DRAFT

FIPS 140-3
Cryptographic Module Validation Program Management Manual

(Date 12/23/2022)

Version 1.2

National Institute of Standards and Technology and
Canadian Centre for Cyber Security

Revision History

Version	Date	Comment
1.0	9/21/2020	First draft release for FIPS 140-3 program
1.1	7/13/2022	Second draft release. Major rewrite.
1.2	12/23/2022	Updates to address feedback during July 2022 review.

Table of Contents

List of Figures

List of Tables

1 Introduction

1.1 Background

The Canadian Centre for Cyber Security (CCCS) and the National Institute of Standards and Technology (NIST) announced the establishment of the Cryptographic Module Validation Program (CMVP) on July 17, 1995. The CMVP validates commercial cryptographic modules to Federal Information Processing Standard (FIPS) 140, NIST-recommended standards, and other cryptography-based standards. The CMVP is a government validation program that is jointly managed by NIST and CCCS. Cryptographic modules validated as conforming to FIPS 140 are used by Federal agencies for the protection of Controlled Unclassified Information (CUI) (Government of the United States of America) or Protected information (Government of Canada).

Vendors of commercial cryptographic modules use independent, National Voluntary Laboratory Accreditation Program (NVLAP) accredited Cryptographic and Security Testing (CST) laboratories to have their modules tested. The Cryptographic and Security Testing Laboratories (CSTL)s may perform all of the tests covered by the CMVP. The Validation Authority reviews laboratory reports, issues validation certificates, and participates in laboratory accreditations.

1.2 Purpose of the CMVP Management Manual

The purpose of the CMVP Management Manual is to provide effective guidance for the management of the CMVP as authorized by FIPS 140-3, and the conduct of activities necessary to ensure that the standards, as referenced in FIPS 140-3, are fully met.

1.3 Applicability and Scope

The *CMVP Management Manual* is applicable to the CMVP Validation Authority, the CSTLs, and the vendors who participate in the program. Consumers who procure validated cryptographic modules may also be interested in the contents of this manual. This manual outlines the management activities and specific responsibilities which have been assigned to the various participating groups. This manual does not deal with the actual standards and technical aspects of the standards.

1.4 Purpose of the CMVP

The purpose of the CMVP is to increase assurance of secure cryptographic modules through an established process.

Prior to CMVP, each office was responsible for assessing encryption products with no standardized requirements. This meant that each office needed some expertise in evaluating manufacturing practices for cryptographic equipment and vendors would have to support each office in their evaluation. With the establishment of the CMVP, a standards-based assessment could be uniformly applied and used across the federal governments and other organizations

finding value in the use of validated cryptography.

CMVP Validation is performed through conformance testing to requirements for cryptographic modules as specified in FIPS 140. Accredited third-party CSTLs perform independent assurance testing with CMVP oversight. CMVP is the Validation Authority, a joint initiative between the Government of Canada and the Government of the United States of America. For more information about CMVP see: https://csrc.nist.gov/projects/cryptographic-module-validation-program.

1.5 Purpose of the Cryptographic Algorithm Validation Program (CAVP)

The purpose of the CAVP is to increase assurance of cryptographic algorithms through a testing process. Validation is achieved by testing the algorithm and comparing results to known or expected answers. Tests are to demonstrate compliance with cryptographic standards listed in SP 800-140C, SP 800-140D, and SP 800-140E. More information about CAVP can be found at: https://csrc.nist.gov/Projects/cryptographic-algorithm-validation-program.

1.6 Use of Validated Products

Both public and private sectors can use cryptographic modules validated to FIPS 140 for the protection of sensitive information. As specified under FISMA of 2002, U.S. Federal departments and agencies are required to use cryptographic modules validated to FIPS 140 for the protection of sensitive information where cryptography is required. Similarly, the CCCS recommends that GC departments and agencies use those validated cryptographic modules for the protection of Protected information.

1.7 CMVP Management Manual Structure

This manual is organized into the following sections:

Section 1 – Introduction provides an introduction and overview of the CMVP.

Section 2 – CMVP Management describes the management of the CMVP including the organization, administration, roles and responsibilities, and policies.

Section 3 – CSTL Processes describes the CSTL processes including accreditation, maintenance, and management of a laboratory.

Section 4 – CMVP Processes describes the various aspects of the cryptographic module validation process.

Section 5 – CMVP and CAVP Programmatic Metrics Collection.

Section 6 – Test Tools describes the necessary and recommended tools for use by the CSTLs.

Section 7 – CMVP General Testing and Reporting Guidance adds requirements to manage the CMVP testing program, minimizing retest and maximizing testing flexibility while maintaining assurance.

Annex A –Validation Issue Assessment Process provides an overview how contentious issues over module previously validated are addressed.

1.8 CMVP Related Documents

FIPS 140 specifies the security requirements for a cryptographic module utilized within a security system protecting sensitive information in computer and telecommunication systems. The CMVP utilizes a set of documents, identified below, containing the security requirements and testing of those requirements that must be satisfied by a cryptographic module. CMVP also works with NVLAP to address CSTL accreditation requirements. A diagram of the relationships for the documents referenced below is available on the CMVP webpage (www.nist.gov/cmvp) under *CMVP FIPS 140-3 Related References*.

1.8.1 FIPS 140-3

Federal Information Processing Standards FIPS 140-3 identifies the CMVP, a joint effort of the US and Canadian governments, as the validation authority for implementing a program utilizing the ISO/IEC 19790:2012 requirements standard and ISO/IEC 24759:2017 derived test methods. The standard also established the CMVP technical requirements to be contained in NIST Special Publication (SP) 800-140, SP 800-140A, SP 800-140B, SP 800-140C, SP 800-140D, SP 800-140E, and SP 800-140F. These security requirements must be satisfied by a cryptographic module utilized within a security system protecting controlled unclassified information (hereafter referred to as sensitive information). This standard will supersede FIPS 140-2, Security Requirements for Cryptographic Modules, in its entirety. FIPS 140-3 is available on-line at https://doi.org/10.6028/NIST.FIPS.140-3.

Responsible Positions: NIST CMVP and CCCS CMVP Program Managers.

1.8.2 Security Requirements for Cryptographic Modules

ISO/IEC 19790:2012 (with Technical Corrigendum 1) specifies the security requirements for a cryptographic module utilized within a security system protecting sensitive information in computer and telecommunication systems. This International Organization for Standardization, (ISO) standard defines different levels for cryptographic modules to provide for a wide spectrum of data sensitivity (e.g., low value administrative data, million-dollar funds transfers, life protecting data, personal identity information, and sensitive information used by government) and a diversity of application environments (e.g., a guarded facility, an office, removable media, and a completely unprotected location). The ISO/IEC Standard specifies four security levels with 11 requirement areas, each security level increasing security requirements over the preceding level.

The standard is typically reviewed by an ISO committee every three years for consideration of revision. Copies can be obtained from ISO.org. NIST made available a limited number of copies of ISO/IEC 19790:2012. To request a copy of ISO/IEC 19790:2012 and ISO/IEC 24759:2017 (see below), see the CMVP webpage, https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-standards.

Responsible Positions: ISO technical committee: ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection.

1.8.3 Test requirements for cryptographic modules

ISO/IEC 24759:2017 specifies the methods to be used by accredited CSTLs to test whether the cryptographic module conforms to the requirements specified in ISO/IEC 19790:2012. The test requirements (TR) contains the security requirements from ISO/IEC 19790:2012, stated as a set of assertions (AS) (i.e., statements that must be true for the cryptographic module to satisfy the requirement of a given area at a given level). All assertions are direct quotations from ISO/IEC 19790:2012. Following each assertion is a set of information requirements that must be fulfilled by the vendor as vendor evidence (VE). These VEs describe the types of documentation or explicit information that the vendor must provide in order for the tester to determine conformance to the given assertion. Following each assertion and corresponding vendor information requirement is a set of test evidence (TE) that must be applied by the tester of the cryptographic module. These TEs instruct the tester as to what they must do in order to test the cryptographic module with respect to the given assertion. ISO/IEC 24759:2017 VE and TE requirements may be modified by the SP 800-140 set of documents and the FIPS 140-3 Implementation Guidance (IG).

Responsible Positions: ISO technical committee: ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection.

1.8.4 NIST SP 800-140*x*

The current version of the following SPs can be found at: https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-standards#sp . Each SP 800-140*x* document will be updated as needed, following the publication of a draft for public comment and resolution by the CMVP.

NIST SP 800-140 specifies the Test Requirements (TR) for Federal Information Processing Standard (FIPS) 140-3. SP 800-140 modifies the TE and/or VE requirements of ISO/IEC 24759:2017. As a validation authority, the CMVP may modify, add, or delete TEs and/or VEs as specified under section 5.2 of ISO/IEC 24759:2017. This NIST SP should be used in conjunction with ISO/IEC 24759:2017 as it modifies only those requirements identified in this document.

NIST SP 800-140A modifies the vendor documentation requirements of ISO/IEC 19790:2012 Annex A. As a validation authority, the CMVP may modify, add, or delete VEs and/or TEs as specified under section 5.2 of ISO/IEC 19790:2012. This document should be used in conjunction with ISO/IEC 19790:2012 Annex A and ISO/IEC 24759:2017 paragraph 6.13 as it modifies only those requirements identified in this document.

NIST SP 800-140B is to be used in conjunction with ISO/IEC 19790:2012 Annex B and ISO/IEC 24759:2017 6.14. The SP modifies only those requirements identified in this document. SP 800-140B also specifies the content of the tabular and graphical information required in ISO/IEC 19790:2012 Annex B. As a validation authority, the CMVP may modify, add, or delete VE and/or TE specified under paragraph 6.14 of ISO/IEC 24759:2017 and as specified in ISO/IEC 19790:2012 paragraph B.1.

NIST SP 800-140C replaces the approved security functions of ISO/IEC 19790:2012 Annex C. As a validation authority, the CMVP may supersede this Annex in its entirety. This document supersedes ISO/IEC 19790:2012 Annex C and ISO/IEC 24759:2017 paragraph 6.15.

NIST SP 800-140D replaces the approved sensitive parameter generation and establishment methods requirements of ISO/IEC 19790:2012 Annex D. As a validation authority, the CMVP may supersede this Annex in its entirety. This document supersedes ISO/IEC 19790:2012 Annex D and ISO/IEC 24759:2017 paragraph 6.16.

NIST SP 800-140E replaces the approved authentication mechanism requirements of ISO/IEC 19790:2012 Annex E. As a validation authority, the CMVP may supersede this Annex in its entirety with its own list of approved authentication mechanisms. This document supersedes ISO/IEC 19790:2012 Annex E and ISO/IEC 24759:2017 paragraph 6.17.

NIST SP 800-140F replaces the approved non-invasive attack mitigation test metric requirements of ISO/IEC 19790:2012 Annex F. As a validation authority, the CMVP may supersede this Annex in its entirety. This document supersedes ISO/IEC 19790:2012 Annex F and ISO/IEC 24759:2017 paragraph 6.18.

Responsible Positions: NIST CMVP and CCCS CMVP Program Managers.

1.8.5 Implementation Guidance

Implementation Guidance is issued to provide clarification and guidance with respect to an assertion or group of assertions found in the documents listed above. Often, implementation guidance is issued to assist CSTLs and vendors to apply the requirements to a particular type of cryptographic module implementation or technology. Implementation guidance is also issued based on responses by NIST and CCCS to questions posed by the CSTLs, vendors, and other interested parties. The document is available on-line on the official website at https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/announcements.

Responsible Position: NIST CMVP and CCCS CMVP Program Managers.

1.8.6 Web Cryptik User Guide

This guide is in draft form, covering the use of FIPS 140-3 Web Cryptik. It is expected to be updated often as new functionality, edits, and program changes are introduced. The user guide will also identify where IG information requested should be included in the report and security policy. This guide also provides guidance on how to fill in the available fields (e.g., vendor name, Hardware/Software/Firmware versioning, algorithms, caveats, and operational environment).

Responsible Position: CMVP Technology Manager.

1.8.7 CSTL Accreditation Standards

NIST laboratory accreditation standards applicable to the NVLAP accreditation of CSTLs are published on the NVLAP website at https://www.nist.gov/nvlap.

NIST laboratory accreditation standards relevant to the NVLAP accreditation of CSTLs are:

NIST Handbook 150 (2020), *NVLAP Procedures and General Requirements,*

NIST Handbook 150-17 (2020), *NVLAP Cryptographic and Security Testing,* Document

Links for these documents are available at https://www.nist.gov/nvlap/publications-and-forms/nvlap-handbooks-and-lab-bulletins.

Responsible Position: Chief of NVLAP.

1.8.8 Additional information on the CMVP Website

The CMVP website contain several pages pertinent to the FIPS 140-3 program:

1. Announcements (https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Announcements) contains information on changes made to documents or test tools.
2. Notices (https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Notices) contains copies of statements published in the Federal Register, programmatic or policy updates or information not related to CMVP documents or test tools.
3. Validated Modules (https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules) contains the link to the search tool for finding a specific module, or aspects of a module validation. In addition, the page contains information describing categories (active, historical, and revoked) and explains the difference between a module that is a product vs one that is a component.
4. Implementation Under Test (IUT) List (https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Modules-In-Process/IUT-List) contains information provided by the CSTLs about cryptographic modules undergoing testing. The result of the testing has not yet been submitted to the CMVP. Inclusion of a module on this list is voluntary, dependent on the vendor. The CMVP has no information regarding the status of these modules or know if or when a test report will be submitted to the CMVP. The modules are listed by vendor name. For more information regarding a specific module, please contact the vendor.
5. Modules in Process (MIP) List (https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Modules-In-Process/Modules-In-Process-List) lists the review status for each cryptographic module whose scenario type is FS (Full submission) or UP (Update). The list tracks the test report after it has been submitted to the CMVP through validation. For each submission, the status and the date it went into that state is listed. (The listing is voluntary; vendors may choose to have their module listed on this list). For additional information regarding a specific module, please contact the vendor.
6. Programmatic Transitions (https://csrc.nist.gov/Projects/cryptographic-module-validation-program/programmatic-transitions) lists algorithm-related transitions. Applicable standards, relevant IGs, ACVTS availability, and the beginning CMVP

acceptance date are listed for each algorithm/scheme. Also available is information related deprecated algorithms/schemes that force validated module certificates to the historical category. Included in this list are dates for last submission date as an approved algorithm/scheme as well as the date whereby the validation certificate of an approved module using the algorithm/scheme will be moved to the Historical list.

7. Management Manual (https://csrc.nist.gov/Projects/cryptographic-module-validation-program/cmvp-fips-140-3-management-manual) contains the link to the latest version of this manual.

8. Related References (https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-standards) describes the FIPS 140-3 standard, referenced standards in FIPS 140-3, and CMVP management documents.

9. IG Announcements (https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-ig-announcements) is where the latest version of the FIPS 140-3 IGs can be found. The webpage also includes links of previous versions, and a short summary of changes.

10. Resources (https://csrc.nist.gov/Projects/cryptographic-module-validation-program/resources) provides guidance that is easily bookmarked. Information that is needed by vendors and CSTLs is listed here. As an example, specifically detailed validation and re-validation information such as minimum testing requirements for revalidation and equivalency can be found here.

11. CVP Certification Exam Information (https://csrc.nist.gov/Projects/cryptographic-module-validation-program/cvp-certification-exam-information) Cryptographic Validation Program (CVP) In order to be a certified tester for a CSTL, an individual must pass this exam.

12. CSTL Accreditation and Fees (https://csrc.nist.gov/Projects/Testing-Laboratories) contains a link to the name and location of every CSTL accredited to perform Cryptographic and Security Testing. The list also includes a point of contact for each laboratory.

Responsible Position: NIST CMVP and CCCS CMVP Program Managers.

2 CMVP Management

2.1 Introduction

The purpose of this section is to describe the overarching management structure and principles of the CMVP.

2.2 Validation Authority

The validation authority is the CMVP. The CMVP is jointly managed by NIST and CCCS. NIST and CCCS have both signed agreements for the management of the program that contains precepts by which both parties must abide. Copies of the agreements are kept by the Partnerships Group at CCCS and by the Computer Security Division at NIST.

2.3 Programmatic Directives, Policies, Internal Guidance and Documentation

The CMVP issues programmatic directives, policies, internal guidance, and documentation to all CSTLs. These communications are normally distributed by email. These communications are very important and can seriously impact on-going validation efforts. Information will be incorporated into the CMVP documentation over time.

The CMVP will strive not to make those directives and guidance retroactive to previous validations. However, the status of previous validations may be affected. CSTLs are encouraged to provide timely comments to the CMVP about those communications.

2.4 CMVP Points of Contact

Questions concerning the general operation of the CMVP can be directed to either NIST or CCCS. If a vendor is under contract with a CSTL for cryptographic module or algorithm testing, the vendor must contact the contracted laboratory for all questions concerning the test requirements.

A list of CMVP points of contact can be found on the CMVP website at: https://csrc.nist.gov/projects/cryptographic-module-validation-program.

2.4.1 Language of Correspondence

All correspondence between NIST, CCCS, NVLAP, and the CSTLs **shall** be in the English language only.

2.5 Request for Guidance from CMVP

The CMVP suggests reviewing the CMVP Management Manual, IGs, the CMVP Announcements, and CMVP Notices posted on the CMVP web sites first as answers to questions may be readily available. The information found on the CMVP web site provides the official position of the CMVP. If the information cannot be found in the aforementioned guidance,

CMVP will accept informal requests (general knowledge) and formal requests (specific application). In addition, CMVP will accept post-validation inquiries for any perceived issues relating to existing modules.

Vendors who are under contract with a CSTL for cryptographic module or algorithm testing of a specific implementation(s) must contact the contracted CSTL for any questions concerning the test requirements and how they affect the testing of the implementation(s).

Once a vendor is under contract with a laboratory, NIST/CCCS will only provide official guidance and clarification for the vendor's module through the point of contact at the laboratory. In a situation where the vendor and laboratory are at an irresolvable impasse over a testing issue, the vendor may ask for clarification/resolution directly from NIST/CCCS. The point of contact at the laboratory **shall** be included on distribution of this correspondence. All correspondence from NIST/CCCS to the vendor on the issue will be issued through the laboratory point of contact.

Federal agencies and departments, and vendors not under contract with a CSTL who have specific questions about cryptographic module testing requirements or any aspect of the CMVP should contact the appropriate NIST and CCCS points of contact. Questions can either be submitted by e-mail, telephone, or written (if electronic document, Microsoft Word document format is preferred).

CSTLs must submit all test-specific questions in the Request for Guidance (RFG) format described below. These questions must be submitted to all points of contact.

2.5.1 Request for Guidance Details

Requests must be aimed at clarifying issues about cryptographic module testing or other aspects of the CMVP and must be submitted to the CMVP written in the RFG format described below.

A response may require internal review by both NIST and CCCS, as well as with others as necessary, and may require follow up questions from the CMVP. Therefore, such requests, while time sensitive, may not be immediate. If the CMVP has not sent feedback within a month's time, a follow up status request is recommended.

CMVP replies to RFGs will state current policy or interpretations with every attempt made to be accurate, consistent, and clear, on a timely basis. However, these are non-binding and subject to change once the full report submission is received.

Direct your RFG to both cmvp@nist.gov and cmvp@cyber.gc.ca. Do not send the requests to individuals.

The email will have the subject line "[ID]-FIPS140-3-RFG-[NAME]-yyMMdd" where ID is CSTL code (if not applicable, enter NA), NAME is the submitters name (e.g., CSTL, vendor, or other entity), and yyMMdd is the year, month, and day of submission.

Example 1: NA-FIPS140-3-RFG-VendorA-230630
Example 2: 01-FIPS140-3-RFG-CSTL_A-230630

2.5.2 Request for Guidance Format

For each RFG, the following information must be included, in the order outlined below:

1. **Clear indication of whether the RFG is PROPRIETARY or NON-PROPRIETARY**

   With a view to increased collaboration and transparency, if PROPRIETARY is not indicated (preferrable), the CMVP may make the RFG public in its entirety (e.g., posted to the Cryptographic Module User Forum (CMUF)). The CMVP will remove identifiable information if requested by the submitter.

   Whether NON-PROPRIETARY or PROPRIETARY, the CMVP may derive generalized guidance from the problem and response and share that guidance with the community (e.g., IG or CMUF).

2. **A descriptive title**

3. **A concise statement of the problem**

4. **A clear and unambiguous question regarding the problem**

5. **The configuration, embodiment of the module as it affects the answer**

6. **Applicable statement(s) from ISO/IEC 19790:2012**

7. **Applicable assertion(s), VE requirement(s), and test procedure(s) from ISO/IEC 24759:2017**

8. **Applicable assertion(s), VE requirement(s), and test procedure(s) from the SP 800-140**

9. **Applicable statements from FIPS 140-3 SP800-140A, B, C, D, E, and F**

10. **Applicable statements from FIPS 140-3 Implementation Guidance**

11. **Applicable statements from algorithmic standards**

12. **Additional background information if applicable, including any previous CMVP or CAVP official rulings or guidance**

13. A proposed resolution by the submitter, with justification

2.5.3 Post Validation Inquiries

Once a module is validated and posted on the NIST CMVP web site, many parties review and scrutinize the merits of the validation. These parties may be potential procurers of the module, competitors, academics, or others. If a party performing a post-validation review believes that a conformance requirement has not been met and this was not determined during testing or subsequent validation review, the party may submit an inquiry to the CMVP for review.

An Official Request must be submitted to the CMVP in writing with signature following the guidelines above. If the requestor represents an organization, the official request must be on the organization's letterhead. The assertions must be objective and not subjective. The module must be identified by reference to the validation certificate number(s). The specific technical details must be identified and the relationship to the specific FIPS 140 Derived Test Requirements assertions must be identified. The request must be non-proprietary and not prevent further distribution by the CMVP.

The CMVP will distribute the unmodified official request to the CSTL that performed the conformance testing of the identified module. The CSTL may choose to include participation of the vendor of the identified module during its determination of the merits of the inquiry. Once the CSTL has completed its review, it will provide to the CMVP a response with rationale on the technical validity regarding the merits of the official request.

The CSTL will state its position whether its review of the official request regarding the module:

1. is without merit and the validation of the module is unchanged.
2. has merit and the validation of the module is affected. The CSTL will further state its recommendations regarding the impact to the validation.

The CMVP will review the CSTL's position and rationale supporting its conclusion. If the CMVP concurs that the official request is without merit, no further action is taken. If the CMVP concurs that the official request has merit, a security risk assessment will be performed regarding the non-conformance issue. Please see Annex A for the flow diagram illustrating the assessment process.

2.6 Roles and Responsibilities of Program Participants

The various roles and responsibilities of the participants in the CMVP are illustrated in Figure 1 below.

Who	Vendor	CSTL	CMVP	User
Function	Designs & Produces	Tests for Conformance	Reviews & Approves	Specifies & Purchases

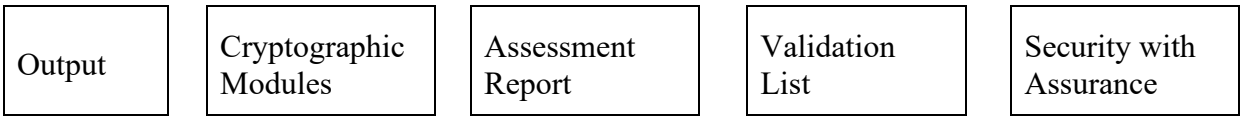

Figure 1 - Roles, Responsibilities, and Output in the CMVP Process

2.6.1 Vendor

The role of the vendor is to design and produce cryptographic modules that comply with the requirements specified in the applicable ISO/IEC standards and NIST SPs. Among other functions, the vendor defines the boundary of the cryptographic module, determines its modes of operation and its associated services, and develops an entropy and algorithm strategy and its non-proprietary security policy. When a cryptographic module is ready for testing, the vendor submits the module and the associated documentation to the accredited CSTL of its choice.

After the cryptographic module has been validated, the vendor manages post module validation through either a new validation or a revalidation process submitted by a CSTL. Any change to the module that is not part of either a validation or revalidation will invalidate the module.

2.6.2 Cryptographic and Security Testing Laboratory

The role of the CSTL is to independently test the cryptographic module to the requirements defined for the FIPS 140-3 security level and embodiment, and to produce a written test report for the CMVP Validation Authorities based on its findings. The CSTL conducts algorithmic testing and verifies compliance to the algorithm standards (requirements may be more than what is CAVP-tested), reviews the cryptographic module's documentation and source code, and performs requirements testing of the module in accordance with the TR, SP 800-140*x* and IG. If a cryptographic module conforms to all the requirements of the standards, the CSTL submits a written report to the Validation Authority. If a cryptographic module does not meet one (or more) requirements, the CSTL works with the vendor to resolve all discrepancies prior to submitting the validation package to the Validation Authority.

The following information is supplemental to the guidance provided by NVLAP, and further defines the separation of the design, consulting, and testing roles of the laboratories. The CMVP policy in this area is as follows:

1. A CSTL may not perform validation testing on a module for which the laboratory has:
    a. designed any part of the module,
    b. developed original documentation (e.g., design specifications) for any part of the module,
    c. built, coded, or implemented any part of the module, or
    d. any ownership or vested interest in the module.
2. Provided that a CSTL has met the above requirements, the laboratory may perform validation testing on modules produced by a company when:
    a. the laboratory has no ownership in the company,
    b. the laboratory has a completely separate management from the company, and

c. business between the CSTL and the company is performed under contractual agreements, as done with other clients.

3. A CSTL may perform consulting services to provide clarification of the *Security requirements for cryptographic modules*, the *Test requirements for cryptographic modules*, and other associated documents at any time during the life cycle of the module.

4. A CSTL may also create the Finite State Model (FSM), Security Policy, Entropy Assessment Report (EAR) for an Entropy Source Validation, entropy Public Use Document (PUD), Non-administrator guidance and Administrator guidance which are specified as vendor documentation in FIPS 140-3. These must be taken from existing vendor documentation for an existing cryptographic module (post-design and post-development) and consolidated or reformatted from the existing information (from multiple sources) into a set format. CMVP **shall** be notified of this at the time of submission. The CSTL must be able to show a mapping from the consolidated or reformatted CSTL-created documentation back the original vendor source documentation. The mapping(s) must be maintained by the CSTL as part of the validation records. Source code information is considered vendor-provided documentation and may be used in the CSTL-created documentation.

2.6.3 CMVP Validation Authorities

The CMVP Validation Authority is a joint effort of the National Institute of Standards and Technology for the Government of the United States of America and the Canadian Centre for Cyber Security for the Government of Canada.

The role of the Validation Authorities is to establish a program to validate the testing for every cryptographic module. The tests are performed, and results are documented in the submission package prepared by a CSTL and reviewed by the CMVP. If the cryptographic module is determined to be compliant, then the module is validated, a validation certificate is issued, and the on-line validation list is updated. During the review process, the Validation Authorities submit any questions they may have to the CSTL. The questions are typically technical in nature and are intended to ensure that the cryptographic module meets the requirements of the standard and that the information provided is accurate and complete. The CSTL may need to re-submit the validation submission along with supporting documentation such as a draft validation certificate, validation report, or security policy.

The CMVP participates, on behalf of NVLAP, in the CSTL accreditation process which includes the review of the management system manual, creating and administering the proficiency exam, performing the on-site assessment and the oversight of the artifact testing.

2.6.4 Validated Module User

The user verifies that a cryptographic module that they are considering procuring has been validated and meets their requirements. A listing of validated cryptographic modules is available from https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules/Search. A non-proprietary security policy is posted on the list for each validated cryptographic module so that a potential user can determine if the validated

cryptographic module provides cryptographic services and protection required for their particular application and threat environment.

The CMVP validates specific versions of a cryptographic module, and the user must verify that the version procured is in fact the validated version. The version numbers for a validated cryptographic module are specified on the CMVP web site and in the latest Security Policy.

Users can also develop product or system specifications that include the requirements for FIPS 140-3 validated cryptographic modules. It is important to note that a cryptographic module may be a complete product or a component thereof. Therefore, understanding the boundary and interface of the validated cryptographic module will help in the determination of an adequate cryptographic product.

2.7 CMVP Meetings

The CMVP is jointly managed by NIST and CCCS. Decisions are made jointly by both organizations with the NIST and the CCCS Program Managers communicating regularly. While most CMVP internal meetings focus on interactions with the CSTL, the CSTL Manager Meeting is focused on assessments and improvements of the CMVP program operations and management.

2.7.1 CSTL Manager Meetings

NIST and CCCS organize CSTL manager meetings (typically annually) to discuss issues relating to the CMVP, CAVP, and CSTLs. An agenda is created and distributed to the CSTLs before the meetings and presentation materials are distributed to the CSTLs for reference following the meetings. CSTL managers are welcomed to add any new agenda items at any time. Typically, the CSTL manager meetings are to include only CSTL managers and the CMVP and CAVP Validation Authorities, however CSTL staff may be invited to attend, space permitting. It is mandatory for CSTLs to have at least one attendee at the CMVP Lab Manager's meeting.

Usual discussion topics for CSTL manager meetings include the following:

- Status of Cryptographic Module Validation Program
- Changed or new CMVP processes and/or procedures
- Standards updates
- Laboratory accreditation process update news
- Implementation Guidance in development
- Status of Cryptographic Algorithm Validation Program
- Test tool development
- Upcoming meetings and/or symposiums

When possible, CSTL manager meetings are collocated with the annual International Cryptographic Module Conference (ICMC) so that CMVP and CSTLs can also directly interact with the community at large.

2.7.2 CMUF participation

The Cryptographic Module User Forum (CMUF) was established in 2013 by module vendors, users, and CSTLs to provide a platform for practitioners in the community of UNCLASSIFIED Cryptographic Module (CM) and UNCLASSIFIED Cryptographic Algorithm (CA) Validation Programs (VP). The CMUF formed the annual ICMC which was held along with the CSTL manager meetings. CMVP participated in the Conference and found the ICMC to be an excellent way to communicate with the community at large.

In recent years, CMUF has asked CMVP to attend and present at the scheduled (e.g., monthly) meetings. In this way, CMVP has been able to communicate with both CSTLs and vendors to define the planning and goals more clearly, while accepting feedback from the community. It has also allowed CMVP to hear programmatic issues that vendors and CSTLs are experiencing or anticipating in which CMVP may not have adequate awareness.

2.8 Confidentiality of Information

The protection of vendor proprietary information is paramount to the success and credibility of the CMVP and CAVP. Proper safeguards must be implemented by NIST, CCCS, and the CSTLs to protect against unauthorized disclosure of vendors' proprietary information. Any potential or actual breach of confidentiality could have an adverse effect on the NIST, CCCS, a CSTL's accreditation, or the program.

As required by the CSTL accreditation standards listed in Section 3.1 of this manual, CSTLs are required to establish and implement procedures for protecting the integrity and confidentiality of data entry or collection, data storage, data transmission and data processing. CSTLs must encrypt and digitally sign cryptographic module validation test reports, and any proprietary information when these documents are submitted to NIST and/or CCCS.

NIST, CCCS, and the CSTLs must ensure that personnel joining or departing these organizations are advised of their responsibilities about safeguarding the vendor proprietary information they may have been authorized to access during their period of employment.

3 CSTL Processes

This section describes administrative processes affecting CSTLs, including the granting and maintenance of accreditation, confidentiality of information, code of ethics, management of test data, and documentation.

3.1 Accreditation of CMVP scopes for CSTLs

This section describes in general terms the process for a laboratory to become an accredited CSTL for scope 17CM under the National Voluntary Laboratory Accreditation Program (NVLAP). Candidate laboratories may optionally apply for NVLAP 17CM-NI at the same time. 17ESV is also supported by CMVP, though is considered a separate program. Laboratories are responsible for complying with the Cryptographic and Security Testing LAP which can be found at https://www.nist.gov/nvlap/cryptographic-and-security-testing-lap.

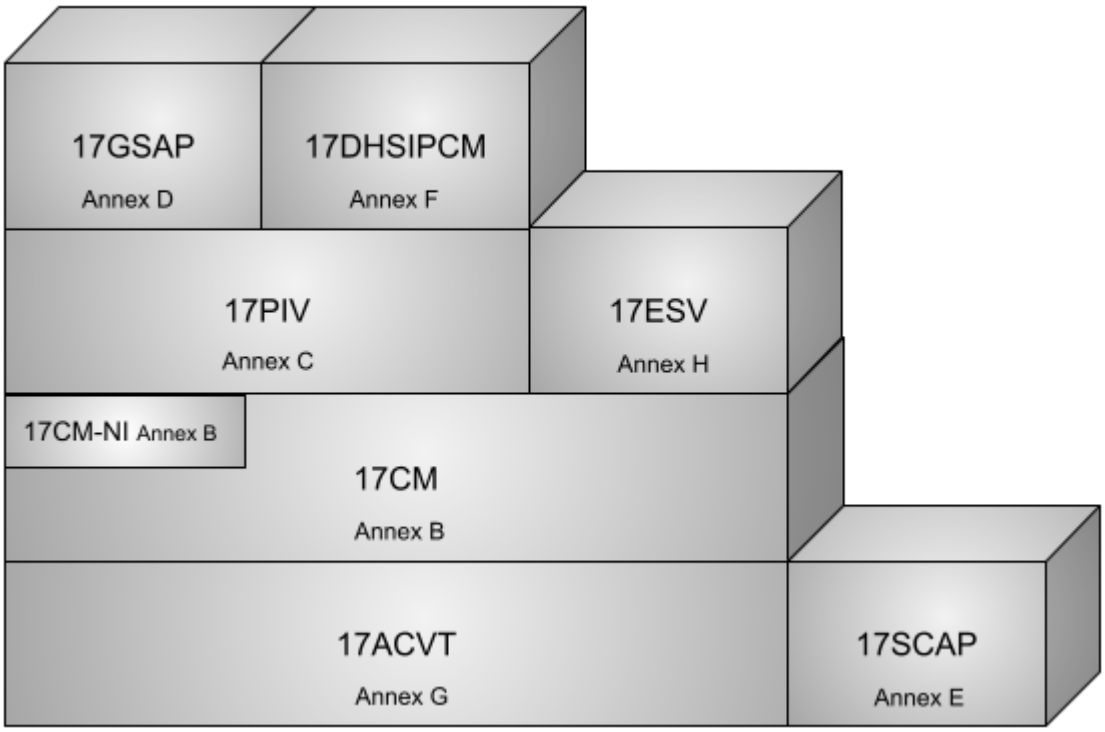

Figure 2 - CSTL NVLAP scopes

NOTE: Accreditation of the CAVP scope is necessary to obtain the 17CM scope for CMVP testing laboratories. For more information about CAVP accreditation, please see **Becoming a 17ACVT Laboratory** on the CAVP website https://csrc.nist.gov/Projects/cryptographic-algorithm-validation-program/how-to-access-acvts.

3.1.1 Accreditation Process for the CMVP scope

Applicant laboratories must complete the 17CM scope accreditation process within one year of

submission of the NVLAP application. Applications that are not completed within one year will have to be re-submitted and the process started again from the beginning. If the content of the accreditation process contained herein diverges from the aforementioned standards documents, those documents have precedence.

The accreditation process is illustrated in Figure 3. All steps in the accreditation process must be completed in the order shown.

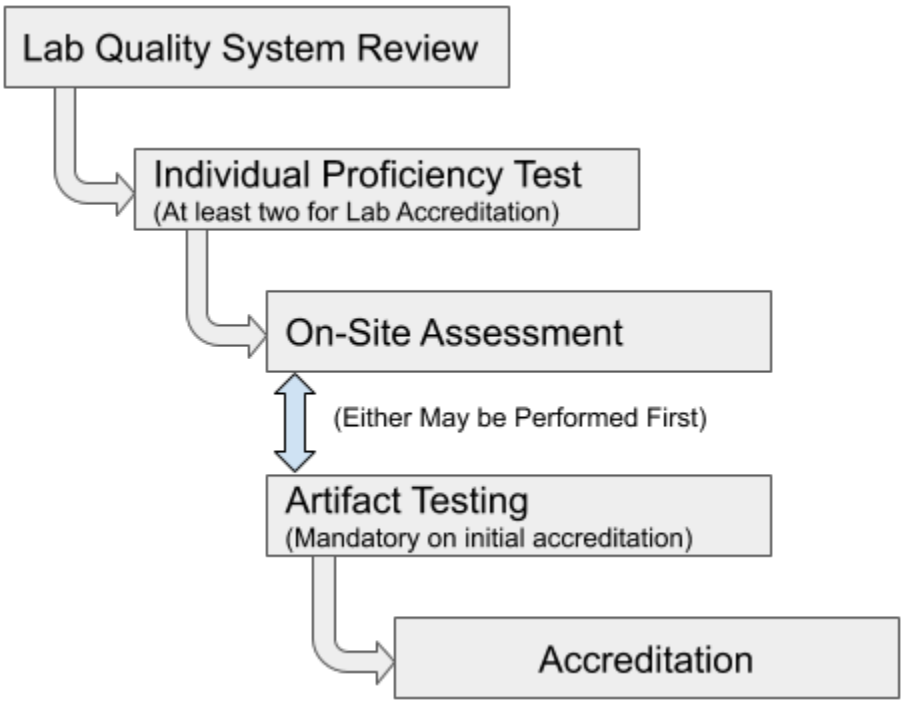

Figure 3 - CSTL Accreditation Process

3.1.1.1 Application for Accreditation and Selection of Assessment Team

The prospective CSTL must complete an application form, pay the respective fees, agree to the conditions of accreditation, and provide their quality system to NVLAP prior to the on-site assessment. Upon notification by NVLAP of an acceptable application, an assessment team is selected. This team is typically comprised of one or more technical assessors representing CMVP and one lead assessor from NVLAP. NVLAP technical assessors for CSTLs are selected by the NVLAP Program Manager and are chosen based upon their knowledge of the relevant FIPS standards and related documentation, NVLAP requirements, assessment techniques, and quality systems. The assessors must not have a conflict of interest with the CSTL they will be assessing.

3.1.1.2 Management System Evaluation

The assessment team will review the Management System to determine if it meets the requirements of NIST Handbook 150 and NIST Handbook 150-17.

3.1.1.3 CVP Proficiency Examination

Every independent tester, technical reviewer and submission signatory **shall** maintain Cryptographic Validation Program (CVP) certification by passing the current proficiency exam.

The current written examination consists of approximately one hundred questions relating to various aspects of CSTL activities, FIPS 140-3, and cryptographic algorithm implementation testing. The exam is an individual certification exam administered by a third-party organization. The certification exam will encompass the domains listed below:

- Physical Security
    - Understand the different module types and different embodiments for modules.
    - Understand requirements for physical security for modules specific to levels.
    - Understand requirements for physical security for modules specific to level 4.
- Authentication, Roles, Services, Software/Firmware Security and Operational Environment
    - Understand authentication requirements and concepts.
    - Define the requirements for roles.
    - Understand the concepts of services using approved and non-approved functions, and bypass.
    - Understand the self-initiated cryptographic output capability, Software/Firmware security including loading requirements and their applicability.
    - Describe the operational environment requirements/concepts and how to test them.
- Algorithms and Self-Test
    - Understand the concepts of the approved and allowed algorithms.
    - Identify which algorithms are approved or allowed.
    - Identify testing for components of the algorithms.
    - Identify the tester's responsibilities when reviewing an algorithm's implementation.
    - Identify the pre-operational self-tests (e.g., integrity, bypass) and know the associated requirements.
    - Understand the requirements for conditional and cryptographic self-tests.
- Sensitive Security Parameter (SSP) Establishment
    - Understand the requirements for SSP generation, SSP agreement, SSP transport and SSP derivation and applicable standards and guidance.
    - Understand and identify the approved random bit generators.
    - Understand the notion of entropy and methods of entropy estimation.
    - Possess general knowledge of the SSP establishment protocols and standards in the IT industry.

- SSP Management
  - Understand the requirements for SSP entry and output and trusted channels.
  - Understand the requirements for SSP storage.
  - Understand the various types of SSPs and their zeroization requirements.
- Security Assurances
  - Understand the requirements of module specification including degraded operation, approved and non-approved modes.
  - Understand the programmatic guidance and associated documentation requirements.
  - Understand the requirements for ports & interfaces, finite state model, development, mitigation of non-invasive and other attacks, and design assurance.

The exam is graded by an independent testing organization, and the results are provided to the CMVP. Scoring is adjusted for the difficulty of the exam taken, but transparent to the tester. The reexamination period for maintaining the certification for CVP certified testers is four years. In the event of major program updates, e.g., a new FIPS 140 standard, the reexamination frequency may be increased to encompass changes in the technical requirements. For the most up to date information, refer to the CVP Certification Exam Information tab on the CMVP website (https://csrc.nist.gov/projects/cryptographic-module-validation-program).

3.1.1.4 On-Site Assessment

An on-site assessment of the laboratory is conducted to determine compliance with the accreditation criteria. The on-site assessment is scheduled by the assessment team following receipt of payment and a passing grade on the CST Proficiency Examination by a minimum of two CST testers. An assessment typically takes two to three business days to perform. The activities performed during an assessment are described in Section 3.2 of NIST Handbook 150.

If deficiencies are found during the assessment of an **accredited** CSTL, the laboratory must submit a satisfactory plan concerning resolution of deficiencies to NVLAP within thirty days of notification.

If deficiencies are found during the assessment of an **applicant** CSTL, the accreditation process may be allowed to continue, on the condition that the laboratory must submit a satisfactory plan concerning resolution of deficiencies within thirty days of notification.

3.1.1.5 Artifact Testing

After two testers pass the CVP exam or following the on-site assessment, the assessment team may provide an artifact that the applicant laboratory must test according to the policies of the CMVP. Once completed, the applicant laboratory must submit the test report to the CMVP for their review. The CMVP will then assess the competency of the laboratory using the responses provided in the test report. The initial NVLAP application includes the testing of the artifact, all of which must be completed within one (1) year.

3.1.1.6 Accreditation Decision

The CMVP will make a recommendation to grant or deny the accreditation of the applicant laboratory. NVLAP will evaluate the results of the report on the laboratory and the recommendations of the CMVP, including any deficiencies and the corresponding response by the CSTL, before making the final accreditation decision.

3.1.1.7 Granting Accreditation

If approval has been granted to accredit the CSTL for Cryptographic Security testing, NVLAP will assign the CSTL one of four renewal dates for beginning of operation:

- January 1
- April 1
- July 1
- October 1

The accreditation period is one year. After initial accreditation, NVLAP will conduct an on-site assessment during the first year of accreditation and then every two years (see NIST HB 150, 3.2.3.3). The CSTL receives a NVLAP certificate and scope of accreditation identifying the CSTL address, lab code, the CSTL's authorized representative, and the expiration date of the accreditation.

3.1.1.8 CMVP Test Tools

Once accreditation has been granted and the CMVP is advised by NVLAP that the applicant laboratory has been accredited, the CMVP will issue to the newly accredited CSTL access to the latest version of Web Cryptik and associated tools. CMVP will also issue the latest programmatic directives and policies, and internal guidance and documentation. The CSTL is also required to have secure email capability using PGP to any IP communications that is not covered by Web Cryptik. The Lab is limited to two PGP email addresses in which to communicate with the CMVP, of which one may be a shared email address within the CSTL. PGP is not provided by the CMVP.

3.1.1.9 Cooperative Research and Development Agreement

All accredited CSTLs must execute a Cooperative Research and Development Agreement (CRADA) agreement with NIST in order to do business with the CMVP. The agreement covers protection of information as well as the fees being charged by NIST for each type of CMVP test report submission (scenario). This agreement is effective through October 31, 2026. The agreement may be reviewed and revised on an as needed basis. New laboratories are required to execute the agreement once they become accredited through NVLAP. Existing laboratories must re-execute the agreement upon change or expiration. The NIST CMVP Program Manager is the point of contact for obtaining a copy of the current CRADA.

3.2 Maintenance of CSTL Accreditation

3.2.1 Proficiency of CSTL

There is no requirement for a test report submission during the first year of accreditation. For all successive years of accreditation, the following requirements apply. An accredited CST laboratory must submit a minimum of three (3) test reports within the two-year period of the accreditation date. The laboratory must submit a minimum of one (1) test report within each

successive one-year accreditation cycle. For more information, see HB 150-17 Section B.3.5.3 *Minimum number of vendor product test reports*.

This permits the CMVP staff to monitor the quality of the laboratory processes, and the technical skills and knowledge of the laboratory staff. Failing this, NVLAP may suspend or revoke the laboratory's accreditation.

In addition, laboratories are also required to have a minimum of two CVP FIPS 140 Certified Testers throughout the accreditation period.

3.2.2 Renewal of Accreditation

Each accredited CSTL will receive a renewal application package before the expiration date of its accreditation to complete the renewal process. Fees for renewal are charged in accordance with the fee schedule published on the NVLAP website at https://www.nist.gov/nvlap/nvlap-fee-structure. Both the application and fees must be received by the accreditation body prior to expiration of the laboratory's current accreditation to avoid a lapse in accreditation.

On-site assessments of accredited laboratories are performed in accordance with the procedures in Section 3.3 of NIST Handbook 150. The re-accreditation process is the same as illustrated in Figure 3 - CSTL Accreditation Process and described in Section 3.1.1 above. If deficiencies are found during the assessment of an accredited laboratory, the laboratory must submit to NVLAP a satisfactory plan outlining the resolution of deficiencies within thirty days of notification.

3.2.3 Ownership of a CSTL

In the event a CSTL changes ownership, the accreditation body and the CMVP Validation Authorities must be informed within ten working days of the identity of the new owner of the laboratory and the effective date of the change. The laboratory must also submit an updated Quality System to NVLAP showing the new owner information.

3.2.4 Relocation of a CSTL

In the event a CSTL relocates to a new facility, the laboratory director must submit a relocation plan to the accreditation body and the CMVP at least one month before the relocation. The relocation plan must demonstrate that the new location meets the requirements as set out in the accreditation standards including information protection. The plan must also describe how sensitive information will be moved between locations. The accreditation body and the CMVP staff may conduct a monitoring visit after the relocation is completed to ensure all accreditation requirements continue to be met.

3.2.5 Change of Approved Signatories

In the event of a change of the CSTL's Approved Signatories, the accreditation body and the CMVP must be informed within thirty working days of the new signatories and the effective date of the change. All approved signatories must have passed the CVP exam prior to signing a validation submission.

3.2.6 Change of Key Laboratory Testing Staff

Key personnel include:

- laboratory director;
- laboratory manager(s);
- staff members(s) responsible for maintaining management system;
- authorized representative;
- approved signatories; and
- other key technical persons in the laboratory (e.g., testers).

In the event of changes to key laboratory testing staff, the accreditation body and the CMVP must be informed of the new staff and the effective date of the change within thirty working days. Failure to communicate laboratory staff changes to the accreditation body and the CMVP may result in an adverse action regarding accreditation. The laboratory must submit an updated organizational chart to NVLAP and the CMVP noting any changes.

3.2.7 Monitoring Visits

Monitoring visits may be conducted by the accreditation body at any time during the accreditation period, for cause or on a random basis. While most monitoring visits will be scheduled in advance with the laboratory, the accreditation body may conduct unannounced monitoring visits. The scope of the monitoring visits may range from an informal check of specific designated items to a complete review.

3.2.8 Suspension, Denial and Revocation of Accreditation

If the accreditation body becomes aware that an accredited laboratory has violated the terms of its accreditation, it may suspend the laboratory's accreditation or advise the laboratory of their intent to revoke the accreditation. The determination by the accreditation body whether to suspend the laboratory or to propose revocation of a laboratory's accreditation will depend on the nature of the violation(s).

Potential violations include but are not limited to, not performing tests in accordance with the standards, inadequate maintenance of CSTL equipment, or persistent process or technical shortfalls. An accredited laboratory **shall** maintain an Extended Cost Recovery (ECR) point total of less than 12 points. If a laboratory accumulates 12 or more points during the previous 2-year period, the accreditation for the cryptographic module testing will be suspended.

In order to pre-empt a suspension and assist the CSTLs through corrective action, if a CSTL reaches 9 to 11 points through the ECR process, the CMVP recommends the following actions:

The lab should compile a list of all reports in the Review Pending state in the CMVP queue. Per policy, those reports are eligible for resubmission. If the CSTL elects to review those submissions for potential resubmission, the CMVP may initiate up to a 30-day HOLD to allow the CSTL time to make any corrections needed prior to the reports moving to the In Review state. The CMVP would need to be notified in writing with regard to which reports, if any, the

CSTL would like to put on HOLD pending a resubmission. The final determination will be up to the CMVP.

ECR points are levied as follows:

0 points - Excessive number of modules in one report, or excessive submission size and/or complexity. Or for special exception requests received from the labs that create extra work for the CMVP.

1 to 4 points - Excessive comments; excessive comment rounds; missing, incomplete, or inconsistent documentation

5 points - Nonconformities such as a security-related issue or inaccurate representation of a module

Laboratories that fail to maintain a minimum of two CVP certified testers during their accreditation cycle will be suspended.

Discovery of serious violations such as breach of information confidentiality will result in an immediate recommendation by the CMVP to the accreditation body to suspend the CSTL's accreditation while an investigation is conducted, and necessary corrective actions are taken.

3.2.9 Voluntary Termination of the CSTL

A CSTL may at any time terminate its participation and responsibilities as an accredited laboratory by advising the accreditation body and the CMVP Validation Authorities in writing of its intent. Upon receipt of a request for termination, the accreditation body **shall** begin the termination process by notifying the laboratory that its accreditation has been terminated. The laboratory will be instructed to return its Certificate and Scope of Accreditation and to remove the accreditation body's logos from all test reports, correspondence, and advertising. Finally, the laboratory **shall** return or provide signed confirmation of the destruction of all CMVP and CAVP provided material, test tools and documentation. The CMVP will determine the course of action taken for any outstanding work that has not been completed. This will be handled on a case-by-case basis.

3.3 Confidentiality of Proprietary Information

Maintaining confidentiality of proprietary information is paramount to the operation of the CMVP and requires the establishment and enforcement of appropriate controls.

3.3.1 Confidentiality of Proprietary Information Exchanged between NIST, CCCS and the CSTL

The confidentiality of the proprietary information exchanged between NIST, CCCS and the CSTL is required by the NVLAP at all times during and following the testing. All proprietary materials must be marked as PROPRIETARY by the CSTL or the vendor.

3.3.2 Non-Disclosure Agreement for Current and Former Employees

The CSTL must develop and maintain non-disclosure agreements for staff that participate in the

testing of modules.

3.4 Code of Ethics for CSTLs

The laboratory **shall**:

1) Maintain ISO/IEC 17025 NVLAP accreditation for the Cryptographic Security Testing Program;
2) Refrain from misrepresenting the scope of its accreditation;
3) Act legally and honestly;
4) Act ethically.

3.5 Management of CMVP and CAVP Test Tools

Test tools provided by NIST and CCCS **shall** not be distributed to any entity outside the CSTL, including firms contracted by the CSTL, unless explicitly authorized by CMVP management. Personnel temporarily employed by and working under the supervision of a CSTL (i.e., a contractor) can use the provided test tools when they are used within the CSTL facilities. Test tools include all versions of Web Cryptik, the Automated Cryptographic Validation Testing System (ACVTS) and any other tools developed by NIST and CCCS for use by the CMVP and CAVP. Violation of this policy may be considered cause for suspension of the CSTL's accreditation.

4 CMVP Processes

This section describes cryptographic module validation processes, including an overview of the program and the steps required to attain and maintain validation.

4.1 Cryptographic Module Validation Process Overview

This section provides a high-level overview of the validation program, primarily focused on the CSTL and CMVP interaction, followed by the vendor and laboratory interaction. The remaining subparagraphs work through the process performed by the vendor, CSTL, and CMVP for any submission, including full submissions and resubmissions. Figure 4 shows the general flow of testing and validation of a cryptographic module.

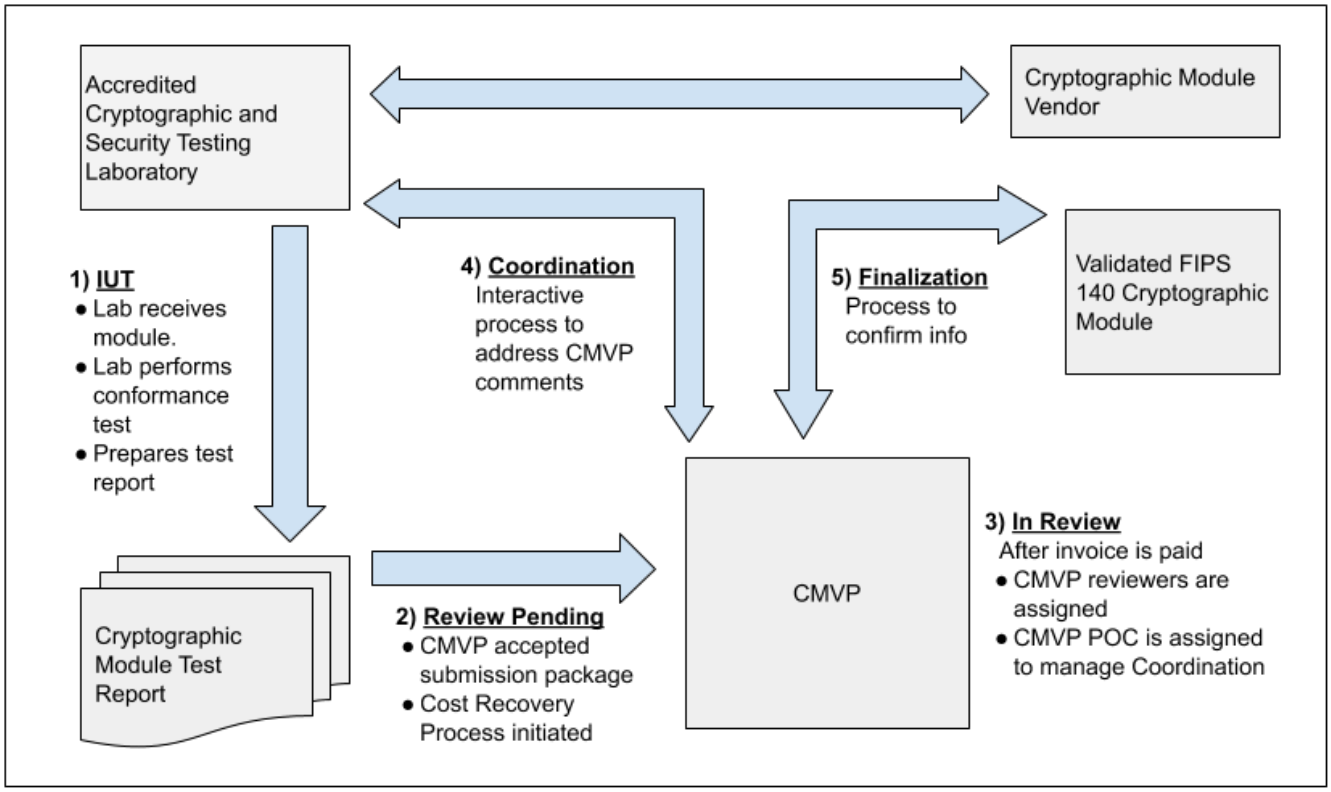

Figure 4- Cryptographic Module Testing and Validation Process

4.1.1 Vendor, CSTL, and CMVP duties for Testing of the Cryptographic Module

A vendor contracts with an accredited CSTL to perform the cryptographic module validation testing. The vendor provides the laboratory with the necessary documentation and either provides the cryptographic module to the laboratory for testing or prepares it for testing at the vendor's facility.

In order to communicate specific validation information to CMVP, the CSTL **shall** assign a Tracking Identification Number (TID). The first two digits of the TID are assigned by the CMVP once laboratory accredited, the second set of four digits is assigned by the laboratory which must

be unique to the validation, and the last four digits are "0000" unless otherwise specified, when the validation submission is accepted. In all, a ten-digit TID number is created and used to track the submission. Most communications with the CMVP are aided by the use of Web Cryptik with attachments as indicated in the Web Cryptik User Guide. For the latest information refer to the Web Cryptik User Guide.

4.1.1.1 Implementation Under Test

Once the documentation is delivered to the laboratory and the cryptographic module is available for testing, and with the vendor's agreement, the laboratory may optionally notify the CMVP that the cryptographic module is to be included on the IUT List. The laboratory provides the name of the cryptographic module and the cryptographic module vendor's name and indicates that this information is to appear in the IUT List. Inclusion in this list is voluntary. The module on the IUT List will be removed after 18 months. The CSTL will be notified when the IUT is dropped.

The CSTL performs the cryptographic module testing as prescribed by the ISO/IEC 24759:2017 Test Requirements, SP 800-140 and applicable IGs, entering all testing assessments in the Web Cryptik tool. Although testing requirements are in the ISO/IEC 24759:2017 TR, ISO/IEC 19790:2012, *Security Requirements for Cryptographic Modules* remains the definitive reference for whether or not the cryptographic module meets the requirements of the standard. The SP 800-140 series and Implementation Guidance (IG) provides clarifications of the CMVP, and in particular, clarifications and guidance pertaining to the TR. Cryptographic algorithm and/or random number generator validation testing may also need to be done as part of the FIPS 140-3 validation testing.

The cryptographic module validation process is an iterative process. At any point in the testing the CSTL may wish to request guidance from CCCS and NIST in determining how to apply the FIPS 140 standard to the particular cryptographic module. If the CSTL discovers any non-conformances in the cryptographic module documentation or the cryptographic module itself, it must bring details of the non-conformance(s) to the attention of the cryptographic module vendor. The cryptographic module vendor must correct the non-conformance(s) and resubmit updated documentation and the updated cryptographic module as necessary for validation testing.

Once the CSTL completes all required validation testing and has determined that the cryptographic module is conformant to FIPS 140-3, the laboratory prepares the validation submission. In responding to assessments through Web Cryptik, the CSTL addresses each TE independently, not by referencing a response in another TE. Having to search and piece together information increases the CMVP review time and may facilitate a NIST ECR Fee and possible points.

Once the testing is completed and the CSTL confirms the module meets all requirements, the CSTL prepares the test submission package and sends it to CMVP for validation. See the Web Cryptik User Guide for a summary table that describes what must be submitted by the laboratory for validation. Web Cryptik aids the CSTL in preparing submissions, please refer to the Web Cryptik User Guide for additional information.

4.1.1.2 Review pending

All FIPS 140 validation submissions received by the CMVP are examined to assure a full package was received. If the initial examination reveals issues, the CSTL is notified, and the

submission is not accepted for review. When the submission is accepted by the CMVP, the module is moved to the REVIEW PENDING stage of the MIP List. The module will remain in the REVIEW PENDING stage until the NIST Cost Recovery fee is paid and the first reviewer begins the review.

During periods when the CMVP submission queue is long, CSTLs are encouraged to submit updated submissions to minimize any follow-on revalidations that might be necessary (see Section 4.4.5 *Resubmission while in Review Pending*). The CSTL should advise the CMVP of expected updates prior to their submission.

4.1.1.3 Test Report Review

When the reviewer begins the review, the cryptographic module is moved to the IN REVIEW stage of the MIP List. The module validation must be completed and cannot exceed 24 months after transitioning to IN REVIEW. IN REVIEW indicates that CMVP reviewers have been assigned to the submission. Once they have completed their review of the validation submission and provided comments, a comment file is sent to the CSTL. The CSTL must respond within 90 days to prevent the review being placed on hold. During long submission queues, the CSTL may ask for minor updates that would otherwise require a revalidation submission to be incorporated into the current submission. CMVP will consider this and will respond in a timely fashion. The cryptographic module is then moved to the COORDINATION stage.

4.1.1.4 Coordination

After conferring with the vendor, as necessary, the CSTL addresses the comments and resubmits a complete submission package containing any modified documents. The reviewers examine the responses and respond with any additional comments if necessary. Additional rounds due to errors or complex issues may result in a NIST ECR Fee and possible points. This process continues until the CSTL receives an All OK from CMVP. Each round of comments will result in an update in the MIP List Coordination date. See Section 4.4.6 *Changes while in Coordination* for more information.

4.1.1.5 Finalization

The FINALIZATION stage focuses on assuring any changes during the coordination phase have been updated by the CSTL. In addition, the CSTL is asked to review and confirm with CMVP the vendor and module information is accurate. With the completion of the submission review, the validation is posted on the CMVP website.

4.1.1.6 Validation Certificate

When NIST and CCCS are satisfied with the test report, the finalized comment file and the electronic version of the draft validation certificate is sent to the CSTL. The CSTL must review and confirm or correct the information on the certificate. Once the information is confirmed, the Validation Authorities, issue a certificate number which is added to the database. The web-based search tool for the database can be found at https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules/Search. An entry includes the version number of the validated cryptographic module and benchmark configuration of the original validation testing.

The information on the certificate pertains to the module from the time of its validation. During validation life cycle, information for that validation may change. For revalidations that do not create a separate validation number, the module's validation will be updated on the website and

the dates of the updates and the CSTLs that submitted the updates are appended to the entry. Therefore, users should refer to the NIST website for the latest information concerning a validation. A Consolidated Certificate is generated at the end of each month which lists all of the certificates that were published during the month. CCCS and NIST sign the consolidated certificate listing and it is posted as a link on each of the individual module validation entries

4.2 Implementation Under Test (IUT) and Modules in Process (MIP)

The *CMVP Implementation Under Test (IUT) and Modules In Process (MIP) Lists* are provided for information purposes only. Participation on the list is *voluntary* and is a joint decision by the vendor and the CSTL. Modules are listed alphabetically by name.

The IUT List provides the Module Name, Vendor Name, FIPS 140 standard and the date of the last update from the CSTL under contract to perform the testing. Not all modules being tested are listed, as the listing is optional.

Similarly, if a vendor and CSTL chose not to list the module on the MIP List, the module will be reflected at the end of the list in the "Not Displayed" row. If the CSTL requests the listing be posted, the Module Name, Vendor Name (and expandable contact information), FIPS 140 standard, the submission status (including the current MIP state and the date of the last MIP state change) will be shown. Posting on the list does not imply or guarantee FIPS 140 validation.

The IUT and MIP Lists are explained and accessible on the NIST webpage https://csrc.nist.gov/Projects/cryptographic-module-validation-program/modules-in-process.

4.3 Submission Scenarios

There are twelve possible FIPS 140-3 submission Scenarios:

Full Submission (FS), Vendor Update (VUP), Vendor Affirmed Operating Environment (VAOE), Non-Security Relevant (NSRL), Algorithm Update (ALG), Operating Environment Update (OEUP), Rebrand (RBND), Port Sub Chip (PTSC), Update (UPDT), Common Vulnerabilities and Exposures (CVE), Algorithm Transition (TRNS), and Physical Enclosure (PHYS). See Section 7.1 for details for each of these scenarios.

4.4 Validation Submission Queue Processing

4.4.1 Full and Update Submission Validations

Modules submitted for initial validation (FS) and those submitted with less than 30% security changes (UPDT) will be queued together and addressed on a first-come, first-serve basis. All submissions in this queue must meet all requirements as of the submission date. The internal review disposition of a module report is left to the sole discretion of the NIST and CCCS CMVP program managers. If additional time is required due to complexity or errors, additional cost and possible points may be required in the form of a NIST ECR. The status of these submissions can be tracked through the MIP List on the webpage at https://csrc.nist.gov/Projects/cryptographic-module-validation-program/modules-in-process/Modules-In-Process-List. Vendors should work

with their CSTL for any additional information.

In cases whereby submissions are related to or dependent on other submissions, especially for bound or embedded modules, the CMVP must be notified for consideration prior to their submission and added to the special instructions field in Web Cryptik. This will allow CMVP to manage resources in support of these larger efforts. If a submission is put on hold due to dependency, it is the responsibility of the lab to notify the CMVP when the initial submission is completed in order for the CMVP to remove the hold on related or dependent submissions. In general, and for dependent or related modules, testing must be completed prior to submission (including CAVP and/or ESV certificates).

4.4.2 All other submissions

Separate queue(s) are maintained by the CMVP internally to maximize throughputs for all other submissions, as they are expected to require less intense review and faster turnaround. If additional resources are required, an ECR Fee and possible points could be levied or a new submission as a full validation may be required.

4.4.3 HOLD Status for Cryptographic Modules on the Modules In Process

HOLD status can be initiated by the CMVP only. There are several reasons that a submission review may be placed on HOLD status. Some of these reasons are as follows:

1. If a module test report is sent incomplete or is determined to be incomplete once the module has moved to the IN REVIEW or a later stage, a NIST ECR Fee and points will apply. When the ECR is agreed to by the CSTL, the module will be placed on HOLD. If the ECR has been paid and the CSTL resubmits the report, the HOLD is removed.
2. If a non-compliance issue is discovered during module IN REVIEW or later a NIST ECR Fee and points will apply. When the ECR is agreed to by the CSTL, the module will be placed on HOLD. If the ECR has been paid and the CSTL resubmits the report, the HOLD is removed.
3. If a module is dependent on the completion of another module, the dependent module may be placed on HOLD until the base validation has been completed. The CSTL must indicate the module dependency upon submission via Special Instructions.
4. During COORDINATION, CMVP comments are sent to the lab and if the lab has not responded within 90 calendar days, the module will be placed on HOLD and removed from the MIP List.
5. A CSTL has been placed in a suspension status by NVLAP. All work in progress will be placed in a HOLD until the suspension is lifted. No new work may be submitted during a period of suspension.

In general, a module that is on HOLD will be removed from the MIP List and placed on the IUT List. While the MIP status will be the same after coming out of HOLD, it may or may not retain its position in the queue depending on what the module state was prior to going on HOLD (i.e., once the HOLD is removed, REVIEW PENDING or earlier will not retain its position while IN REVIEW or later will retain its position in the queue).

4.4.4 Validation Deadline

CMVP drops consideration of modules that have not completed the validation process within 2 years from being placed in IN REVIEW status. The CSTL will be notified 30 days prior to the termination of the submission. When the module is dropped, the vendor and lab must restart the validation process including paying a new cost recovery fee at the current rate. This applies to all submissions currently in the process as well as to new submissions.

4.4.5 Resubmission while in Review Pending

An updated submission may be provided to the CMVP while in review pending under the following rules:

1. The updated submission will REPLACE (as opposed to ADD to) the previous submission and will keep its place in queue.
2. This is not to be used as a placeholder until testing is completed, and penalties may be applied if misused. For example, the initial submission must have been the intended version to be validated, but unforeseen and necessary updates may need to be addressed while still in review pending (e.g., addressing CMVP checklist items, or non-security relevant bug fixes).
3. Full testing or regression testing may apply depending on the changes (following the guidance specified in Section 7.1 *Submission Scenarios*).
4. Updates to improve documentation is encouraged to ensure accurate, quality reports and avoid ECR.

4.4.6 Changes while in Coordination

An updated submission may be provided to the CMVP while in coordination under the following rules:

1. The updated submission will REPLACE (as opposed to ADD to) the previous submission and will keep its place in queue.
2. Changes are purely documentational (no module code changes) UNLESS non-security relevant that do not require regression testing (following the guidance specified in Section 7.1 *Submission Scenarios*). The change summary is provided to the CMVP (may be part of the Comment document).
3. This is not to be used as a placeholder until testing is completed, and penalties may be applied if misused. For example, the initial submission must have been the intended version to be validated, with unforeseen and necessary updates while in coordination (e.g., addressing CMVP checklist items, or non-security relevant bug fixes).
4. Full testing or regression testing may apply depending on the changes (following the guidance specified in Section 7.1 *Submission Scenarios*).
5. Updates to improve documentation is encouraged to ensure accurate, quality reports and avoid ECR.

6. If changes are not purely documentational, the CSTL must submit an RFG to the CMVP (see Section 2.5) indicating the hardship justification and on how the above 5 items are met prior to submission.

Please be aware, the review may be delayed and an ECR may apply for complexity (time incurred) depending on the impact of the changes.

Note: post-validation, additional changes can be made using the revalidation scenarios per Section 7.1 of this document.

4.5 Validation when Test Reports are not Reviewed by both Validation Authorities

In rare occasions, laws from either country or other unusual circumstances prevent the release of product information outside its borders for specific products. In those occasions both Validation Authorities will be advised of the circumstances and the Validation Authority from that country will carry out the validation process on its own and will present the certificate to the other Validation Authority for its signature (where applicable).

4.5.1 Controlled Unclassified Information

If a CMVP test report is received from a CSTL and it is identified in the cover letter that it is subject to the International Traffic in Arms Regulations[1] (ITAR), the following CMVP programmatic guidance will be adhered to:

4.5.1.1 CMVP ITAR Guidance

1. Report submission as specified in Web Cryptik applies and should include the following changes from a normal submission:
    a. A proprietary security policy [PDF] submitted in lieu of a non-proprietary security policy.
    b. Provide a signed letter of affirmation from the vendor stating the applicability of ITAR to the submitted test report.
    c. To satisfy binding of Cryptographic Algorithm Validation Certificates, (see IG 2.3.A), the test report must affirm that the CSTL has PDF images (front and back) for any ITAR cryptographic algorithm validation certificates, where the algorithm web site will not have any detailed information.
    d. The test report package is submitted only to NIST CMVP. The TID field will be formatted as: TID-*nn*-*nnnn*-ITAR. The characters ITAR will replace the field that was allocated for the CCCS TID.

[1] Example: **Not Releasable to Foreign Persons or Representatives of a Foreign Interest.**

INFORMATION SUBJECT TO EXPORT CONTROL LAWS of the UNITED STATES of AMERICA

Information subject to the export control laws. This document, which includes any attachments and exhibits hereto, may contain information subject to the International Traffic in Arms Regulation (ITAR) or Export Administration Regulation (EAR). This information may not be exported, released, or disclosed to foreign persons inside or outside the United States without first obtaining the proper export authority. Violators of ITAR or EAR are subject to civil and criminal fines and penalties under Title 22 U.S.C. Section 2778, and Title 50, U.S.C. 2410. Recipient **shall** include this notice with any reproduced portion of this document.

e. Actual module names, version numbers, and vendor information will be provided. This information will not be masked by dummy information.

2. Report review
   a. Each ITAR report will be reviewed by NIST reviewers.
3. Certificate generation and posting
   a. Certificates will be prepared by NIST only.
   b. Certificates will be signed only by NIST. The CCCS signature field will be marked as: Not Applicable – ITAR.
   c. The NIST CMVP web page will only post the following information: Certificate number, applicable FIPS standard, Status, Module Type, Embodiment, Validation Date, Sunset Date and Overall Level. It will also include the testing Lab and associated NVLAP Code.
   d. The official certificate will be sent to the CSTL for presentation to the vendor.
4. Re-validation
   a. All re-validation changes will result in a new certificate sent to the CSTL for presentation to the vendor since the web site will not have any identifiable information.
   b. Report submission, report review, certificate generation and posting as outlined above and following the submission requirements.

4.6 CMVP Fees[2]

Fees are charged to the CSTL by NIST CMVP to offset the cost of the validation authority activities performed by NIST CMVP. Cost recovery fees are collected depending on the scenario as listed in section 4.4. Extended Cost recovery fees are collected when the submission review is in excess of the allotted resources.

4.6.1 Cost Recovery Fee

Cost recovery (CR) is a fee charged to the CSTL by NIST CMVP to offset the cost of the validation authority activities performed by NIST CMVP. The fee is applied to new module submissions and modified module submissions.

Fees charged by NIST as part of the cost recovery program are listed on: https://csrc.nist.gov/Projects/cryptographic-module-validation-program/nist-cost-recovery-fees.

4.6.2 Extended Cost Recovery Fee

An extended cost recovery (ECR) fee is applicable when a report submission requires significant

[2] CCCS does not levy any charges for the validation of cryptographic modules.

additional review effort by the validators. The extended fee may be applied to all report submissions. The CMVP will review the rationale for the application of the ECR fee and possible points with the CSTL before determination of its applicability. The ECR fee is billed separately from any applicable CR fee and must be remitted prior to validation. The ECR fee varies by submission type and security level.

A number of factors may lead to an ECR fee and possible points:

Complexity

Typically, a report submitted by the CSTL to the CMVP addresses a single module. If the module represents a new technology, new type of fabrication or unique implementation, an unusual level of complexity and/or many functions and services; the review time will exceed the average and ECR will be applied.

If the single report submission represents many modules, the review time will increase based on the quantity and module differences. If the review exceeds the average time an ECR will be applied or the report may be rejected unless the report is simplified, typically by reducing the number of modules to a more unified set.

Additionally, technical issues resulting in a significant effort by CMVP to determine how new or unusual applications apply to the testing standards would result in the application of ECR.

Quality

Errors in the CSTL's submission package or following an incorrect process can cause a significant effort by CMVP to identify and work with the CSTL to discover and correct; ECR will be applied.

An ECR may be applied if, during CMVP review and coordination, the CSTL generates many responses that result in unproductive rounds due to issues in the report such as: incomplete information, inconsistent information, insufficient information, or not following CMVP Implementation Guidance or adherence to the conformance requirements. Else, if significant or specialized effort is required by CMVP to resolve; an ECR will be applied. In addition, if during CMVP review and coordination it is discovered that the module is not conformant to FIPS 140 or CMVP Implementation Guidance, an ECR will be applied.

Fees charged by NIST as part of the cost recovery program are listed on: https://csrc.nist.gov/Projects/cryptographic-module-validation-program/nist-cost-recovery-fees.

4.6.3 NIST Payment Policy

NIST CMVP maintains the billing information for each CSTL. If the CSTL's information needs to be updated, contact NIST CMVP. Upon receipt of the CSTL's submission or a request for an invoice, NIST billing prepares an invoice and submits it to the identified payee. Only CSTLs with an active CRADA agreement will be invoiced by NIST billing. For questions about methods of payments and associated handling fees contact NIST Billing Information: 301-975-3880 or at billing@nist.gov.

The NIST CMVP fee schedule is published at https://csrc.nist.gov/Projects/cryptographic-module-validation-program/nist-cost-recovery-fees. Review of submissions will not begin until

NIST CMVP receives confirmation from NIST Receivables that the invoice has been paid.

4.6.4 Invoice for a Report Submission

Currently, the CR process is initiated upon receipt of the report submission and typically adds an average of 60 days to the validation process. The CR process can be initiated before the report submission. In order to initiate the CR process before the report submission. The lab **shall** send an IUTA using Web Cryptik indicating the correct number of modules, overall security level and submission type. The IUTA can be submitted without requesting that the module be placed on the IUT List. The IUTA must be successfully processed by the NIST CMVP automated system. When the submission is successfully processed, the lab will receive an automated response, "Thank *you for your submission".*

At any time after the lab receives the automated response to the IUTA, the lab has the option to send an IUTB to initiate the CR process before submitting the report. When the IUTB is successfully processed, the lab will receive an automated response, "Thank *you for your request. The cost recovery process for this submission has been initiated.*" Changes to the overall security level and submission type will not be accepted.

- If the lab sends an IUTB and then needs to cancel the invoice, the lab must send an IUTC. When the IUTC is successfully processed, the lab will receive the automated response, "Your *request has been received and will be processed. If there are any issues in cancelling the invoice, you will be notified.*"
- Once the invoice has been paid, the payment may be refunded if the module submission is dropped prior to the IN REVIEW stage.
- Only the vendor.json and report*.json file is required, where * is the section identifier of the report, for an IUTB or IUTC. See the Web Cryptik help for more information on this process.

Labs should note when the cost recovery process starts, no changes to the Security Level or Submission Type will be accepted. In addition, if a report has not been received by 90 days after the IUTB was accepted, the module will be moved to On Hold and removed from the IUT List. The module can be automatically removed from On Hold and placed on the MIP List by sending the report. If the lab chooses to not send an IUTB, the CR process will initiate upon receiving the report submission.

4.6.5 Request for Transition Period Extension

Some Implementation Guidance is assigned a transition period before compliance to this guidance is required; since meeting the guidance may likely require changes to cryptographic modules or the functional testing of them as opposed to documentation changes. In some instances, the transition period may not be long enough for the vendor to perform the modifications needed to the cryptographic module for it to be compliant with the issued Implementation Guidance nor complete the additional cryptographic algorithm validation testing before the scheduled date for submission of the validation report.

These situations will be reviewed on a case-by-case basis at the request of the CSTL performing the validation testing. A ruling will be made by the CMVP as to whether an extension can be

granted for this particular requirement, for this particular cryptographic module, depending on the type of cryptographic module and the status of the validation testing.

4.7 Flaw Discovery Handling Process

When a flaw is discovered in a **validated** cryptographic module and brought to the attention of the CMVP Validation Authorities, the following actions will be taken:

1. NIST, CCCS and the CSTL will investigate the allegation about the flaw, and determine its impact on the validation;
2. NIST and CCCS will decide whether the flaw requires the revocation of the validation, a caveat be placed on the entry in the *Cryptographic Module Validation List*, or no action;
3. NIST and CCCS may advise their respective federal departments of the flaw and its impact; and
4. NIST and CCCS may notify NVLAP about the possible shortfall with the CSTL's proficiency.

The diagram found in Annex A outlines the flaw discovery handling process. There are several ways for a flaw to be identified including a security-relevant CVE from the National Vulnerability Database (NVD).

4.8 Validation Revocation

FIPS 140 validation may be revoked for any one of the following reasons:

1. Discovery of a flaw in a validated cryptographic module or that the cryptographic module was validated using false information; or
2. Validated cryptographic module only implements cryptographic algorithm(s) that are no longer Approved.

The entry in the *Cryptographic Module Validation List* will be annotated as follows for each of these cases:

1. Discovered flaw; or
2. Algorithm(s) no longer Approved for US Federal Government use: *No longer meets FIPS 140 requirements and can no longer be used by a Federal agency*.

The Validation Authorities will jointly make the final decision on the validation revocation. The CSTL that performed the testing for the validation will be advised one week in advance of the upcoming validation revocation. If the validation certificate is revoked, it will appear on the *CMVP Validation List* with the validation status *Revoked*.

4.9 Entropy Source Validation (ESV) Processes

In April 2022, the CMVP introduced a new submission process for entropy sources leading to

standalone entropy source validation certificates. The validation certificates provide the assurance that a particular entropy source on a particular operating environment conforms to SP 800-90B and associated IGs.

Similar to ACVTS, the CMVP maintains two environments: a Demo ESVTS, and a Prod ESVTS. The Demo environment is for testing and becoming familiar with the platform. The Prod environment is for certification.

After December 2022, Prod ESVTS will be the only mechanism the CMVP allows on a new submission that requires a validation on an entropy source. Entropy source validation will no longer be accepted as part of a module submission (i.e., designated as ENT on the module certificate). Instead, the module submission must cite an existing entropy validation certificate. See Section 7.1.14 for additional information on ESV and ENT claims.

4.9.1 Entropy Source Validation Submissions

To submit to ESVTS, a client must be used to interact with the server. The CMVP provides two clients for use: an HTML-based WebClient, and a Python client. Both have their advantages and features. It is encouraged that a lab is familiar with both options.

Several files are expected to be included in the submissions. It is the best practice to have these ready before making the initial request to ESVTS. The files are as follows:

1. Entropy Assessment Report (EAR) – This file addresses the requirements in SP 800-90B and describes how the entropy source on the listed operating environments conforms to the standard and associated IGs.
2. Public Use Document (PUD) – This file provides information to a user that may incorporate or use the entropy source within a cryptographic module.
3. Data Files – These are files described in SP 800-90B that capture outputs from the entropy source. The files are subject to the SP 800-90B Entropy Assessment Tool available on GitHub. The number of files required depends on the entropy source being evaluated.

Part of the certify step is the inclusion of an Entropy Identifier (EID) that will help the lab track the submission as it goes through the review process. The EID must be four alphanumeric characters and must not repeat with previous EIDs used by the lab. This is similar to the TID used within the module review process. A string used as an EID may still be used as a TID and vice versa.

After a submission is sent for certification the CMVP will perform cost recovery before the submission is passed along for manual review. During the manual review, two CMVP entropy reviewers will confirm the documentation provided addresses all of the SP 800-90B requirements.

An ESV certificate has a reuse status of either “Reuse restricted to vendor” or “Open for reuse”.

“Reuse restricted to vendor” means:

- Any module that has the same vendor can use the ESV certificate with no additional permission, if the entropy source is portable to that module per the PUD guidance (e.g., identical environments, configuration steps, etc.).

- The vendor's name of the ESV certificate must match exactly with the module vendor name, unless the two vendors are part of the same company (e.g., different divisions with slightly different names, or a company is a subsidiary of another company that has a validation). This vendor relationship would need to be explained with evidence provided to the CMVP as part of the module submission.
- Someone other than the vendor can only use the certificate with written and signed permission from the vendor's point of contact (as indicated on the ESV certificate). The signed permission may be appended to the PUD of the certificate or be a separate document attached to the module submission package.

"Open for reuse" means any vendor can use that certificate without any specific permission from the ESV certificate vendor.

4.9.1.1 Entropy Source Validation WebClient

The WebClient provides forms that guide a submitter through the process. All information must be submitted at once including the EAR, PUD. Once a request is submitted to NIST, the user is expected to store the resulting output. This provides a way to follow up on the request if needed. The URL to access the WebClient is the base URL of the ESVTS environment. The WebClient is available for both Demo and Prod.

4.9.1.2 Entropy Source Validation Python Client

The Python Client provides a more automated way of submitting data to ESVTS. Requests may be made piecemeal when information becomes available. The user is expected to store the outputs from the tool. The tool automatically logs important information. The Python Client is controlled with JSON files to drive the functionality needed at the time. This allows a user to start making requests and pick them back up later. Configuration JSON files control if the Python Client is accessing Demo or Prod.

4.9.2 Entropy Source Validation Comment Remediation Process

When an entropy source submission is picked up for manual review, the lab will receive an email about the change in status of the submission. The reviewers will evaluate the claims made in the EAR, and evaluate the information provided in the PUD. If there are questions or comments about the submission, a file will be sent to the lab with PGP-encrypted email for further clarification. The email will have the subject line "EID-XX-YYYY-{transaction code}-yyMMddHHmm" where XX is the lab code, and YYYY is the four character EID provided during the certification request. On emails from the CMVP to the lab, the transaction code will be "CCOM#" where # is the number of comment rounds. For responses back to the CMVP, the lab must include the same subject line but the transaction code must be "LCOM#" where the # matches the latest number sent from the CMVP.

4.9.3 Entropy Source Validation Webpages

For more information about the ESV Process, see https://csrc.nist.gov/Projects/cryptographic-

module-validation-program/entropy-validations.

The ESV Certificate List is available on CSRC. See https://csrc.nist.gov/Projects/cryptographic-module-validation-program/entropy-validations/search.

For access to the Python Client and ESVTS on Demo or Prod, see https://github.com/usnistgov/ESV-Server.

4.10 CMVP Webpages

This section provides information about the CMVP program that can be found on the web.

4.10.1 Official CMVP Website

The official CMVP website with all current publicly-available information on the CMVP is https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program. It can also be reached through https://nist.gov/cmvp.

4.10.2 Cryptographic Module Validation Lists

The official CMVP website can generate the following lists related to the validation of cryptographic modules:

- *Modules In Process* – A listing of the modules currently being reviewed by CMVP and the review state of each module. For more information about the MIP List, see section 4.2

  This list is updated as additional information is available. The validation process is a joint effort between the CMVP, the laboratory and the vendor and therefore, for any given module, the action to respond could reside with the CMVP, the lab or the vendor. This list does not provide granularity into which entity has the action.

- *Implementation Under Test* – A listing of the modules currently being tested at the CSTL. This list is provided by the CSTLs and includes module name, vendor, FIPS 140-2 or FIPS 140-3, and the date when added to the list.

  This list is updated as information is available. The IUT is under the control of the laboratory and the vendor. The CMVP is not aware of the submission schedule for these modules under testing.

- *Cryptographic Module Validation Search can be found at:* https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules/Search

  - A basic search supports a single overall list or a list resulting from a combination of vendor, module name, or certificate number. The basic search only addresses active modules.
  - An advanced search will generate a single list with the following options:
    - Certificate Number:
    - Vendor:

- Module Name:
- Standard: (FIPS 140-1, FIPS 140-2, or FIPS 140-3)
- Module Type:
- Validation Status: (Active, Historical, or Revoked)
  See the following web page for additional information
  https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules
- Embodiment:
- Year Validated:
- Overall Security Level:
- Algorithm:
- Allowed Algorithms:
- Tested Configuration:
- Caveat:
- Hardware Versions:
- Software Versions:
- Firmware Versions:
- Lab:

The search is updated when new validation certificates are posted to the website for a cryptographic module or group of cryptographic modules, when validations are extended to new versions of the cryptographic module through a revalidation, or when a change is requested in the Vendor information, such as the Point of Contact or the Vendor's Name. Only the current validation information is shown, however, changes are indicated in the validation history.

The lists are being improved as needs and time allows, so that more information than indicated here may be available from these sources before the next update of this document.

4.10.3 CMVP Certificate Page Links

Once the validation is identified, the information displayed typically includes vendor information, module information, and required caveats. For each certificate there are also several links from these pages that may be useful. These are described below.

4.10.3.1 Security Policy

This link is connected to the security policy that is the vendor provided summary of the capabilities and security information of the module in a PDF format. The file is created under the agreement from the vendor and is available from the CMVP website.

4.10.3.2 Consolidated Certificate

This link is connected to a list of certificates that were issued for the month of interest. It provides summary information that is accurate at the time of signing. For the latest module information, please refer to the certificate page. The file is created by CMVP and is from the

CMVP website. Recent validations may not have this link available until the consolidated certificate process can be completed.

4.10.3.3 Vendor Link

This link is provided by the vendor to CMVP. The vendor is responsible for the accuracy of the link and the content. The CMVP does not endorse the views expressed or the information presented in the directed link, nor does it endorse any commercial products that may be advertised or available at the directed link.

4.10.3.4 Vendor Product Link

The purpose of this web link is for vendors to provide a concise listing of known products which incorporate their validated cryptographic module or, if the cryptographic module is a standalone product, additional relevant information about the product. The CMVP hopes that this link will make it easier for potential customers and users to identify products that use validated cryptographic modules.

The link in the certificate details page is to a vendor provided URL that is vendor created and vendor maintained. The provision of this Vendor Product Link by the vendor is optional. The CMVP does not endorse the views expressed or the information presented in the directed link nor does it endorse any commercial products that may be advertised or available at the directed link. Press releases are not accepted.

4.10.3.5 Algorithm Certificates

Links to the CAVP validation certificate for the approved algorithms used in the module are provided for those wishing to know more details to the specific testing performed. The link is from the CAVP website. This currently is under development and may change. Algorithm validation certificates can also be found in the security policy.

4.10.3.6 Validation History

The initial validation and all updates are shown along with the CSTL responsible. The validation shown includes all updates and is considered the official validation. If information concerning a revalidation is needed, contact the CSTL indicated on the validation certificate.

4.10.3.7 Usage of FIPS 140-3 Logos

Once validation is achieved CMVP will forward through the CSTL to the Vendor instructions about the use of the NIST FIPS 140-3 logo. Vendors who use validated modules in their products may also request use of the NIST FIPS 140-3 Logo. The request instructions and use requirements is available from the CMVP web site: https://csrc.nist.gov/Projects/cryptographic-module-validation-program/use-of-fips-140-2-logo-and-phrases. Completed forms are sent to cmvp@nist.gov.

5 CMVP and CAVP Programmatic Metrics Collection

This section provides an overview of the CMVP and CAVP Programmatic Metrics Collection and a description of the collection and reporting processes of the CMVP metrics.

5.1 Overview

The CMVP Programmatic Metrics Collection process is intended to document the quality performance of the testing and validation processes of the CMVP and to allow the program to evaluate its relevance within the government. To achieve these objectives various metrics are collected through the testing and validation processes of the CSTLs and the CMVP. These metrics are intended to identify general programmatic trends and not to measure individual laboratory or vendor performances.

5.2 Confidentially of the Collected Metrics Data

The CMVP considers the data collected and reported by the individual CSTLs as proprietary. CMVP makes every effort to anonymize the information by sampling only larger data sets and combining them without tracking information. The statistical information derived from the collected data is considered to be non-proprietary.

5.3 Collected Metrics

With the migration to FIPS 140-3 and the changes in the collection tools, we are currently reevaluating the methods used to collect useful metrics. Though the program will likely follow much of the previous procedures, it is not possible at this time.

6 Test Tools

This section covers the testing tools CSTLs are expected to utilize in the testing and reporting of validation submissions. Where applicable, the title of the person responsible for the update and/or maintenance of the document is identified.

6.1 Web Cryptik

Web Cryptik is a required tool for the completion of module testing, and generation of documents that **shall** be included in a formal submission from the CST. The Web Cryptik tool is to be used to record details of the cryptographic module being tested, the specific testing performed, and the results of the validation testing. It is also to be used to create, among other documents, the FIPS 140 validation test report and draft certificate. Information about new features, enhancements, and bug fixes are provided with each release of the tool in the Web Cryptik User Guide.

Most submissions to CMVP are done through the use of Web Cryptik. The Web Cryptik User Guide provides a summary table of the submissions supported by Web Cryptik and files that must be included with the submission.

For some submissions that are not handled by Web Cryptik, such as RFGs, but do contain IP, PGP should be utilized.

Responsible Individual: NIST CMVP Program Manager.

6.2 Suggested Tools for Physical Testing

As indicated in HB 150-17 Section B.6.4.2, a CSTL **shall** meet the minimum hardware and software requirements for physical security testing. The CSTL can determine which tools to use to meet the requirements, however, below is a suggested tool list:

- X-Acto or Utility "Type" knives (including various blades)
- Strong artificial light source (Wavelength range of 400nm to 750nm)
- Magnifying glass
- Dremel "Type" Rotary Tool (including accessory bits: cutting, grinding, drilling, carving, etc.)
- Jeweler's screwdrivers (e.g., flat, phillips, robertson, torx, hex key)
- Dentist “Type” Instruments (e.g., picks and mirrors)
- Razor Saw
- Small pliers (e.g., needle nose, standard nose, long nose, curved nose, side cutters)
- Hammer
- Chisels
- Fine (small) files
- Heat Gun or Heat Source
- Spray Coolant
- Volt-Ohm-Milliammeter (VOM) or Digital Multimeter (DMM)
- Digital camera
- Digital scanner

Printer
ANSI C Compiler
Debugger or binary editor
Microsoft Office Professional
Adobe Acrobat Standard
Miscellaneous protection equipment for chemical testing (goggles, gloves)
Variable Power Supply
Digital Storage Oscilloscope and/or Logic Analyzer
Temperature Chamber
Variable power supply

7 CMVP General Testing and Reporting Guidance

In order for CMVP to manage the program more efficiently, additional testing requirements are addressed below. Several of the issues that were under section G of the FIPS 140-2 Implementation Guidance are presented in this section. This guidance does not change the cryptographic module requirements of ISO/IEC 19790:2012 but may impact ISO/IEC 24759:2017 documentation and testing requirements.

7.1 Submission Scenarios

An updated version of a previously validated cryptographic module can be considered for a *revalidation* rather than a *full validation* depending on the extent of the modifications from the previously validated version of the module. (Note: the updated version may be, for example, a new version of an existing cryptographic module or a new model based on an existing model.)

The Modules In Process (MIP) List will include only scenarios that result in issuing a new certificate (e.g., FS, UPDT, RBND, PTSC, TRNS) if the vendor requests the entry to be displayed on the MIP List. The Cryptographic and Security Testing Laboratories (CSTL) must check the appropriate box in Web Cryptik for MIP List inclusion.

The NIST Cost Recovery (CR) fees for all submission scenarios are posted at https://csrc.nist.gov/Projects/cryptographic-module-validation-program/nist-cost-recovery-fees.

Any submission that does not comply with the requirements of this section or requires significant additional review effort by the validators (e.g., due to issues with quality or complexity) will be subject to an ECR.

Upon a satisfactory review by the CMVP, either an updated certificate or a new certificate and an updated security policy, if there are any changes, will be posted on the Validated Modules website.

7.1.1 Requirements for all submissions

For any revalidation, the vendor is responsible for reviewing all FIPS 140-3 requirements and making sure any change has been addressed throughout the module requirements and that proper documentation has been completed. The CSTL is responsible for an independent evaluation of the impacts throughout the module requirements for any change and performs any testing needed prior to submission. The CSTL **shall** address all affected TEs and the CSTL's assessment. The details will be included in an updated Web Cryptik package with a summary of the changes and testing results **shall** be listed in the Change Document (template to fill in located under the "Help" tab in Web Cryptik).

For all revalidations, the Web Cryptik package **shall** include all files that are impacted by the change with their appropriate updates (e.g., Security Policy, Test Report, Draft Certificate, and/or Physical Test Report). The ZIP file and files within the ZIP file **shall** follow the requirements in the Web Cryptik User's Guide and submitted to the CMVP

using the specified encryption methods. Additional documentation may be required if CMVP guidance requiring the additional documentation has been published since the module's original validation.

All scenarios must be processed and submitted to the CMVP by a CSTL.

If a CSTL has been contracted to perform a revalidation for a validated module for which the CSTL did not perform the original testing on the base module:

a. The vendor **shall** provide the CSTL with the design documentation and implementation (including source code, HDL, etc.) of the base validated module and of the module that has been updated.
b. The vendor **shall** provide the CSTL with the latest Security Policy as shown on the base module's most recent certificate.
c. The CSTL **shall** determine that the provided base documentation and implementation is identical to the base validated module.
d. The CSTL **shall** examine each modification and confirm that the change is appropriate for the submission type (e.g., non-security relevant for Scenario NSRL).
e. The CSTL **shall** determine that no other modifications, including unintentional, have been made apart from what is permitted by the revalidation scenario.
f. The CSTL **shall** meet all requirements of the revalidation scenario(s) submitted.
g. The CSTL **shall** indicate which submission scenario is applicable and a summary of associated changes.
h. The CSTL **shall** use the format for listing the information for the certificate as required by each revalidation scenario.
i. The CSTL **shall** submit, at a minimum, what is required by the revalidation scenario.

Below are the twelve possible FIPS 140-3 submission Scenarios (FS, VUP, VAOE, NSRL, ALG, OEUP, RBND, PTSC, UPDT, CVE, TRNS, PHYS).

7.1.2 Full Submission (FS)

The first time a new software, firmware, hardware, or hybrid module is submitted for validation. The module **shall** meet all applicable requirements at the time of submission.

If modifications are made to hardware, software, or firmware components that do not meet any of the below revalidation criteria, then the cryptographic module **shall** be considered a new module and **shall** undergo a full validation testing by a CSTL and submitted as a FS.

7.1.3 Vendor Update (VUP)

Administrative updates (e.g., updating vendor contact information, grammatical Security Policy corrections).

7.1.4 Vendor Affirmed Operating Environment (VAOE)

Security policy change of vendor affirmed OEs (see Management Manual 7.9 *Vendor or User Affirmation of Modules*).

7.1.5 Non-Security Relevant (NSRL)

Modifications are made to hardware, software or firmware components **that do not affect any FIPS 140-3 security relevant items**. The CSTL is responsible for identifying the documentation that is needed to determine whether a revalidation is sufficient, and the vendor is responsible for submitting the requested documentation to the CSTL. Documentation may include a previous validation report, design documentation, source code, source code difference evidence, FSM, security policy differences, etc.

The CSTL **shall**:

- review and independently verify the accuracy of the vendor-supplied documentation and identify any additional documentation necessary to confirm the applicability of this revalidation scenario.
- determine additional testing as necessary to confirm that FIPS 140-3 security relevant items have not been affected by the modification.
- identify the assertions affected by the modification and **shall** perform the tests associated with those assertions. This will require the CSTL to:
    - Review the COMPLETE list of assertions applicable to the module,
    - Identify, from the previous validation report, the assertions that have been affected by the modification,
    - Identify additional assertions that were NOT previously tested but should now be tested due to the modification, and
    - Review assertions where specific Implementation Guidance (IG) was provided at the time of the original validation to confirm that the IG is still applicable.

The CSTL may send the CMVP a Request For Guidance to confirm their analysis on the non-security relevant prior to submission, which is expected to address at least the following questions:

1. What changes are being proposed?
2. What is the justification for being non-security relevant for each change?
3. Are changes made to: approved / allowed security functions/algorithms, SSPs, approved security services, security states within the FSM, lines of code within security files, or other areas that affects how the module meets the requirements of the FIPS 140-3?

7.1.6 Algorithm Update (ALG)

Post validation, approved security relevant functions or services for which CAVP testing was not available (or vendor affirming was still permitted per the CMVP/CAVP transition schedule) at

the time of submission to the CMVP for validation are now CAVP-tested and are being submitted for inclusion as an approved function or service. The CSTL is responsible for identifying the documentation that is needed to determine whether a revalidation is sufficient, and the vendor is responsible for submitting the requested documentation to the CSTL. Documentation may include a previous validation report and applicable CMVP rulings, design documentation, source code, security policy differences, etc. Code changes are not permitted under this revalidation scenario. For example, if self-tests are required for approved algorithms, the module must already support these self-tests.

The CSTL **shall**:

- review and independently verify the accuracy of the vendor-supplied documentation and identify any additional documentation necessary to confirm the applicability of this revalidation scenario.
- identify the assertions affected by the modification and **shall** perform the tests associated with those assertions. This will require the CSTL to:
    - Review the COMPLETE list of assertions applicable to the module,
    - Identify, from the previous validation report, the assertions that have been affected by the modification,
    - Identify additional assertions that were NOT previously tested but should now be tested due to the modification, and
    - Review assertions where specific Implementation Guidance (IG) was provided at the time of the original validation to confirm that the IG is still applicable.

7.1.7 Operating Environment Update (OEUP)

No changes to the module with an addition of tested operational environments (OEs). This requires CAVP-testing the algorithm validations on the new OEs. As applicable per IG 9.3.A, ESV(s) to cover all newly added OEs and/or platforms **shall** be submitted and validated separately prior to submission. The CSTL **shall** perform the full regression test suite shown on the CMVP website.

Upon re-testing and validation, the CMVP provides the same assurance as the original OE(s) as to the correct operation of the module on the newly listed OS(s) and/or OE(s). The new OS and/or OE will be added to the module's validation entry.

7.1.8 Rebrand (RBND)

This scenario applies if there are no modifications to a module and the new module is a re-branding of an already validated Original Equipment Manufacturer (OEM) module. The CSTL **shall** include the OEM's written approval for re-branding in the submission package and determine that the re-branded module is identical to the OEM module (n.b. this requirement applies equally to open source and non-open-source modules). Written approval **shall** note the terms of permission (e.g., subsequent addition of OEs, possible re-use of CAVP certificates, entropy, remediation of CVEs, non-security relevant changes, whether a rebrand of a rebrand is acceptable, etc.). If these terms do not explicitly allow a vendor to further rebrand the OEM

module, then a rebrand of that rebranded module is not permitted unless written permission is granted by the OEM. Additionally, for modules containing any open-source licensed code, the CSTL **shall** ensure the open-source licensing requirements are met (e.g., any required notices are contained in the Security Policy). The submission **shall** include a letter requesting the validation of the re-branded module and indicate the applicable documentation changes (e.g., vendor name, address, POC information, versioning information, etc.).

The CSTL **shall** provide an updated security policy which is technically identical to the originally validated security policy and describes the re-branded module.

7.1.9 Port Sub Chip (PTSC)

A sub-chip cryptographic subsystem that was previously validated in a single-chip (see IG 2.3.B) can be ported to other single-chip constructs as a PTSC submission to the CMVP. The following is applicable to validate this new single-chip module:

- The CSTL **shall** verify that there are no security relevant changes in the sub-chip cryptographic subsystem;
- If an entropy source is contained within the sub-chip cryptographic subsystem, ESV(s) to cover all new single-chip environments **shall** be submitted and validated separately prior to submission;

  Note 1: An ESV may not be required, if the entropy is collected outside the sub-chip cryptographic subsystem, depending on changes to the entropy source or the subsystem housing it. Please refer to IG 9.3.A and IG D.J for details on applicable caveats and entropy estimates.

  Note 2: Single chip embodiments may implement an ESV or a DRBG linked to a dedicated entropy source inside the physical boundary. Such cases may be implemented (a) inside the sub-chip cryptographic subsystem or (b) in two or more sub-chip cryptographic subsystems. The case (b) represents multiple disjoint sub-chip cryptographic subsystems (see 3 of IG 2.3.B).

- Approved security functions **shall** be retested and validated by the CAVP if implemented in a soft circuitry core recompiled in a different part configuration.

  Note 3: If the original algorithm testing was performed as stated in the Management Manual Section 7.3 – *Testing using Emulators and Simulators* in a module simulator, and there is no change to the soft-core, no additional algorithm testing is required.

- Full regression testing (see FIPS 140-3 Resources page) **shall** be performed on the new sub-chip cryptographic subsystem after fabrication (transformation of the HDL to a gate or physical circuitry representation);
- **ISO/IEC 19790:2012** Section 7.3 **shall** be addressed for the new single-chip module for all Security Levels within this Section.
- **ISO/IEC 19790:2012** Section 7.7 **shall** be addressed for the new single-chip module at Security Level 1.

- **ISO/IEC 19790:2012** Sections 7.11.2 and 7.11.9 **shall** be addressed for the new single-chip module for all Security Levels within this Section.
- A new Security Policy **shall** be provided for the new single-chip module.
- Versioning information on the new certificate **shall** be provided for:
    - the new physical single-chip,
    - non-security relevant single-chip functional subsystem firmware if applicable,
    - the sub-chip cryptographic subsystem soft and hard circuitry cores (which are unchanged from the original validation), and
    - the associated firmware.

7.1.10 Update (UPDT)

Modifications are made to hardware, software or firmware components **that affect some of the FIPS 140-3 security relevant items**. An updated cryptographic module can be considered in this scenario if less than a 30% of security changes were made to the module. Security changes include impacts to: lines of code in security files (files that include known security relevant data), approved / allowed security functions/algorithms, SSPs, approved services, self-tests, overall number of security files, TE's, and security states within the FSM. None of these, assessed individually, can exceed 30% of changes. The individual ratios for each of these **shall** be provided to the CMVP within the Change Document (e.g., 100 lines of code in security files out of 1000 total lines of code in security files results in 10% change).

The CSTL is responsible for identifying the documentation that is needed to determine whether a revalidation is sufficient, and the vendor is responsible for submitting the requested documentation to the CSTL. Documentation may include a previous validation report and applicable CMVP rulings, design documentation, source code, source code difference evidence, FSM etc.

The CSTL **shall**:

- provide a summary of the changes and rationale of why this meets the <30% guideline. The CMVP upon review, may determine that the changes are >30% and **shall** be submitted as an FS.
- review and independently verify the accuracy of the vendor-supplied documentation and identify any additional documentation necessary to confirm the applicability of this revalidation scenario.
- identify the assertions affected by the modification and **shall** perform the tests associated with those assertions. This will require the CSTL to:
    - Review the COMPLETE list of assertions applicable to the module,
    - Identify, from the previous validation report, the assertions that have been affected by the modification,
    - Identify additional assertions that were NOT previously tested but should now be tested due to the modification, and

- Review assertions where specific Implementation Guidance (IG) was provided to confirm that the IG is still applicable.

In addition to the tests performed against the affected assertions, the CSTL **shall** perform the regression test suite shown on the CMVP website.

The UPDT can also be used to for resetting the module's sunset date when a module has not changed, provided the above requirements are met.

7.1.11 Common Vulnerabilities and Exposures (CVE)

A CSTL has been contracted to perform a revalidation for a module on which the vendor has made FIPS 140 security-relevant changes in response to one or more CVEs (Common Vulnerability and Exposure). For more information about CVEs please see https://cve.mitre.org/.

The purpose of this revalidation scenario is to provide the vendor a means to quickly fix, test and revalidate a module that is subject to a *security-relevant CVE*[1], while at the same time providing assurance that the module still meets the FIPS 140-3 standard. If a CVE does not require security relevant changes to address it, then the vendor may pursue a Scenario NSRL revalidation.

To complete a Scenario CVE revalidation:

a. The CSTL **shall** determine that security relevant changes to the module are only to correct the vulnerability disclosed in the CVE.
b. The CSTL **shall** examine each modification and confirm that the change does not conflict with the requirements of FIPS 140-3.
c. The CSTL **shall** determine that no other modifications have been made.
d. The CSTL **shall** identify the assertions affected by the security-relevant modification and **shall** perform the tests associated with those assertions.
e. The vendor is not required to address IGs that have been published since submission of the original module, besides following the continual guidance of IG 11.A (CVE Management).
f. If the fix to address the CVE is in the scope of an algorithm implementation, then this algorithm **shall** be CAVP tested again to obtain a new CAVP certificate with the new module version.

In addition to the tests performed against the affected assertions, the CSTL **shall** also perform the predefined regression tests shown on the CMVP website, under CVE.

Because the change to the module is to address a security-relevant CVE, **the previous version of the module is no longer considered validated and shall be removed from the certificate**; exceptions may be made if the vendor shows how the CVE can be mitigated by policies included in the Security Policy, while still adhering to the FIPS 140-3 standard.

[1] A *security-relevant CVE* is one that affects how the module meets the requirements of the FIPS 140-3 standard.

7.1.12 Algorithm Transition (TRNS)

A CSTL has been contracted to perform a revalidation for a module on which the vendor has made FIPS 140-3 security relevant changes solely in response to a published CMVP algorithm transition that will cause some previously validated modules to be placed on the Historical list. If the algorithm transition will NOT cause the module to move to the historical list (i.e., "soft" transition), changes cannot be made as part of this submission. For example, the non-SP 800-56Brev2 RSA-based key encapsulation/un-encapsulation transition explained in FIPS 140-3 IG D.G.

Note: a single Scenario TRNS submission may combine multiple algorithm transitions. However, this may increase review time.

The purpose of the TRNS revalidation is to provide the vendor a means to quickly address algorithm transition requirements, test and revalidate a module in order to meet a CMVP transition, while at the same time providing assurance that the module still meets the FIPS 140-3 standard.

If the module code is *changed* to address an algorithm transition, the following requirements apply:

a. Submitted as a Scenario TRNS.
b. The CSTL **shall** determine that security relevant changes to the module are only to address a specific CMVP transition.
c. The CSTL **shall** examine each modification and confirm that the change does not conflict with the requirements of FIPS 140-3.
d. The CSTL **shall** determine that no other modifications have been made. The vendor is not required to address IGs or guidance that have been published since submission of the original module, unless directly applicable to the transitioning algorithm (e.g., CAVP testing or self-test requirements).
e. The CSTL **shall** identify the assertions affected by the security-relevant modification and **shall** perform the tests associated with those assertions.
f. If the means to meet the transition are in the scope of an algorithm implementation, and the path chosen to meet the requirements necessitates testing, then this algorithm **shall** be CAVP tested to obtain a new CAVP certificate with the new module version.
g. In addition to the tests performed against the affected assertions, the CSTL **shall** also perform the predefined regression tests shown on the CMVP website under TRNS on all versions listed on the module's certificate and on at least one of the listed OEs for hybrid or software/firmware modules (if the module binary image is identical across all OEs; if not, testing on at least every binary image is required).
h. The CSTL **shall** provide justification on why regression testing is not necessary for the untested OEs. With proper justification, these may remain on the module's certificate.

i. If regression testing is not performed on some versions, then those **shall** be removed from the module's certificate. OEs without proper justification or regression testing **shall** be removed from the module's certificate.

If the module code is *unchanged* to address an algorithm transition and the change is purely to documentation, one of the following four options apply. For each option, the CSTL **shall** state that the change to address the transition is purely documentational and which option applies.

Option 1: services or functionality were not moved to or from the approved mode to remain compliant (e.g., previously non-compliant services remain in the approved mode but are updated to demonstrate compliance rather than moved into non-approved mode), then the vendor may pursue a Scenario ALG revalidation.

Option 2: The vendor moves all non-compliant functionality into the non-approved mode of operation from the approved mode of operation.

a. Submitted as a Scenario TRNS.
b. The CSTL **shall** determine that security relevant changes to the module are only to address a specific CMVP transition.
c. The CSTL **shall** examine each modification and confirm that the change does not conflict with the requirements of FIPS 140-3.
d. The CSTL **shall** determine that no other modifications have been made. The vendor is not required to address IGs or guidance that have been published since submission of the original module, unless directly applicable to the transitioning algorithm (e.g., CAVP testing or self-test requirements).
e. The CSTL **shall** identify the assertions affected by the security-relevant documentation modification and **shall** perform the tests associated with those assertions.
f. The CSTL **shall** demonstrate how the module still meets IG 2.4.C after the reclassification of non-compliant functionality into the non-approved mode of operation.
g. In addition to the tests performed against the affected assertions, the CSTL **shall** also perform the predefined regression tests shown on the CMVP website under TRNS on all versions listed on the module's certificate and on at least one of the listed OEs for hybrid or software/firmware modules (if the module binary image is identical across all OEs; if not, testing on at least every binary image is required).

The only exception to this requirement (g.) is if the algorithm being transitioned is part of a standalone service and is not used by any other module service (e.g., cryptographic library where the module only provides the algorithm as an API service to a calling application as a stand-alone service). In this case, the CSTL **shall** provide justification on why regression testing is not necessary at all.

j. The CSTL **shall** provide justification on why regression testing is not necessary for the untested OEs. With proper justification, these may remain on the module's certificate.
k. If regression testing is not performed on some versions, then those **shall** be removed from the module's certificate. OEs without proper justification or regression testing **shall** be removed from the module's certificate.
h. The CSTL **shall** provide assurance that the non-compliant functionality is not used to meet any FIPS 140-3 requirements (key/CSP establishment, generation, storage, etc.).
i. The CSTL **shall** provide assurance, upon module examination, that no service, algorithm or CSP that relied on or used the non-compliant functionality, parameters, keys, etc. remain in the approved mode. The approved mode **shall** only contain approved services.
j. Documentation **shall** be updated to indicate the module does not utilize non-compliant functionality in the approved mode of operation.

Option 3: The vendor recategorizes the non-compliant functionality as claiming no security per IG 2.4.A, and this functionality remains in the approved mode of operation.

a. The same rules for Option 2 above **shall** be followed except for bullets 'i' and 'j'.
b. The CSTL **shall** provide justification on how the requirements of IG 2.4.A are met. This scenario is intended to be rarely used/accepted and depends on the purpose or use of the service that utilizes the non-approved algorithms. For example, a software library implementing three-key Triple-DES Encryption as one of its approved services cannot simply state this algorithm does not claim any security (per IG 2.4.A) and be used in the approved mode, as this does not meet 3) or 4) in IG 2.4.A Additional Comment #2.

Option 4: A combination of any of three options above (CAVP testing, moving non-compliant functionality into the non-approved mode, and/or recategorized per IG 2.4.A), in which case, requirements of each option apply.

a. Submitted as a Scenario TRNS.
b. Each option **shall** be listed/indicated in the Change Document under Option 4 (e.g. under Option 4, the following are claimed: Options 1 and 2) and note how each of the applicable 'shall' statements for each option are met).

In order to accommodate vendors who are updating their validation to prepare for an algorithm transition, fully compliant TRNS or ALG revalidations that have addressed the transition and are submitted to the CMVP before the date the transition is to take effect, will remain on the active list through the completion of the revalidation, even if it is not completed until after the transition date, unless the algorithm transition is to address a security concern that is deemed unacceptable by the CMVP. For newly submitted ALG submissions that address the transition, the CSTL **shall** include in the Special Instructions field the text "algorithm_transition" (with or without the

underscore) in order for the CMVP not to move this submission to the historical list come the algorithm transition date.

Changes made to a module, whether to the module code or purely to documentation, in order to meet a transition are security-relevant, due to their potential impacts on core and downstream services and the treatment of keys and SSPs. For example, moving *allowed* functionality from approved mode to non-approved mode - by either changing the software/firmware or a purely documentation change - is considered security relevant. Therefore, besides the case in **Option 1** above, all submissions that address a transition will require a Scenario UPDT, TRNS or FS submission regardless of module type or security level.

If a Scenario TRNS revalidation addresses an algorithm transition that moved the original certificate to the Historical list, and the sunset date of the certificate has yet to expire, then upon the revalidation of the module under Scenario TRNS, a new certificate will be issued on the Active list (inheriting the original sunset date) for the version of the module compliant with the transition requirements. Otherwise, if the original certificate was moved to the Historical list for reasons that are not addressed in the TRNS revalidation (e.g., a separate algorithm transition or the sunset date expired), the new certificate will be shown on the Historical list *immediately* after completion of the TRNS revalidation.

7.1.13 Physical Enclosure (PHYS)

Modifications are made only **to the physical enclosure of the cryptographic module that provides its protection and involves no operational changes to the module**. The CSTL is responsible for ensuring that the change only affects the physical enclosure (integrity) and has no operational impact on the module. The CSTL **shall** fully test the physical security features of the new enclosure to ensure its compliance to the applicable requirements of the standard.

The CSTL **shall**:

a. Describe the change (pictures may be required),
b. State that it is a security relevant change,
c. Provide sufficient information supporting that the physical only change has no operational impact,
d. Describe the tests performed by the CSTL that confirm that the modified enclosure still provides the same physical protection attributes as the previously validated module. For physical security levels 2, 3 and 4, the CSTL **shall** submit an updated Physical Security Test Report.

7.1.14 Submission Scenario Summary Table

Scenario	Long Name	Active or Historical [1]	New or Updated Cert[2]	New Sunset Date[3]	Meet All Latest Guidance[4]	Entropy Testing Applicable (ESV)[5]	ENT Remain on Cert[7]	Predefined Regression Testing[8]
VUP	Vendor Update	A or H	Updated	No	No	No	Possible	No (nor optional testing)
VAOE	Vendor Affirmed Operating Environment	A or H	Updated	No	No	No	Possible	No (nor optional testing)
NSRL	Non-Security Relevant	A only	Updated	No	No	No	Possible	No
ALG	Algorithm Update	A only	Updated	No	No (except for the algorithm updated)	No	Possible	No
OEUP	Operating Environment Update	A only	Updated	No	No	Yes[6]	Possible	Yes (full regression table)
RBND	Rebrand	A only	New	No	No	No	Possible	No (nor optional testing)
PTSC	Port Sub Chip	A only	New	No	No	Yes[6]	Possible	Yes (full regression table)
UPDT	Update	A or H	New	Yes	Yes	Yes	No	Yes (full regression table)
CVE	Common Vulnerabilities and Exposures	A or H	Updated	No	No	No	Possible	Yes (subset of regression table)
TRNS	Algorithm Transition	A or H	New	No	No (except for the algorithm transitioning)	No	Possible	Yes (subset of regression table)
PHYS	Physical Enclosure	A only	Updated	No	No	No	Possible	Yes (physical security)
FS	Full Submission	N/A	New	Yes	Yes	Yes	No	Full testing

[1] A or H means the revalidation can be on a completed validation that is either Active *or* Historical; A

only means it can only be on an Active validation.

[2] The result of this validation or revalidation will either be a new certificate (new number) or an updated certificate (same number).

[3] The result of this validation or revalidation will either be a new sunset date of 5 years, or the sunset date will remain the same. See Additional Comment #3 below for more details.

[4] If Yes, the validation or revalidation **shall** meet all the latest applicable guidance and requirements (e.g., standards, implementation guidance, management manual guidance, algorithm testing/self-tests, and other CMVP guidance) at the time of submission to the CMVP unless there is an implementation guidance transition that affects reports in the queue. If No, the revalidation **shall** meet all applicable requirements at the time of *original* validation (a module does not need to meet requirements that were added since the time of original validation, except those specified in the table).

[5] If applicable per IG 9.3.A.

[6] Only required on the new OEs for OEUP, or new single-chip environments for PTSC.

[7] Only for the original validation's ENT claim.

[8] Note: additional regression testing (on top of the predefined ones) may be applicable per requirements of the scenario.

7.1.15 Additional Comments

1. If the overall Security Level of the cryptographic module is lowered, the module may be submitted as a UPDT with full testing on the individual section(s) that is being lowered.
2. If the overall Security Level of the cryptographic module is raised or if the physical embodiment changes, e.g., from multi-chip standalone to multi-chip embedded, then the cryptographic module will be considered a new module and **shall** undergo full validation testing by a CSTL and submitted as an FS.
3. The sunset date for the module is determined based on the scenario:
    - Scenarios FS, UPDT – sunset date will be 5 years from the validation date
    - Scenarios VUP, VAOE, NSRL, ALG, OEUP, CVE, PHYS – sunset date unchanged
    - Scenarios RBND, PTSC, TRNS – sunset date is inherited from the original certificate
4. It is **not** possible to combine any revalidation scenarios. For example, if a vendor would like to submit a TRNS that has non-security relevant changes, the TRNS must be completed before or after a separate NSRL submission. Similarly, despite it being a simple change, a VU would need to be submitted separately to address any vendor admin change and cannot be combined with other scenarios.
5. A revalidation submission cannot be performed on a submission that is in the queue. It **shall** be on a completed validation (e.g., UPDT on a *validated* FS).

7.2 CMVP requirements pertaining to testing and approved algorithms

FIPS 140-3 describes approved security functions which can be used in the approved mode of operation, and non-approved security functions which cannot be used in the approved mode of operation. Approved security functions are expected to be CAVP tested, but CAVP testing has not always been available for these methods.

In such cases where CAVP testing is not available, guidance must be written to permit using these algorithms in the approved mode. These algorithms may be "vendor affirmed" to meet the applicable standard(s).

In addition, security methods that fall outside of the list of approved methods cannot be used in the approved mode, unless guidance is written to permit such special cases, where these methods are *allowed* to be used in the approved mode of operation.

This section explains when vendor affirmed or *allowed* methods are permitted, as well as the transitioning from vendor affirmed to CAVP Testing.

7.2.1 Vendor Affirmation of Security Functions and Methods

If CAVP testing is not available or the module is submitted during a transition period, then the following guidance is applicable.

If new approved methods (e.g., NIST FIPS, SP, etc.) are added to SP 800-140 documents, until such time that CAVP testing is available or the transition period has not yet expired for the new method, the CMVP will:

- if applicable, allow methods as provided by existing guidance (untested, and listed as non-approved but *allowed* in approved mode as shown in IGs D.F and D.G); and
- permit the vendor to implement the new approved method if an IG that supports vendor affirmation of this algorithm is published and met (untested, listed as approved for use in the approved mode with the caveat "vendor affirmed").

Note:

1. The Cryptographic Technology Group (CTG) at NIST may determine prior methods may be retroactively disallowed and moved to non-approved and not permitted in an approved mode of operation (e.g., DES). A transition notice would appear in NIST publications.
2. For all approved methods, all applicable FIPS 140-3 requirements **shall** be met. An IG may further clarify the requirements for a vendor affirmed algorithm.

Additional Comments

Vendor Affirmed: a security method reference that is listed with this caveat has not been tested by the CAVP, and the CMVP or CAVP provide no assurance regarding its correct implementation or operation. Only the vendor of the module affirms that the method or algorithm was implemented correctly.

The users of cryptographic modules implementing vendor affirmed security functions must consider the risks associated with the use of untested and unvalidated security functions.

7.2.2 Transitioning from vendor affirmed to CAVP Testing

When CAVP algorithm testing is released on the ACVTS production server in any of the following 3-month periods identified below, the transition occurs at the end of the following 3-month transition date. More specifically:

CAVP testing release	CMVP report submitted by
Jan 1 – March 31	June 30
April 1 – June 30	Sept 30
July 1 – Sept 30	Dec 31
Oct 1 – Dec 31	March 31

Table 1 - CAVP testing release dates and subsequent CMVP Transition dates

To illustrate, if the CAVP releases new testing for algorithm A, B and C, during the July 1 – September 30 period, then the transition date will be September 30 + three months, so after December 31 vendor affirming to algorithms A, B, or C will be prohibited in initial report submissions.

During the transition period, a new approved method would either be listed as approved with a reference to a CAVP validation certificate, or as vendor affirmed if testing was not performed and an IG that supports vendor affirmation of this algorithm was met.

When the transition period ends, for newly received test reports:

- only approved methods that have been tested, receives a CAVP validation certificate and is verified to meet the underlying algorithm standard is permitted. All other methods would be listed as non-approved and not allowed in an approved mode of operation.
- the vendor could optionally follow up with testing of untested vendor affirmed methods and if so, the reference to vendor affirmed would be removed and replaced by reference to the algorithm certificate. If there are no changes to the module, this change can be submitted under Scenario ALG (see Section 7.1 – *Submission Scenarios*). If the module is changed, this can be submitted under Scenarios UPDT or FS as applicable.

Note: To track the algorithms and their transition dates, the CMVP maintains a table available on (https://csrc.nist.gov/Projects/cryptographic-module-validation-program/programmatic-transitions).

Note: If a self-test requirement is associated with the algorithm, the algorithm will only be considered as an approved algorithm by CMVP if the self-test requirement is also met.

7.3 Testing using Emulators and Simulators

Under certain circumstances it may not be possible to test a module or algorithm directly. In these cases, CMVP has permitted the use of emulators and simulators to model the behavior of the item being tested. It is important to note the differences of these models and to apply them under the correct circumstances.

An emulator attempts to “model” or “mimic” the behavior of a cryptographic module. The correctness of the emulators' behavior is dependent on the inputs to the emulator and how the emulator was designed. It is not guaranteed that the actual behavior of the cryptographic module is identical, as other variables may not be modeled correctly or with certainty.

A simulator exercises the actual source code (e.g., Very High-Speed Integrated Circuit (VHSIC) Hardware Description Language (VHDL) code) prior to physical entry into the module (e.g., a Field-Programmable Gate Array (FPGA) or custom Application-Specific Integrated Circuit (ASIC)). From a behavioral perspective, the behavior of the source code within the simulator may be logically identical when placed into the module or instantiated into logic gates. However, many other variables exist that may alter the actual behavior (e.g., path delays, transformation errors, noise, environmental, etc.). It is not guaranteed that the actual behavior of the cryptographic module is identical, as many other variables may not be identified with certainty.

Labs may apply emulators or simulators depending on the type of testing results to be achieved. There are three broad areas of focus during the testing of a cryptographic module: operational testing of the module at the defined boundary of the module, algorithm testing and operational fault induction testing.

1. Operational Testing – Emulation or simulation is prohibited for the operational testing of a cryptographic module. Actual testing of the cryptographic module must be performed utilizing the defined ports and interfaces and services that a module provides. A test harness or a modified version to induce an error may be utilized; however, no changes to code or circuitry responsible for the tested response may be made.
2. Operational Fault Induction – An emulator or simulator may be utilized for fault induction to test a cryptographic module’s transition to error states as a complement to the source code review. Rationale must be provided for the applicable TE as to why a method does not exist to induce the actual module into the error state for testing.
3. Algorithm Testing – Algorithm testing utilizing the defined ports and interfaces and services that a module provides is the preferred method. This method most clearly meets the requirements of IG 2.3.A. If this preferred method is not possible where the module’s defined set of ports and interfaces and services do not allow access to internal algorithmic engines, two alternative methods may be utilized:
    a. A module may be modified under the supervision of the CSTL for testing purposes to allow access to the algorithmic engines (e.g., test jig, test API), or
    b. A module simulator may be utilized.

When submitting the algorithm test results to the CAVP, the actual OE on which the testing was performed must be specified (e.g., including modified module identification or simulation environment). When submitting the module test report to the CMVP, AS2.20 must include rationale explaining why the algorithm testing was not conducted on the actual cryptographic

module. An emulator may not be used for algorithm testing.

7.4 Remote Testing of Software and Hybrid Software Modules

The guidance below addresses the need for testing a module remotely while obtaining the equivalent assurance as if the test were performed at the vendor's facility.

While it may not be possible or advantageous to complete all testing remotely (e.g., tamper labels), aspects of a cryptographic module **shall** only be tested remotely if the following conditions are met:

1. The vendor remotely provides a cryptographic module to the test laboratory and its boundary and version is verified against the Security Policy. (TE04.13.01, 02, 03)
2. The network access to a remote test operating environment **shall** be authorized and controlled by the vendor. The cryptographic module under test **shall** be confirmed to be running on an OE that is well-defined and has a specific OS version, hardware platform and version, and processor (including microprocessor version), as shown on the module's certificate and security policy and where this can be confirmed during the test session. A 3rd party cloud system (e.g., Amazon Web Services, Microsoft Azure, and Google Cloud) may be used if these rules are met and the operating environment provides the same or additional level of security as the lab would provide for internal testing. The tester **shall** have control (oversight) of the testing environment. The tester's network **shall** be connected to the vendor's network via a secure connection (e.g., VPN or SSH) as permitted within a signed agreement by the lab and vendor. The tester's tools must satisfy the lab's network requirements before connecting to the vendor's network to test the module.
3. The required operating environment information (e.g., operating system name and version, processor family, hardware platform model) **shall** be obtained and verified against the operating environment information listed on the CAVP algorithm certificates for this module.
4. The tester **shall** understand, direct, and assume control of testing operations to initialize, install, and operate the module.
5. If a test harness is used, it **shall** be reviewed or written by the lab. It **shall** be verified to have been maintained properly with no vendor manipulation prior to its execution. The test results on the remote operating environment **shall** be captured and transmitted back to lab without the risk of being modified. The tester **shall** verify the test harness runs properly on its operating environment. The tester must verify the integrity of the testing session as well as the completeness and accuracy of the test results.
6. The vendor may provide assistance, under the direction of the tester, to obtain evidence of test results or restarting the operating environment as a means to recover from the induced error state of the cryptographic module.
7. The remote testing **shall** cover the same set of FIPS 140-3 requirements including but not limited to the following list, as if the operating environment were local to the tester:
    a. The services listed in the module Security Policy can be invoked and verified by the

tester.

b. For a module to be validated at Level 2 or 3 for ISO/IEC 19790:2012 Section 7.4.4, the role-based or identity-based authentication **shall** be performed and verified by the tester.

c. The failure of self-tests and the subsequent transition to an error state where module data output interfaces are inhibited can be observed and verified by the tester.

e. As applicable per IG 9.3.A, entropy has been effectively analyzed and received an ESV for all specific OEs and/or platforms prior to submission.

8. The test report **shall** document how the above conditions are met.

The vendor must provide a signed affirmation letter to the lab describing the remote testing process and access control mechanism that allows the lab to perform the test on the remote operating environment and protects the integrity of the test results. The lab **shall** provide a signed letter to the CMVP stating that the module had been tested remotely, affirming that the vendor provided their affirmation letter, stating what TEs were tested remotely, and explaining how the requirements were met during the remote testing.

Additional Comments

1. It is the responsibility of the tester to determine if a module is eligible to be tested remotely. If the tester cannot confirm a test requirement during remote testing, then the module **shall** not be fully tested remotely. If the tester wishes to test a subset of test requirements remotely, the remaining test requirements **shall** be tested onsite.

2. The tester **shall** confirm that the operating environment exactly matches the agreed upon test environment, including any virtual environments used. A Virtual Machine may not be used in lieu of an OS, unless the VM has been agreed to be part of the test environment and will be listed on the certificate.

7.5 Partial validations and non-applicable areas

CMVP will not issue a validation certificate unless the cryptographic module meets at least the Security Level 1 requirements for each area in Section 6 of ISO/IEC 24759:2017. Areas can be designated as Not Applicable (N/A) if they meet the following criteria:

- Section 6.5, Software/Firmware Security may be designated as N/A if the module is hardware-only without firmware or software;
- Section 6.6, Operational Environment may be designated as N/A if the operational environment for the cryptographic module is a limited or non-modifiable operational environment and Section 6.7, Physical Security is greater than Security Level 1 (AS06.04).
- Section 6.7, Physical Security may be designated as N/A if the cryptographic module is a software-only module and thus has no physical protection mechanisms;
- Section 6.8, Non-invasive security is N/A as there are currently no requirements in SP 800-140F. Any claims for non-invasive will be identified under Section 6.12.

- Section 6.12, Mitigation of Other Attacks is Applicable if the module has been purposely designed, built, and publicly documented to mitigate one or more specific attacks. Otherwise, this section may be designated as N/A.

7.6 CMVP requirements for PIV validations

PIV card applications can only be tested on a CMVP validated module, such as a smartcard. The CMVP validated module then obtains NPIVP validation, by adding the PIV card application to the module. The validated smartcard and the PIV card application is then re-validated as a CMVP module.

A PIV card application that is included as a component of a cryptographic module **shall** be referenced on the module validation. The cryptographic module validation entry **shall** provide reference to the PIV card application(s) validation certificate number. The cryptographic module's versioning information **shall** include the complete versioning information of the module including the PIV application(s). Each PIV application's name **shall** be clearly identified, and the PIV Certificate number is referenced on the CMVP module validation.

The PIV NPIVP validation entry include the following information:

1. the name of the PIV card application,
2. the name of the cryptographic module the PIV application was tested on, and
3. the complete versioning information of the module including the PIV application(s)

The NPIVP validation entries can be found at:

http://csrc.nist.gov/groups/SNS/piv/npivp/validation_lists/PIVCardApplicationValidationList.htm

7.7 Module count definition

The CMVP allows multiple modules to be validated on a single certificate. However, the identification of these modules in the report must be made clear throughout the report.

Determining the module count for a validation depends on the module type: Software, Hardware, Firmware, or a Hybrid as described below.

7.7.1 Software:

For a software module, its binary package(s) compiled from its source code is the IUT. The same source code may result in different sets of binaries when it's compiled for the different target platforms. The module count **shall** be the number of distinct sets of binaries (may map to software version, but not necessarily).

Examples:

- If a software module was validated on software version 1.0, and this source code package was compiled on three operating environments of the same family (e.g., iOS 8.0 running on iPhone5, iOS 9.0 running on iPhone5, and iOS 9.1 running on

iPhone5) resulting in a single binary set, the module count is "1".

- If a software module was validated on software version 1.0, and this source code package was compiled on two operating environments (e.g., iOS 9.0 running on iPhone5 and Android 4.0 running on a Galaxy Nexus) resulting in two separate sets of binaries (each set forming the logical boundary of the module), the module count is "2".
- If a software module was validated on software version 1.0 and software version 2.0, and these source code packages were compiled on four operating environments (e.g., iOS 9.0 running on iPhone5, iOS 9.1 running on iPhone5, Microsoft Windows Phone 8.1 running on Windows Phone 8.1, and Android 4.0 running on a Galaxy Nexus), where two of the environments are of the same family (iOS 9.0 and iOS 9.1) resulting in six separate sets of binaries (software versions 1.0 and 2.0 each map to three distinct sets of binaries), the module count is "6". In this case, a single iOS binary maps to both iOS 9.0 and 9.1, a single Microsoft Windows Phone binary maps to Microsoft Windows Phone 8.1, and a single Android binary maps to the Android 4.0, resulting in three distinct binaries for each software version (1.0 and 2.0), for a total of 6.

7.7.2 Hardware:

For a hardware module report, the module count can be determined by the physical boundary of the module and understanding the components that are either tested individually and have their own boundary, or the boundary encompasses multiple components which are tested collectively.

- If the boundary of the module consists of one hardware component with other hardware components within it, with each having its own hardware version number listed in the certificate (such as tamper seals, service processing cards, switch fabric, core switch blades, control processor blade, power supplies, fan kits, filler panels, management modules, network modules), then the module count **shall** be the number of 'base' modules which support the components within it.

  Examples:

  - If a hardware module report contains a switch (Series 1500, P/N 1010) which can optionally support four additional network modules for uplink ports without cryptographic capability (P/Ns 10, 20, 30, 40), then the module count is "1" (the switch being the 'base' component).
  - If a hardware module report contains a router with three separately tested part numbers (Series 2000, P/Ns 10, 20, 30), and each router can be configured to use service processing card A (P/N 100) or service processing card B (P/N 101), along with tamper seal TAMP1 (P/N 500), then the module count is "3" (the routers, each part number – 10, 20 and 30 - being a 'base' component).
  - If a hardware module report contains a series of four switches and two chassis-based switches (all running either the same firmware, or firmware with non-security relevant differences), and within the boundary of each of the chassis-based switches is a common control processor blade, four different core blades, fiber channel (FC)

port blades, an optional extender blade, a power-supply and a tamper seal, then the module count is “6” (the switches being the ‘base’ component: four switches and two chassis-based switches).

- If the report has several hardware modules that are individually tested and independent from one another, each having their own cryptographic boundary (flash drives, hard drives, single chips, multi-chips, etc.), but have slight hardware differences (shape, capacity storage, number, or type of ports, etc.), then each of the independent hardware pieces **shall** contribute to the module count.

Examples:

  - If a hardware module report contains two hard drive series with five separately tested configurations [Series SSD1 (P/Ns 128, 256, 500) and SSD2 (P/Ns 1000, 2000)], each with their own cryptographic boundary, the module count is “5”.
  - If a hardware module report contains three switch series with eight separately tested configurations [Series 6000 (P/Ns 100, 101, 102), 7000 (P/Ns 200, 201) and 8000 (P/Ns 300, 301, 302)], each with their own cryptographic boundary, the module count is “8”.

- If the hardware module report contains multiple firmware versions tested (with non-security relevant differences) on the same hardware platform, then the module count **shall** reflect the number of hardware modules only, not the number of firmware versions that are running on it.

  - For example, if a hardware module includes two hard drives (one being a 250GB drive and the other being a 500GB drive), and each of these drives map to four firmware versions, the module count is “2” to reflect the hardware platforms.

7.7.3 Firmware:

For a firmware module, its binary package(s) compiled from its source code imaged onto one or more hardware platforms is the IUT. The same source code may result in different sets of binaries when it's compiled for the different target platforms. The module count **shall** be the number of distinct sets of binaries (may map to firmware version, but not necessarily).

Examples:

- If a firmware package was validated as firmware version 1.0 with only a single binary, and this package was tested on two hardware platforms (e.g., hardware X version 1.0 and hardware Y version 2.0), the module count is “1”.
- If a report includes firmware version 1.0 and firmware version 2.0 each with their own binary, then the module count is “2”, regardless of the number of hardware platforms these packages were tested on.
- If a firmware package was validated as firmware version 1.0, and this package results in two different sets of binaries that map to two tested hardware platforms (e.g., hardware X version 1.0 and hardware Y version 2.0), the module count is “2” based on distinct firmware binaries.

7.7.4 Hybrid:

Since hybrid modules (hybrid firmware or hybrid software) are dependent on both the software/firmware and the hardware components, the module count **shall** be the total number of configurations that are possible that map to a single module boundary.

Examples:

- If a hybrid firmware includes hardware version 1.0 and firmware version 3.1, the module count is "1" since there is only a single combination of these two components.
- If a hybrid firmware includes hardware versions 1.0, 1.1, and 1.2, and firmware versions 1.1 and 1.2, and each of the hardware version can map to either of the firmware versions, then the total combination is equal to "6" (3 hardware versions times 2 firmware versions)

7.8 Module definitions for same certificates

The be on the same certificate, each module version **shall** have identical:

1. Section and overall levels.
2. Suite of approved security services.
3. Cryptography.
4. Suite of security functions and underlying algorithms, modes, and key sizes.
5. Suite of SSPs associated with the security services.
6. Suite of roles and authentication methods.
7. Finite State Model except related to the allowed differences.
8. SSP establishment methods.
9. Design assurance.
10. Mitigation of other attacks.
11. Module type (i.e., Software, Hardware, Firmware, or Hybrid).
12. Module embodiments (i.e., single-chip, multi-chip embedded/standalone). And similarly constructed including physical boundary.

7.9 Vendor or User Affirmation of Modules

The tested/validated module version, OE upon which it was tested, and the originating vendor are stated on the validation certificate entry. The certificate validation entry serves as the benchmark for the module-compliant configuration. This guidance addresses two separate scenarios: changes a vendor can affirm the module will perform as tested in the CSTL's validation submission and changes a user can affirm the module will perform as tested in the CSTL's validation submission.

This guidance is *not applicable* for validated modules when the requirements of **ISO/IEC 19790:2012** Section 7.7 Physical Security has been validated at Levels 2 or higher. This guidance is however, applicable at Level 1 for *firmware* or *hybrid* modules.

7.9.1 **Vendor**

1. A vendor may perform post-validation recompilations of a software or firmware module and affirm the modules continued validation compliance. By adding vendor support of non-tested configurations to the validated module security policy, the vendor bears all responsibility. These non-tested configurations versions may be considered by the user at their risk, provided the following is maintained:

   a) Software modules that do not require any source code modifications (e.g., changes, additions, or deletions of code) to be recompiled and ported to another OE must:

      i) For **Level 1 OE**, a software cryptographic module can be considered compliant with the FIPS 140-3 validation when operating on any general-purpose platform/processor that supports the specified operating system as listed on the validation entry or another compatible[3] operating system, or

      ii) For **Level 2 OE**, a software cryptographic module can be considered compliant with the FIPS 140-3 validation when operating on any general-purpose platform/processor that supports the same level 2 operating environment settings specified on the validation entry.

   b) Firmware modules that do not require any source code modifications (e.g., changes, additions, or deletions of code) to be recompiled, and its identified unchanged tested operating system (i.e., same version or revision number) may be ported together from one platform to another platform while maintaining the module's validation.

      Level 2 and above Firmware modules cannot be ported and maintain their validation, since Physical Security must be retested.

   c) Hybrid modules may be ported together from one OE to another OE while maintaining the module's validation provided that they do not require any of the following:

      i) software or firmware source code modifications (e.g., changes, additions, or deletions of code) to be recompiled and its identified unchanged tested operating system (i.e., same version or revision number) or another compatible operating system;

      ii) modified hardware components utilized by the software or firmware (e.g., changes, additions, or deletions).

      Level 2 and above hybrid modules cannot be ported and maintain their validation, since Physical Security must be retested.

   The CMVP allows vendor porting and re-compilation of a validated software, firmware or hybrid cryptographic module from the OE specified on the validation certificate to an OE which was not included as part of the validation testing as long as the porting rules are followed. Vendors may affirm that the module works correctly in the new OE. However, the CMVP makes no statement as to the correct operation of the module or the security strengths of the generated keys when so ported if the specific OE is not listed on the validation certificate.

[3] Compatibility may be based on how the module is compiled (e.g., for a specific processor, or general purpose). General purpose (universal) can be ported to other OEs.

The vendor **shall** work with a CSTL to update the security policy and submit it to the CMVP under one of the available revalidation scenarios (see Scenario VAOE in Section 7.1). The update would affirm and include references to the new vendor affirmed OE(s) (see devoted table in SP 800-140B). The module's Security Policy **shall** include a statement that no claim can be made as to the correct operation of the module or the security strengths of the generated keys when ported to an OE which is not listed on the validation certificate.

2. Software or firmware modules that require source code modifications (e.g., changes, additions, or deletions of code) to be recompiled and ported to another hardware or OE must be reviewed by a CSTL and revalidated per Section 7.1 (including regression testing) to ensure that the module does not contain any OE-specific or hardware environment-specific code dependencies. See Scenarios UPDT, NSRL, and OEUP (note, scenarios *cannot* be combined but can be validated in succession). This is not porting but rather incorporating the new versions and environment onto the certificate.

The vendor must meet all applicable requirements in ISO/IEC 19790:2012 Section 7.11, SP 800-140 Section 6.11, and CMVP IGs.

7.9.2 User

A user may not modify a validated module. Any user modifications invalidate a module validation. [4]

A user may perform post-validation porting of a module and affirm the module's continued validation compliance provided the following is maintained:

1. For **Level 1 OE**, a software, firmware, or hybrid cryptographic module will remain compliant with the FIPS 140-3 validation on any general-purpose platform/processor that supports the specified operating system listed on the validation entry, or another compatible operating system.

The user may affirm that the module works correctly in the new OE if the porting rules are followed. However, the CMVP makes no statement as to the correct operation of the module or the security strengths of the generated keys when ported and executed in an OE not listed on the validation certificate.

7.10 Operational Equivalency Testing for HW Modules

CMVP requires full testing of any module that the vendor wishes to list on the certificate. However, modules may be grouped together if they are the same except for devices listed under Equivalence Categories, which are currently considered for five classes of devices. Each Category and sample technologies for each Category are provided in Table 2.

[4] A user may post-validation recompile a module if the unmodified source code is available and the module's Security Policy provides specific guidance on acceptable recompilation methods to be followed as a specific exception to this guidance. The methods in the Security Policy must be followed without modification to comply with this guidance.

Category	Examples
Memory/Storage Devices	o HDD, SSD, DRAM, NAND, NOR, ROM, Solid State Memory Device, USB Flash Drive o Optical Disk Drive o Magnetic Tape Drive
Field Replaceable and Stationary Accessories	o Power Supplies o Fans
Interfaces (I/O Ports)	o Port Count o Line Card Count o Serial: RS232, RS422, RS485 o SAS, SATA, eSATA o Fiber Optic, FCoE, Fiber Channel o Ethernet, FireWire, DVI, SCSI, USB
Computational Devices	Refer to CAVP equivalency criteria and entropy constraints for guidance
Programmable Logic Devices	o CPLD, FPGA, PAL

Table 2 - Equivalence Categories

For details on the Equivalency Categories, please see the Equivalency Categories Tables under the FIPS 140-3 Resources Tab of the CMVP website. Also note, for modules that have differences within each of those categories, the level of testing required is dependent on the differences. Some differences require analysis only, while others require full or limited regression testing. The following are the general categories of the levels of testing. The actual testing required depends on the Equivalency Category (See Equivalency Regression Test Table and Equivalency Categories Tables found under the FIPS 140-3 Resources Tab of the CMVP website):

- Analysis Only (AO) for Equivalency Category X: Once the equivalency evidence/argument is provided and validated for the Equivalency Category X, there is no additional test other than the proof of its physical existence required on a module with the equivalent components in Category X to the module that has been fully tested under the same validation.
- Required Testing (RT) for Equivalency Category X:
  - If a module has some security relevant differences in the Equivalency Category X, the module **shall** be tested against all of the listed TEs for that category in Equivalency Regression Test Table found under the FIPS 140-3 Resources Tab of the CMVP website.
  - If a module claims equivalency in multiple categories in comparison to a fully tested module under the same validation, all of the required TEs for each claim equivalency category **shall** be satisfied.
- Focused Testing (FT) for Equivalency Category X:

- The use of some technologies may introduce Security Relevant differences that cannot be predicted by this Section 7.10. For example, Programmable Logic Devices may be used to support the Cryptographic Module in a number of different ways that are security relevant (e.g., authentication). It is up to the lab to determine what section of the standard is affected by this security relevant difference and apply the Revalidation Regression Test Table found under the FIPS 140-3 Resources Tab of the CMVP website. For other sections not affected by this difference, Regression Testing per Equivalency Regression Test Table found under the FIPS 140-3 Resources Tab of the CMVP website shall be performed.

- Complete Regression Testing (CRT): If an equivalency justification cannot be made, or the module differences can be mapped to a CRT entry within Equivalency Categories Tables under the FIPS 140-3 Resources Tab of the CMVP website, all modules, which lack an equivalency justification must, according to their security level, satisfy each TE listed in the Revalidation Regression Test Table under the FIPS 140-3 Resources Tab of the CMVP website.

In each report where the vendor wishes to claim equivalency, the lab **shall**:

- List the Equivalency Category, and specific component types being claimed in TE02.15.01. The lab must justify the component categorizations. The assumption is that the vendor initiated the Equivalency Category argument while the lab performed the analysis.
- List the additional testing performed (if any) between the modules. This list shall be provided as an addendum to the test report.
- Include in the Test Report how each module meets the TE's that are required for testing per this Section 7.10.

For example:

- Two devices to be on the same certificate have Hard Drives with different storage capacities, so testing requirement is Analysis Only, e.g., proof that both modules exist as claimed by the vendor.
- Two devices to be on the same certificate have different types of Solid State Memory: one has NOR Flash and the other has NAND. This will require a small selection of testing, per Equivalency Regression Test Table found under the FIPS 140-3 Resources Tab of the CMVP website.
- Two devices to be on the same certificate have different types of storage: one has a Hard Disk and the other has a Solid-State Drive. This will require complete regression testing per Revalidation Regression Test Table.

Additional Comments

- The lab shall perform full testing on at least one module.
- This only applies to Operational testing of Hardware modules
- Physical security testing (ISO/IEC 19790:2012, section 7.7) is not addressed for Security Level 2 and above. In other words, this does not exempt the lab from performing physical security testing for modules at Level 2 or above. This is because the lab needs to examine

each module for, e.g., opacity and tamper evidence, if there are physical differences between the modules.

- Components considered equivalent may still affect the entropy generated within the modules in different ways. This must be accounted for in the entropy report, if entropy is applicable.
- Equivalency considerations of the main processors/CPUs are out of scope of this Section 7.10. If the CPU is different between modules on the same certificate, then the full Revalidation Regression Test Table must be run (found under the FIPS 140-3 Resources Tab of the CMVP website). If the entropy is OE based, the entropy must address the new OE.
- ISO/IEC 24759:2017 Section 6.7 Physical Security, Section 6.8 Non-Invasive Security and Section 6.12 Mitigation of Other Attacks are not applicable.

Annex A CMVP Post Validation Issue Assessment Process

Annex A.1 Addressing Security Relevant Issues

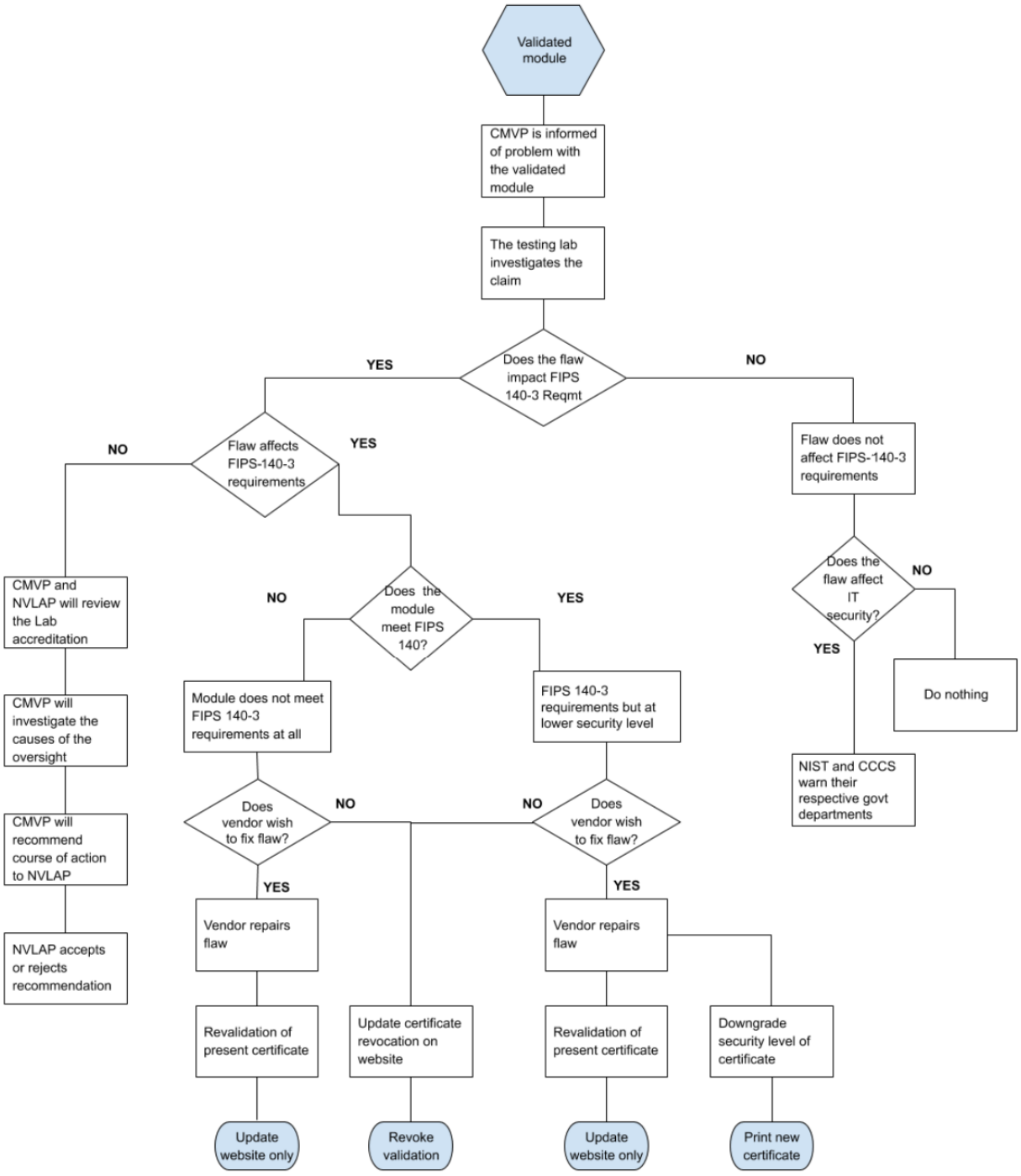

Figure 5- Annex A. Validation Issue Assessment Process

Annex A.2 Addressing CVE Relevant Vulnerabilities

The list of CVEs is maintained by NIST in the NVD at https://nvd.nist.gov/. The purpose of the Scenario CVE revalidation (described in Section 7.1) is to provide the vendor a means to quickly fix, test and revalidate a module that is subject to a security-relevant CVE, while at the same time providing assurance that the module still meets the current FIPS 140 standards.

Vendors **shall** reference this database and address the security relevant CVE's that are within the boundary of the module, not only during the validation process, but also after the module has been validated. Without published security relevant CVEs being addressed by the vendor and verified by the testing laboratory, the CMVP has no assurance that the module meets the requirements to obtain or maintain validation.

At the discretion of the CMVP, certificates will be revoked that do not comply. It is the goal of the CMVP to maintain the security of validated modules.

For more information about CVEs please also refer to https://cve.mitre.org/. See also IG 11.A *CVE Management* for more guidance on this topic.

ACRONYMS

AES	Advanced Encryption Standard
ANSI	American National Standards Institute
APLAC	Asia Pacific Laboratory Accreditation Cooperation
AS	Assertion
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CCCS	Canadian Centre for Cyber Security
CMVP	Cryptographic Module Validation Program
CSTL	Cryptographic and Security Testing Laboratory
CVC	Consolidated Validation Certificate
CVP	Cryptographic Validation Program
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
EA	European co-operation of Accreditation
ECR	Extended Cost Recovery
ESV	Entropy Source Validation
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FSM	Finite State Model
GC	Government of Canada
HB	Handbook
IAAC	InterAmerican Accreditation Cooperation
ID	Identification
IG	Implementation Guidance
ILAC	International Laboratory Accreditation Cooperation
ISO	International Organization for Standardization
ITAR	International Traffic in Arms Regulation
IUT	Implementation Under Test
LC	Laboratory Code

MLA	Multilateral Recognition Arrangement
MOU	Memorandum of Understanding
MRA	Mutual Recognition Arrangement
N/A	Not Applicable
NACLA	National Cooperation for Laboratory Accreditation
NCR	NIST Cost Recovery
NECR	NIST Extended Cost Recovery
NIST	National Institute of Standards and Technology
NVLAP	National Voluntary Laboratory Accreditation Program
OE	Operational Environment
OS	Operating System
PDF	Portable Document Format
RFG	Request for Guidance
SP	Special Publication
TE	Tester Evidence
TID	Tracking Identification Number
TM	Trademark
TR	Test Requirements
URL	Uniform Resource Locator
VE	Vendor Evidence