Cryptographic Module Validation Program CMVP

Overview

Welcome to the CMVP

The Cryptographic Module Validation Program (CMVP) is a joint effort between the National Institute of Standards and Technology under the Department of Commerce and the Canadian Centre for Cyber Security, a branch of the Communications Security Establishment. The goal of the CMVP is to promote the use of validated cryptographic modules and provide Federal agencies with a security metric to use in procuring equipment containing validated cryptographic modules.

Each Cryptographic and Security Testing Laboratories (CSTL) is an independent laboratory accredited by NVLAP. CSTLs verify each module meets a set of testable cryptographic and security requirements, with each CSTL submission reviewed and validated by CMVP.

CMVP accepted cryptographic module submissions to Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules* until March 31, 2022**.** On April 1, 2022 the CMVP no longer accepted FIPS 140-2 submissions for new validation certificates except as indicated in the table below.

As of September 22, 2020, CMVP began validating cryptographic modules to Federal Information Processing Standard (FIPS) 140-3, *Security Requirements for Cryptographic Modules*.

Applicability of Validated Modules

Modules validated as conforming to FIPS 140-2 will continue to be accepted by the Federal agencies of both countries for the protection of sensitive information (United States) or Designated Information (Canada) through September 21, 2026. After that time CMVP will place the FIPS 140-2 validated modules on the Historical list, allowing agencies to continue using these modules for existing systems only. Agencies should continue to make use of FIPS 140-2 modules until replacement FIPS 140-3 modules become available.

FIPS 140-3 submissions for validations are being accepted. Upon validation, modules will be placed on the Active list for 5 years (or 2 years for Interim Validations) and may be purchased for new and existing systems.

Interim Validations (NEW)

The CMVP is offering an interim validation process for module submissions that meet the following criteria:

- Submitting Cryptographic Security Testing (CST) lab must be in an active status with NVLAP.
- Received by the CMVP prior to 1 Jan 2024, and have not yet been validated.
- Fully tested and evaluated for conformance to the FIPS 140-3 standard by an active, accredited CST lab.
- Recommended for validation by the accredited CST lab who performed the testing.

- In addition to the original submission documents, the CST lab must also complete and sign a CMVP-provided requirement checklist.
- The vendor must inform the CMVP through their CST lab if they elect to choose interim validation. Electing for interim validation is available until 1 Oct 2024.

These module submissions will be reviewed for completeness by CMVP staff. If needed, there will be a brief period of Coordination with the CST lab to resolve any questions. Once this step is successfully completed:

- A two-year sunset date (expiration date) will be awarded.
- The 'Interim Validation" caveat will be added to the certificate validation entry to distinguish them from a full validation (see CMVP Caveats webpage for more information)
- An optional follow-up submission that conforms to the SP 800-140Br1 format may be submitted to the CMVP. Upon successful review and completion of this submission, the "Interim Validation" caveat will be removed, and the sunset date modified to add three more years to reflect a change from two to five years for the total sunset length.
- Any non-compliance identified (e.g., during the follow-up review) will be resolved with existing processes and provide the opportunity for a timely resolution prior to moving the validation certificate to the Historical or Revocation lists (see FIPS 140-3 Management Manual 4.8 for more information).
- This follow-up submission must be received by the CMVP prior to the two-year sunset date to remain on the active list until the completion of the follow-up submission.
- The validation will be moved to the historical list if the follow-up submission is not received prior to the two-year sunset date.

This interim validation option is voluntary. Vendors do not need to take any action if they would prefer to wait for their full review to be completed to receive full, five-year validation. Vendors who would like to elect the interim validation should follow the process above.

Status of CMVP validation effort

CMVP is experiencing a significant backlog in the validation process. Use of validated modules currently on the Active list is encourage

Date	**Activity**
September 22, 2020	CMVP accepts FIPS 140-3 submissions.
June 14, 2021	Last date CSTLs accepted contracts for FIPS 140-2 Scenario 5 and Scenario 3.

Date	Activity
September 22, 2021	CMVP no longer accepts FIPS 140-2 submissions for new validation certificates unless the vendor is under contract with a CSTL prior to June 15, 2021, the CSTL has submitted an extension request, and the CSTL has received acceptance by the CMVP. However, CMVP continues to accept FIPS 140-2 reports that do not change the validation sunset date, i.e. Scenarios 1, 1A, 1B, 3A, 3B, and 4 as defined in FIPS 140-2 Implementation Guidance G.8.
October 1, 2021	*Scenarios 2 and 1B submissions are no longer accepted.*
April 1, 2022	*CMVP only accepts FIPS 140-2 reports that do not change the validation sunset date, i.e. Scenarios 1, 1A, 3A, 3B, and 4 as defined in FIPS 140-2 Implementation Guidance G.8.*
September 21, 2026	*FIPS 140-2 active modules can be used until this date for new systems. After this date, FIPS 140-2 validation certificates will be moved to the Historical List.*

Use of Non-validated Cryptographic Modules by Federal Agencies and Departments

Non-validated cryptography is viewed by NIST as providing ***no protection*** to the information or data—in effect the data would be considered unprotected plaintext. ***If the agency specifies that the information or data be cryptographically protected***, then FIPS 140-2 or FIPS 140-3 is applicable. In essence, if cryptography is required, then it must be validated. Should the cryptographic module be revoked, use of that module is no longer permitted.