&A



Greg Kent
Vice President, SecureIT

TECH BULLETIN

Introduction

Understanding the FIPS 140-2 validation requirements for FedRAMP represents a critical step on the path to FedRAMP authorization for many cloud service providers. This security standard for cryptographic modules requires more than "FIPS 140-2 compliant" ciphers and key lengths that some vendors reference. FedRAMP authorization requires that full encryption modules have been independently validated and certified by a NIST-specified accredited laboratory and that the SSP documentation includes certification/validation numbers and dates for all relevant products.

As a 3PAO, SecureIT often encounters service providers who find the FIPS 140-2 security requirement confusing. Many times, cloud providers think they have implemented FIPS 140-2 as required, when in fact they are not using a validated module. Below are answers to the most frequently asked questions about FedRAMP authorization and FIPS 140-2 validation requirements.

Q1: For FedRAMP, are there are any special requirements related to FIPS validation?

A: FedRAMP requires the use of FIPS 140-2 validated encryption generally (SC-13) and for specific functions like the generation and distribution of encryption keys (SC-12), encryption of digital media during transport (MP-5), and multi-factor authentication for remote access (IA-2(11)). The FedRAMP-defined Assignment parameters and/or additional FedRAMP guidance for these controls indicate that FIPS 140-2 validated encryption modules must be used.

For some controls, the language of these FedRAMP-defined parameters might suggest that an alternative other than FIPS-validated cryptography may be permissible. For example, the FedRAMP assigned value for control IA-02(11) indicates that multi-factor authentication devices must meet "FIPS 140-2, NIAP Certification, or NSA approval." This language reads as if an encryption module that is not FIPS 140-2 validated might still be permitted if NSA approval is available. As a practical matter, however, cloud providers are unlikely to avoid the requirement for FIPS 140-2 validation. Despite the language of the assignment parameters in the control, FedRAMP guidance on Digital Identity Requirements clarifies that only FIPS 140-2 validated cryptographic modules are approved as cryptographic techniques for multi-factor authentication for Moderate and High systems within the FedRAMP program.

For cloud providers seeking a FedRAMP Readiness Assessment Report (RAR), the requirements are even stricter. The RAR requires that FIPS 140-2 validation cryptographic algorithms and modules be used for each of the following functions: data at rest (SC-28), transmission (SC-8(1), SC-12, SC-12(2), SC-12(3)), remote access (AC-17(2)), authentication (IA-5(1)), and digital signatures/hashes (CM-5(3)). During a Readiness assessment, the 3PAO is required to identify all non-validated cryptographic modules in use within the system.

FedRAMP also requires that the System Security Plan (SSP) documentation include the FIPS 140-2 certification/validation numbers and dates for all relevant products.

Q2: What is FIPS 140-2?

A: The Federal Information Processing Standard 140-2 (FIPS 140-2) is a security standard for cryptographic modules. The standard specifies security requirements spanning 11 areas related to the design and implementation of cryptographic modules. For each area, the module receives a security level rating (1-4, from lowest to highest) depending on what requirements are met. A module can be hardware, firmware, software or a combination of the three that implements some form of cryptographic function (encryption, hashing, digital signatures, message authentication, random number generation). Only cryptographic modules validated by the Cryptographic Module Validation Program (CMVP), with an active certificate, are FIPS 140-2 validated.

Federal agencies are required to implement FIPS 140-2 validated modules when using cryptography to protect sensitive information. While mandatory for the U.S. government, FIPS 140-2 has become the standard for many other regulated industries such as finance and healthcare.

Q3: Is "FIPS 140-2 Compliant" sufficient?

A: No. When a company claims their product is FIPS 140-2 compliant, it is not the same as saying they are FIPS 140-2 certified or validated. Compliant means some but not all of the product has been FIPS validated. Often when a vendor claims that their product is "FIPS 140-2 compliant" they only mean that their product uses approved encryption ciphers and key lengths. To be FIPS 140-2 certified or validated, the full encryption module itself (which implements the ciphers) must be independently validated by one of the NIST-specified accredited laboratories. Unvalidated cryptography is viewed by the Federal government as providing no protection to the information or data, effectively considering it to be unprotected plaintext.

Q4: How can I check whether I'm using a FIPS-validated module?

A: Follow these steps below to identify whether you're using a FIPS-validated module. For more detailed step-by-step examples, refer to FAQ #5.

Step 1: Identify the module being used

A module may either be an embedded component of a product or application, or a complete product in and of itself.

a. If the module is the complete product, move to Step 2.

b. If the module is a component of a larger product or application, contact the vendor to determine the embedded validated cryptographic module. Many vendors provide and promote this information on their websites.

When in doubt, contact the vendor to identify the module.

Step 2: Confirm the module is FIPS 140-2 validated

Search the NIST CMVP database and confirm that the module (including the particular version) has been validated and that the validation for the module is active: https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules/Search

Step 3: Confirm the module is configured in accordance with the FIPS 140-2 Security Policy

As part of the validation process, a Security Policy is created to describe how the encryption module meets the security requirements of FIPS 140-2 and to provide guidance on how to run the module in a FIPS 140-2 mode of operation. The Security Policy is stored in the NIST CMVP database and linked from the validation certificate. The guidance within the Security Policy should be followed to ensure that the module has been properly implemented and configured in accordance with the requirements for FIPS 140-2 validation. For example, it may be necessary to confirm software/firmware version, FIPS mode configurations, and permitted ciphers and algorithms are implemented. If a system is not properly configured, those configurations need to be changed to match the details listed in the validated Security Policy.

Q5: The vendor has released a patch that changes the version of the module I'm using. Should I apply the patch, and would the system still be considered FIPS-validated after the patch in installed?

A: If the cryptographic module you're using changes, the previous FIPS 140-2 certificate number is no longer applicable. Search the NIST CVMP site to see whether the newer version of the module has also been validated: https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules/Search.

If the newer version of the module has not been validated, then installing the patch will make the system non-compliant with Federal requirements. We suggest determining whether validation of the module is "in process" by checking with the vendor and confirming via the NIST CMVP site: https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Modules-In-Process. Based on the nature of the patch and timing of when FIPS 140-2 validation is expected to occur, a risk-based decision needs to be made about whether (and when) to apply the patch.

Q6: If my cloud system needs to comply with FedRAMP, should I patch a high-risk vulnerability if doing so will make a device no longer compliant with FIPS validation requirements?

A: In most cases, the FedRAMP requirement to remain FIPS validated is considered more important than the requirement to patch vulnerabilities in a timely manner. In general, cloud providers with FedRAMPed systems should submit an operational requirement deviation request for any vulnerabilities that cannot be remediated without impairing FIPS validation. However, the operational requirement exists only until the new version of the encryption module is validated, which means that the cloud provider needs to review the FIPS Validated Modules list every week or so in order to determine when the patch can safely be applied.

The FedRAMP PMO has also emphasized that patches that impact encryption module versions should not be applied during the initial testing period. After an initial 3PAO assessment begins, it is crucial that encryption modules remain active and unchanged until the initial assessment has been completed.

In rare situations, a patch may address a particularly critical vulnerability that is clearly riskier than unvalidated encryption modules. Then, it may be possible to obtain an operational requirement deviation for the FIPS validation requirement. In such circumstances, the cloud provider should consult with their authorizing official and the FedRAMP PMO. Under extreme circumstances, these constituencies may agree that it may be risk-justified to apply the patch immediately and establish an operational requirement for the FIPS validation requirement.

In rare situations, a patch may address a particularly critical vulnerability that is clearly riskier than unvalidated encryption modules. Then, it may be possible to obtain an operational requirement deviation for the FIPS validation requirement. In such circumstances, the cloud provider should consult with their authorizing official and the FedRAMP PMO. Under extreme circumstances, these constituencies may agree that it may be risk-justified to apply the patch immediately and establish an operational requirement for the FIPS validation requirement.

Q7: An auditor is asking for evidence of FIPS 140-2 validation. What artifacts do I need to gather to demonstrate this?

A: Typically, you will need to provide the following information to your auditor:

- The FIPS 140-2 CVMP certificate number and date
- Evidence that the module version listed in the certificate is being used in the system (e.g., if the module is embedded within a product) and that the version you have installed corresponds to the version described in the certificate and Security Policy
- Evidence that the module has been implemented and configured in accordance with the requirements specified in the FIPS 140-2 Security Policy

For step-by-step examples of confirming and providing evidence of compliance with FIPS 140-2 requirements, refer to our FedRAMP Tech Bulletin titled “Demonstrating FIPS Validation.”

SECURE IT

A key component of achieving FedRAMP authorization requires CSP's to demonstrate that their cloud service is compliant with FIPS 140-2 requirements. Success entails understanding of the requirements put forth in standard, validating existing cryptographic software modules, possibly applying software patches and addressing any changes in your service associated with the changes. Finally, CSPs need to demonstrate FIPS 140-2 compliance through the proper documentation. Without the right resources and time, addressing FIPS-related requirements can be challenging for some CSPs,

As an accredited FedRAMP 3PAO, SecureIT has extensive compliance and audit experience to help you achieve FedRAMP authorization. Whether you need an advisor to guide compliance efforts or a 3PAO to conduct an assessment, SecureIT provides FedRAMP compliance expertise targeted to the specific needs of small and mid-sized businesses.

About SecureIT

SecureIT provides compliance, IT audit and cybersecurity services to enterprises, government entities, and cloud service providers. Our certified professionals assess cyber risk, conduct FedRAMP 3PAO assessments, and advise companies seeking compliance with regulatory requirements. Every day, we partner with our clients to deliver solutions critical to protecting and growing business.

12110 Sunset Hills Road
Suite 600
Reston, VA USA 20190
703.464.7010
www.secureit.com

Design by Marketlocity