DRAFT

FIPS 140-3

Cryptographic Module Validation Program Management Manual

(Date 9/21/2020)

Version 1.0

**National Institute of Standards and Technology and
Canadian Centre for CyberSecurity**

Revision History

Version	Date	Comment
1.0	9/21/2020	First release for FIPS 140-3 program

Table of Contents

List of Figures

List of Tables

1 Introduction

1.1 Background

The Canadian Centre for CyberSecurity (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. Products or modules validated as conforming to FIPS 140 are used by Federal agencies for the protection of Sensitive but Unclassified (SBU) information (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 CST laboratories may perform all of the tests covered by the CMVP. NIST and CCCS, as the joint CMVP Validation Authorities, review laboratory reports, issue validation certificates, and participate 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, and the conduct of activities necessary to ensure that the standards are fully met.

1.3 Applicability and Scope

The *CMVP Management Manual* is applicable to the CMVP Validation Authority, the CST laboratories, 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 Cryptographic Module Validation Program

The purpose of the Cryptographic Module Validation Program is to increase assurance of secure cryptographic modules through an established process. Validation is performed through conformance testing to requirements for cryptographic modules as specified in FIPS 140. Independent accredited third-party CST laboratories perform assurance testing and the results are reviewed and approved by the CMVP. 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 and SP 800-140D. More 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

Note: Issues relating to Web Cryptik, submission communications, and revalidation submissions are currently in draft.

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 – CST Laboratory Processes describes the CST laboratory processes including accreditation, maintenance and management of a laboratory.

Section 4 – Cryptographic Module Validation Program Processes describes the various aspects of the cryptographic module validation process.

Section 5 – CMVP and CAVP Programmatic Metrics Collection provides an overview of the CMVP and CAVP Programmatic Metrics Collection and a description of the collection and reporting processes of the CMVP metrics.

Section 6 – Documentation Maintenance Processes describes the processes and timing for updates and maintenance of documents pertinent to the CMVP.

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 Information Formatting provides guidance in the use of Web Cryptik.

Annex B – CMVP Conventions for Email Correspondence provides guidance in communicating effectively between CMVP and CST laboratories.

Annex C – 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, including voice 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 CST accreditation requirements. A flow diagram of the documents referenced below is available on the CMVP webpage under *CMVP FIPS 140-3 Related References*.

1.8.1 FIPS 140-3

Federal Information Processing Standards FIPS 140-3 identifies the Cryptographic Module Validation Program (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 Publications: 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 sensitive but 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.

1.8.2 Security Requirements for Cryptographic Modules

ISO/IEC 19790:2012 specifies the security requirements for a cryptographic module utilized within a security system protecting sensitive information in computer and telecommunication systems. This International Standard defines four security 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). This International Standard specifies four security levels with 11 requirement areas, each security level increasing security requirements over the preceding level. Copies can be obtained from ISO.org. NIST is making 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 the CMVP webpage under *CMVP FIPS 140-3 Related References*.

1.8.3 Test requirements for cryptographic modules

ISO/IEC 24759:2017 specifies the methods to be used by accredited CST laboratories to test whether the cryptographic module conforms to the requirements specified in ISO/IEC 19790:2012. The methods are developed to provide a high degree of objectivity during the testing process and to ensure consistency across the testing laboratories. It is often referred to as the Derived Test Requirements (DTR) as it is derived from ISO/IEC 19790:2012. The DTR includes detailed procedures, inspections, and tests that a CST laboratory tester must follow, and the expected results that must be achieved, for the cryptographic module to satisfy the requirements. The detailed methods are intended to ensure a high degree of objectivity, accuracy, and consistency during the testing process. This document also specifies the requirements for information that vendors provide to testing laboratories as supporting evidence to demonstrate their cryptographic modules' conformity to the requirements specified in ISO/IEC 19790:2012. ISO/IEC 24759:2017 can be modified by the SP 800-140 set of documents and the FIPS 140-3 Implementation Guidance.

The DTR contains the security requirements from ISO/IEC 19790:2012, divided into 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.

Copies can be obtained from ISO.org. NIST is making available a limited number of copies of ISO/IEC19790 and ISO/IEC 24759:2017. To request a copy of each document, see the CMVP webpage under *CMVP FIPS 140-3 Related References*..

1.8.4 Special Publication 800-140*x*

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

NIST Special Publication (SP) 800-140A modifies the vendor documentation requirements of ISO/IEC 19790:2012 Annex A. As a validation authority, the Cryptographic Module Validation Program (CMVP) may modify, add or delete Vendor Evidence (VE) and/or Test Evidence (TE) as specified under paragraph 5.2 of the 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 Special Publication (SP) 800-140B is to be used in conjunction with ISO/IEC

19790:2012 Annex B and ISO/IEC 24759:2017 6.14. The special publication 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 Cryptographic Module Validation Program (CMVP) may modify, add or delete Vendor Evidence (VE) and/or Test Evidence (TE) specified under paragraph 6.14 of the ISO/IEC 24759:2017 and as specified in ISO/IEC 19790:2012 paragraph B.1.

NIST Special Publication (SP) 800-140C replaces the approved security functions of ISO/IEC 19790:2012 Annex C. As a validation authority, the Cryptographic Module Validation Program (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 Special Publication (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 Cryptographic Module Validation Program (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 Special Publication (SP) 800-140E replaces the approved authentication mechanism requirements of ISO/IEC 19790:2012 Annex E. As a validation authority, the Cryptographic Module Validation Program (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 Special Publication (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 Cryptographic Module Validation Program (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.

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 CST laboratories and vendors to apply the requirements of FIPS 140 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 CST laboratories, vendors, and other interested parties. The document is available on-line on the official Cryptographic Module Validation Program website at https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/announcements.

1.8.6 CST Laboratory Accreditation Standards

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

NIST laboratory accreditation standards relevant to the NVLAP accreditation of CST laboratories 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.

1.8.7 Other Documents on the CMVP Website

The CMVP website contain several pages pertinent to the 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. FAQ on CMVP (https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/CMVP-Management-Manual-and-FAQs) contains questions and answers to several issues pertaining to the CMVP.

4. Validation Lists (https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules) contains the most current information about active, historical, and withdrawn cryptographic modules.

5. Modules in Process (MIP) List (https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Modules-In-Process/Modules-In-Process-List) contains information provided by the CST laboratories about cryptographic modules undergoing testing where the test report has been submitted to the CMVP for validation. (The listing is voluntary in that vendors may choose to have their module listed on this list). For more information regarding a specific module, please contact the vendor.

6. Implementation Under Test (IUT) List (https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Modules-In-Process/IUT-List) contains information provided by the CST laboratories about cryptographic modules undergoing testing, but have not yet been submitted to the CMVP. Inclusion of a module on this list by a vendor is voluntary. The CMVP does not have information regarding the status of these modules or know whether a test report will be submitted to the CMVP for them. For more information regarding a specific module, please contact the vendor.

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

8. Resources (https://csrc.nist.gov/Projects/cryptographic-module-validation-program/resources) provides guidance that is easily bookmarked, specifically for dealing with detailed validation and re-validation information.

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 Authorities

The validation authorities for the CMVP are 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.

2.3 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 CST laboratory for cryptographic module or algorithm testing, the vendor must contact the contracted laboratory for all questions concerning the test requirements.

The name, telephone number and email address for the NIST and CCCS Program Managers are provided in Table 1 below.

NIST	CCCS
Beverly Trapnell	Carolyn French
NIST CMV Program Manager	CCCS CMV Program Manager
Security Testing, Validation, and Measurement Group	Risk Mitigation Program
301-975-6745	613-949-7703
beverly.trapnell@nist.gov	carolyn.french@cyber.gc.ca

Table 1- CMVP Program Manager Contact Information

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

2.4 Request for Guidance from CMVP

The CMVP suggests reviewing the CMVP Management Manual, CMVP Frequently Asked Questions (FAQ), the CMVP Announcements and CMVP Notices posted on the CMVP web sites first as the answer 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 above 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 with existing modules.

Vendors who are under contract with a CST laboratory for cryptographic module or algorithm testing of a particular implementation(s) must contact the contracted CST laboratory 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 CST laboratory 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).

CST Laboratories must submit all test-specific questions in the RFG format described below. These questions must be submitted to all points of contact.

2.4.1 Informal Request

Informal requests are considered as ad hoc questions aimed at clarifying issues about cryptographic module testing and other aspects of the CMVP. Replies to informal requests by the CMVP are non-binding and subject to change. It is recommended that informal requests be submitted to all points of contact.

Every attempt is made to reply to informal request with accurate, consistent, clear replies on a very timely basis.

2.4.2 Official Requests

If an official response is requested, then an official request must be submitted to the CMVP written in the Request for Guidance (RFG) format described below. An official response requires 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.

A Request for Guidance will result in an official response from the CMVP that will state current policy or interpretations. This format provides the CMVP a clear understanding of the question. An RFG **shall** have the following items:

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

2. A descriptive title,

3. Applicable statement(s) from relevant FIPS 140-3 documents,

4. Applicable assertion(s) from the ISO/IEC 24759:2017 and SP 800-140x,

5. Applicable required test procedure(s) from the ISO/IEC 24759:2017 and SP 800-140x,

6. Applicable statements from FIPS 140-3 Implementation Guidance,

7. Applicable statements from algorithmic standards,

8. Background information if applicable, including any previous CMVP or CAVP official rulings or guidance,

9. A concise statement of the problem, followed by a clear and unambiguous question regarding the problem, and

10. A suggested statement of the resolution that is being sought. All questions should be presented in writing. The provided information should include a brief non-proprietary description of the implementation and the target security level. All of this will enable a more efficient and timely resolution by the CMVP. The statement of resolution **shall** be stated in a manner which the CMVP can either answer "YES" or "NO". The CMVP may optionally provide rationale if the answer is not in line with the suggested statement of resolution.

When appropriate, the CMVP will derive general guidance from the problem and response and add that guidance to this document. Note that general questions may still be submitted, but these questions should be identified as not being associated with a particular validation effort.

Preferably, questions should be non-proprietary, as their response will be distributed to ALL CST laboratories. Distribution may be restricted on a case-by-case basis.

2.4.3 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 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 nonproprietary and not prevent further distribution by the CMVP.

The CMVP will distribute the unmodified official request to the CST laboratory that performed the conformance testing of the identified module. The CST laboratory may choose to include participation of the vendor of the identified module during its determination of the merits of the inquiry. Once the CST laboratory 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 CST laboratory 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 CST laboratory will further state its recommendations regarding the impact to the validation.

The CMVP will review the CST laboratory'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 Validated Module Issue Assessment Process for the flow diagram to the assessment process.

2.5 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	CST Laboratory	CMVP	User
Function	Designs & Produces	Tests for Conformance	Reviews & Approves	Specifies & Purchases
Output	Cryptographic Modules	Assessment Report	Validation List	Security with Assurance

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

2.5.1 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 Special Publications. Among other functions, the vendor defines the boundary of the cryptographic module, determines its modes of operation and its associated services, and develops 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 CST laboratories of its choice.

After the cryptographic module has been validated, the vendor cannot change the validated version of the module. Any change to the validated version will result in a new validation test effort on the new or revised module.

2.5.2 CST Laboratory

The role of the CST laboratory is to independently test the cryptographic module to the appropriate FIPS 140 security level and embodiment, and to produce a written test report for the CMVP Validation Authorities based on its findings. The CST laboratory conducts algorithmic testing, reviews the cryptographic module's documentation and source code, and performs operational and physical testing of the module in accordance with the DTR, SP 800-140*x* and IG. If a cryptographic module conforms to all the requirements of the standards, the CST laboratory submits a written report to the Validation Authorities. If a cryptographic module does not meet one (or more) requirements, the CST laboratory works with the vendor to resolve all discrepancies prior to submitting the validation package to the Validation Authorities.

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. CMVP policy in this area is as follows:

1. A CST Laboratory may not perform validation testing on a module for which the laboratory has:
    a. designed any part of the module,
    b. developed original documentation 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 CST Laboratory 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 CST Laboratory and the company is performed under contractual agreements, as done with other clients.
3. A CST Laboratory 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 CST laboratory may also create the Finite State Model (FSM), Security Policy, Non-administrator guidance and Administrator guidance which are specified as vendor documentation in FIPS 140. 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 CST laboratory must be able to show a mapping from the consolidated or reformatted FSM and/or Security Policy back the original vendor source documentation. The mapping(s) must be maintained by the CST laboratory as part of the validation records. Source code information is considered vendor-provided documentation and may be used in the FSM and/or Security Policy.

2.5.3 CMVP Validation Authorities

The CMVP Validation Authorities are 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 validate the test results for every cryptographic module. The test results are documented in the submission package prepared by a CST laboratory 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 CST laboratory. 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 CST laboratory 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 CST laboratory 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.

2.5.4 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 in the latest Security Policy and is available on the CMVP web site.

Users can also develop product or system specifications that include the requirements for FIPS 140 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.

2.6 Management of the CMVP

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.

2.6.1 CMVP Meetings

CCCS and NIST senior management meet annually to discuss programmatic issues related to the CMVP, CAVP, and CST laboratories. These meetings are an opportunity for senior managers to establish program goals and management approaches.

2.6.2 CST Laboratory Manager Meetings

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

Usual discussion topics for CST laboratory 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

2.6.3 Language of Correspondence

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

2.7 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 CST laboratories 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 CST laboratory's accreditation, or the program.

As required by the CST laboratory accreditation standards listed in Section 3.1 of this manual, CST laboratories 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. CST laboratories 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 CST laboratories 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.

2.8 Agreements between Validation Authority Organizations

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.

2.9 Programmatic Directives and Policies, and Internal Guidance and Documentation

The CMVP issues programmatic directives and policies, and internal guidance and documentation to all CST laboratories. These communications are normally distributed by email. These communications are very important and can seriously impact on-going validation efforts.

The CMVP will strive not to make those directives and guidance retroactive to previous validations; however, the status of previous validations may be affected.

CST laboratories are encouraged to provide timely comments to the CMVP about those communications.

3 CST Laboratory Processes

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

3.1 Accreditation of CST Laboratories

This section describes in general terms the process for a laboratory to become an accredited CST laboratory under the National Voluntary Laboratory Accreditation Program (NVLAP).

Note: This section describes the process used by NVLAP.

3.1.1 Recognized Standards and Standard Accreditation Body

The accreditation process is governed by the policies of the applicable accreditation bodies, and readers are encouraged to review the official documentation prepared by these bodies. The content of this section is provided for informational purposes only.

The CMVP and CAVP only recognize the following standards from the associated standards bodies for the accreditation of CST laboratories:

> NIST Handbook 150 (2020) and Handbook 150-17 (2020) under the NVLAP of the Government of the United States of America

3.1.2 Accreditation Process

Applicant laboratories must complete the accreditation process within one year of 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 2. All steps in the accreditation process must be completed in the order shown.

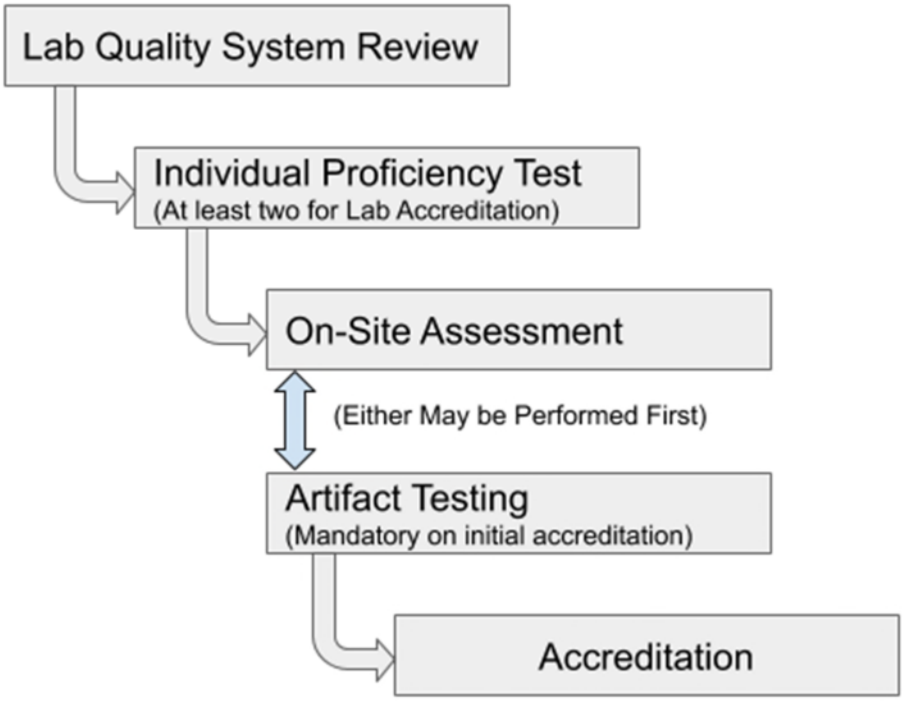
Lab Quality System Review
Individual Proficiency Test
(At least two for Lab Accreditation)
On-Site Assessment
(Either May be Performed First)
Artifact Testing
(Mandatory on initial accreditation)
Accreditation

Figure 2- CST Laboratory Accreditation Process

3.1.2.1 Application for Accreditation and Selection of Assessment Team

The prospective CST laboratory 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 assessor from CMVP and one lead assessor from NVLAP. NVLAP technical assessors for CST laboratories 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 CST laboratory they will be assessing.

3.1.2.2 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.

3.1.2.3 CST Proficiency Examination

Every independent tester, technical reviewer and submission signatory **shall** maintain certification by passing the current Proficiency Exam. Each lab must have at least two testers who have passed the current exam. The current written examination consists of approximately one hundred questions relating to various aspects of CST laboratory activities, FIPS 140-2, 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

  - Switches on doors/removable covers
  - Enclosure removal/penetration test/Thermal coating/potting removal
  - Test on locks
  - Perform tamper label testing using thermal and chemical methods
  - Describe Environmental Failure Testing (EFT)/Environmental Failure Protection (EFP)
  - Determine opacity requirements are met
  - Understand tamper detection/response mechanisms
  - Document tamper label use procedures in the security policy
  - Understand Sub-chip implementation
  - Provide programmatic guidance and, specifically, what it says about submitting the Physical Testing documentation
- Authentication, Roles, Services and Operational Environment
  - Bypass service
  - Revalidation issues related to the operational environment
  - Operator authentication vs message authentication
  - Role & Identity based authentication
  - Authentication strength
  - List and explain the roles
  - Authorized roles
  - A strong integrity test
  - Porting
- Algorithms and Self-Test
  - Listing the data encryption and decryption algorithms
  - Understanding the modes of AES and the Triple-DES
  - Issues specific to the AES GCM mode
  - Prime generation for use in the RSA and DSA algorithms
  - Understanding the elliptic curve technology
  - Use of NIST-recommended and non-NIST-recommended curves
  - Hash functions
  - Message authentication
  - Key derivation functions and the relevant protocols
  - PBKDF and KBKDF

    - Algorithm transitions
    - Known answer tests
    - Understanding cryptographic self-test techniques
    - Integrity testing
    - Documentation
- Key Establishment
    - Key agreement
    - Key transport
    - Documenting the strengths of the key establishment methods
    - Entropy generation
    - DRBGs
    - Identify known weaknesses and attacks against the key establishment methods
- Key Management
    - Zeroization in response to tampering and to the environmental factors
    - Procedural or operator-controlled zeroization
    - Security Level 3 and 4 rules and examples of the methods of plaintext key entry
- Security Assurances
    - Multiple approved modes
    - Module specification
    - Approved and non-approved modes
    - Approved and non-approved security functions
    - Historical List
    - The documentation requirements for the Security Policy and, specifically, for the inclusion of the diagrams
    - Examples and documentation requirements for mitigation of other attacks
    - Revalidation issues related to sub-chip
    - PAA and PAI functions
    - Hybrid modules
    - FSM
    - Ports and Interfaces
    - Design Assurance - Levels 1-3

The exam is graded by the third-party testing organization, and the results are provided to the

CMVP. Testers are required to pass the Cryptographic Validation Program (CVP) Certification Examwith a score of 75% or greater. The reexamination period for maintaining the certification for CVP certified testers is four years. In the event of major program updates, such as the adoption of a new FIPS 140 standard, the reexamination frequency may be temporarily increased to account for new technical requirements. For more information on the CVP Certification exam, refer to the CMVP website: https://csrc.nist.gov/projects/cryptographic-module-validation-program

3.1.2.4 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** CST laboratory, the laboratory must submit a satisfactory plan to NVLAP concerning resolution of deficiencies within thirty days of notification.

If deficiencies are found during the assessment of an **applicant** CST laboratory, 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.

3.1.2.5 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. The completion of the testing should be within one (1) year. 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.

3.1.2.6 Accreditation Decision

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

3.1.2.7 Granting Accreditation

Once the approval has been granted to accredit the CST laboratory for Cryptographic Security testing, the CST laboratory is assigned to one of four renewal dates:

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

After the initial audit the renewal period is one year but after that it is every two years. The CST laboratory will receive an NVLAP certificate that identifies the CST laboratory, the scope of the accreditation, the CST laboratory's authorized representative, the expiration date of the accreditation, and the laboratory code for the CST laboratory.

3.1.2.8 CMVP and CAVP Test Tools

Once accreditation has been granted and the CMVP and CAVP are advised by NVLAP that the applicant laboratory has been accredited, the CMVP and will issue to the newly accredited CST laboratory the latest version of the CRYPTIK tools. The CMVP and CAVP will also issue the latest programmatic directives and policies, and internal guidance and documentation, including use of CAVP Automated Cryptographic Validation Testing System (ACVTS).

3.1.2.9 Cooperative Research and Development Agreement

All accredited CST laboratories must have an executed 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 for the US government fiscal year which runs from October 1 to September 30. The agreement is reviewed and revised on an annual basis. New laboratories are required to execute the agreement initially once they become accredited through NVLAP. Existing laboratories must re-execute the agreement every fiscal year. The NIST CMVP Program Manager is the point of contact for obtaining a copy of the current CRADA.

3.2 Maintenance of CST Laboratory Accreditation

3.2.1 Proficiency of CST Laboratory

CST laboratories must submit at least three validation test reports during their accreditation cycle with a minimum of one per year for renewing laboratories. Newly accredited labs will not be subject to the one test report per year minimum during the first three years of accreditation, but must submit a minimum of three reports within that time-frame in order for 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. Laboratories are also required to have a minimum of two Cryptographic Validation Program (CVP) FIPS 140 Certified Testers throughout the accreditation period.

3.2.2 Renewal of Accreditation

Each accredited CST laboratory will receive a renewal application package before the expiration date of its accreditation to allow sufficient time to complete the renewal process. Fees for renewal are charged to the laboratory in accordance with the fee schedule published by NIST 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 2- CST Laboratory Accreditation Process and described in Section 3.1.2 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. The accreditation is valid for two (2) years.

3.2.3 Ownership of a CST Laboratory

In the event a CST laboratory 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 CST Laboratory

In the event a CST laboratory 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 CST laboratory’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 pass the CVP exam.

3.2.6 Change of Key Laboratory Testing Staff

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 CST laboratory equipment, or persistent process or technical shortfalls. An accredited laboratory **shall** maintain an Extended Cost Recovery (ECR) point total of less than 12 points during the 2-year period of accreditation. If a laboratory accumulates 12 or more points during the 2-year period, the accreditation for the cryptographic module testing will be suspended.

ECR points are levied as follows:

0 points - Excessive number of modules in one report

1 point - No cost based Scenarios ECRs

3 points - Technicalities such as missing documentation or incomplete report

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 CST laboratory's accreditation while an investigation is conducted and necessary corrective actions are taken.

3.2.9 Voluntary Termination of the CST Laboratory

A CST laboratory 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** terminate the laboratory's accreditation, notify the laboratory that its accreditation has been terminated, and instruct the laboratory 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 that will be taken regarding any outstanding work that has not been completed. This will be handled on a case by case basis.

3.3 Confidentiality of Proprietary Information

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 CST Laboratory

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

3.3.2 Non-Disclosure Agreement for Current and Former Employees

The CST laboratory must develop and maintain non-disclosure agreements for staff that participate in the testing of modules.

3.4 Code of Ethics for CST Laboratories

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 honesty;
4) Act Ethically.

3.5 Management of CMVP and CAVP Test Tools

Testers, or any other member of the laboratory, **shall** not distribute any of the test tools provided by NIST and CCCS to any entity outside the CST laboratory, including firms contracted by the CST laboratory. Personnel temporarily employed by and working under the supervision of a CST laboratory (i.e., a contractor) can use the provided test tools, when they are used within the CST laboratory facilities. Test tools include all versions of CRYPTIK, the Automated Cryptographic Validation Testing System (ACVTS), the METRIX tools 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 CST laboratory’s accreditation.

4 Cryptographic Module Validation Program 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 CST laboratory and CMVP interaction, followed by the vendor and laboratory interaction. The remaining subparagraphs cover the tracking of submissions through the process, the laboratory's submittal package, and an overview of the scenarios for submission including full submissions and resubmissions.

4.1.1 General Submission Overview

Figure 3 shows the general flow of testing and validation of a cryptographic module.

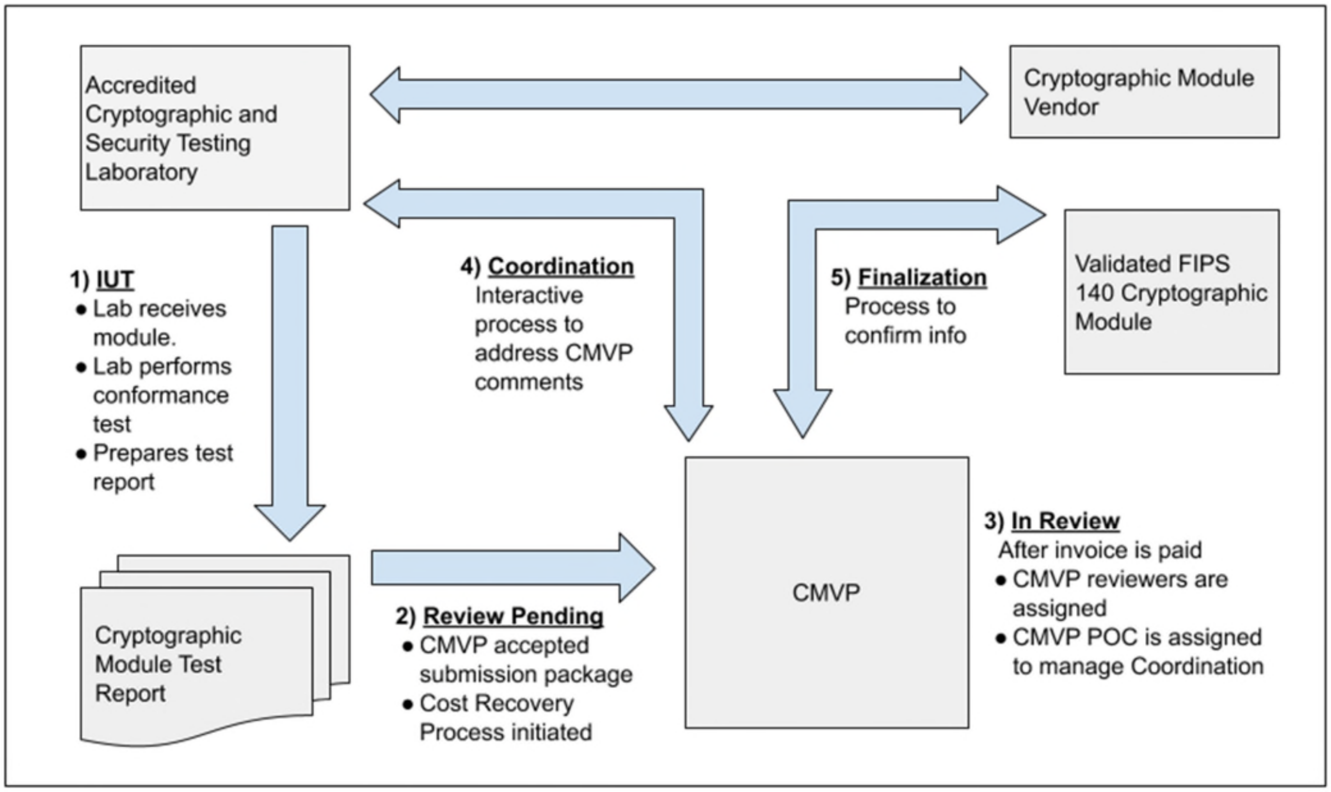
Accredited Cryptographic and Security Testing Laboratory
Cryptographic Module Vendor
1) IUT
• Lab receives module.
• Lab performs conformance test
• Prepares test report
4) Coordination
Interactive process to address CMVP comments
5) Finalization
Process to confirm info
Validated FIPS 140 Cryptographic Module
CMVP
3) In Review
After invoice is paid
• CMVP reviewers are assigned
• CMVP POC is assigned to manage Coordination
Cryptographic Module Test Report
2) Review Pending
• CMVP accepted submission package
• Cost Recovery Process initiated

Figure 3 - Cryptographic Module Testing and Validation Process

The steps for the cryptographic module validation life cycle include:

Step 1. The vendor submits the cryptographic module for testing to an accredited CST laboratory under a contractual agreement. Cryptographic module validation testing is performed using the Derived Test Requirements (DTR. If the CST laboratory has any questions or requires clarification of any requirement in regards to the particular cryptographic module, the laboratory can submit Requests for Guidance (RFG) to NIST and CCCS as described in Section Request for Guidance from CMVP.

Step 2. Once all the testing requirements have been completed, a validation submission is prepared. The Cost Recovery fees are addressed prior to or with the submission.

Step 3. The validation submission is sent to CMVP. After the payment has been processed, two reviewers are assigned to perform the initial review of the documents. One of the reviewers is identified as the point of contact (POC) for CMVP to interact with the CST laboratory to address comments.

Step 4. The coordination process will continue until all comments and/or questions have been satisfactorily addressed.

Step 5. Once the cryptographic module has been validated, and the associated vendor information has been confirmed by the laboratory, the validation information is posted to the *CMVP Validation List* at the CMVP website: https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules/Search.

4.1.2 Vendor and Laboratory Procedures for Testing of the Cryptographic Module

A vendor contracts with an accredited CST laboratory 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.

When the documentation is delivered to the laboratory and the cryptographic module is available for testing, and with the vendor's agreement, the laboratory notifies the primary contacts at NIST and CCCS that the cryptographic module is an Implementation Under Test (IUT). 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 CST laboratory assigns a Tracking Identification Number (TID) using the convention described in the *CMVP E-mail Correspondence document*. The first two digits of the TID are assigned by the CMVP upon laboratory accreditation, the second set of four digits is assigned by the laboratory, and the last four digits are assigned by CCCS when the validation submission is accepted. In all, a ten-digit TID number is created and used to track the submission.

The CST laboratory performs the cryptographic module testing as prescribed by the Derived Test Requirements (DTR) for FIPS 140, *Security Requirements for Cryptographic Modules* and enters all assessments for the testing in the CRYPTIK tool. Although testing requirements are in the DTR, ISO/IEC 19790:2012, *Security Requirements for Cryptographic Modules* remain the definitive reference for whether or not the cryptographic module meets the requirements of the standard. The Special Publications (SP) 800-140*x* and Implementation Guidance (IG) provides clarifications of the CMVP, and in particular, clarifications and guidance pertaining to the DTR. Cryptographic algorithm and/or random number generator validation testing may also need to be done as part of the FIPS 140 validation testing. Please refer to Section 4.1: Cryptographic Module Validation Process Overview for more information.

At any point in the testing the CST laboratory may wish to request guidance from CCCS and NIST in determining how to apply the FIPS 140 standard to the particular cryptographic module.

The cryptographic module validation process is an iterative process. If the CST laboratory 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 the document or the cryptographic module for validation testing.

When the CST laboratory has completed all required validation testing and has determined that the cryptographic module is conformant to FIPS 140, the laboratory prepares the validation test report and the rest of the validation test submission and sends it to NIST and CCCS for validation, see Section 4.1.1: Preparation and Submission of the Validation Submission describes what must be submitted by the laboratory for validation. The CST laboratory is to refer to the tracking identification (TID) number provided to NIST for the validation when submitting the validation test report.

4.1.2.1 Validation Report Review

All FIPS 140 validation submissions are examined by the CMVP. When the submission is accepted by the CMVP, the module is moved to the PENDING REVIEW stage of the Modules in Process list. The module will remain in the PENDING REVIEW stage until the NIST Cost Recovery fee is paid and the first reviewer begins the review. When the reviewer begins the review, the cryptographic module is moved to the IN REVIEW stage of the Modules In Process. When the CMVP reviewers have completed their review of the validation submission and provided comments, the comment file is encrypted and sent to the CST laboratory. The cryptographic module is then moved to the COORDINATION stage.

The CST laboratory addresses the comments and resubmits a complete submission containing any modified documents as per Section 4.3. The CCCS and NIST reviewers examine the responses, and respond with any additional comments if necessary. If found acceptable, the cryptographic module is moved to the FINALIZATION stage. The *CMVP FIPS 140 Modules In Process* is updated daily.

4.1.2.2 Validation Certificate

At the end of the validation process NIST and CCCS, as 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.

For instructions to describe how the validation information is to be formatted to appear on the NIST CMVP web page (via entry into CRYPTIK), please consult the CMVP Resources page at: https://csrc.nist.gov/Projects/cryptographic-module-validation-program/resources.

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 CST laboratory. The CST laboratory must review and confirm or correct the information on the certificate. Once the information is confirmed, CCCS will issue a certificate number to the laboratory and the certificate is posted to the NIST web site. At the end of each month, the Validation Authorities sign a consolidated validation certificate which lists all modules that were validated during the month. A pdf of the consolidated certificate is linked to each of the associated individual certificates.

The information on the certificate pertains to the module from the time of its validation. During its life cycle, the module information for that validation may change. For revalidations that do not include a new validation number, the module's validation will be updated on the website. Therefore, users should refer to the NIST website for information concerning a validation.

4.2 Modules in Process

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 CST laboratory. Modules are listed alphabetically by name. If a vendor and CST laboratory chose not to list the module on either list, the module will be reflected at the end of the list in the "Not Displayed" row. Posting on the list does not imply or guarantee FIPS 140 validation. The IUT and MIP lists are available on the NIST web site https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Modules-In-Process/IUT-List.

Effective July 1, 2017, modules listed on the IUT List for 18 months or longer are automatically dropped.

The following paragraphs describe the requirements or activities that take place during each stage of the Modules In Process. The status of each cryptographic Module In Process is identified.

1. Implementation Under Test (IUT)
    - There exists a viable contract between the vendor and the CST laboratory for the testing of the cryptographic module.
    - The cryptographic module is resident at the CST laboratory.
    - All of the required documentation is resident at the CST laboratory. NOTE: if the vendor requires the CST laboratory personnel to test the cryptographic module on-site, all documents must also be on-site with the module.
2. Review Pending
    - Complete set of testing documents submitted to NIST and CCCS for review. The set includes draft certificate, detailed test report, non-proprietary security policy, and website information. In addition, some modules may require a separate physical security testing report and entropy assessment report.
    - Signed letter from laboratory stating recommendation for validation by NIST and CCCS.
3. In Review
    - NIST and CCCS reviewers assigned.
    - NIST and CCCS perform a review of the test documents.
    - Comments coordinated by NIST and CCCS reviewers and a consolidated

set of comments sent to the CST laboratory.

4. Coordination – This phase of the process may be iterative.
    - Comments received by the CST laboratory from NIST and CCCS for resolution.
    - Additional testing (if required).
    - Additional documentation (if required).
    - Comments resolution developed for resubmission to NIST and CCCS.
    - Testing documents updated for resubmission to NIST and CCCS.
    - Responses to comments and revised test documents submitted to NIST and CCCS.
    - Several iterations may be required to address all comments.
5. Finalization
    - Final resolution of validation review comments submitted to NIST and CCCS are accepted by CMVP.
    - After the NIST and CCCS final review of the draft certificate, a copy is sent to the CST laboratory for a final review.
    - Once the CST laboratory approves the final draft certificate, CCCS assigns a certificate number and NIST posts the certificate to the Validated Cryptographic Modules list.
6. Consolidated Certificate
    - At the end of each month, a consolidated certificate is generated which includes all of the certificates that were published during the month.
    - CCCS and NIST sign the consolidated certificate with each validation entry that appears on that published list and it is posted on the web site as a link on each of the individual module validation entries: https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules.

4.3 Preparation and Submission of the Validation Submission

NIST and CCCS as the Validation Authorities may request any or all information used by the CST laboratory to prepare the validation test report, whether it has been provided by the vendor to the CST laboratory, or was developed by the laboratory.

The following information and documentation **shall** be provided to both NIST and CCCS by the CST laboratory upon report submission. The ZIP file and files within the ZIP file **shall** follow all programmatic naming conventions and be submitted to the CMVP using the specified encryption methods. The naming format indicated in **Annex B**: *CMVP Convention for Correspondence* **shall** be used.

1. **Non-proprietary Security Policy in PDF.** The security policy **shall** not be

marked as proprietary or copyright. It must also include a statement allowing copying and distribution.

2. **Web CRYPTIK v1.0** The validation report submission must be output from the NIST-provided CRYPTIK tool:
    a. **Signature page –** insert PDF of signed signature page;
    b. **General Vendor / Module Information** page – PDF;
    c. **Full Report with Assessments** – PDF; and
    d. **Certificate –** MS Word
    e. **Vendor Text File** - TXT
3. **Physical Security Test Report** (mandatory at Security Levels 2, 3 and 4 for modules that have physical attributes) – PDF. The physical testing report must include photos, drawings, etc. as applicable.
4. **Re-validation Change Summary** – PDF, for re-validation.
5. **Entropy Report –** PDF, if applicable

The CST laboratory has the option to additionally provide *Notes and Proprietary Information* output with the Detailed Report with Assessments, but this is not required by NIST and CCCS. The PDF files **shall** not be protected or locked.

The submission documents **shall** be compressed into a single Zip file, encrypted for all NIST and CCCS reviewers, and sent to the following NIST and CCCS points of contact:

- **NIST**: CMVP@nist.gov
- **CCCS**: CMVP@cyber.gc.ca

Once the electronic report submission document is received by the CMVP it will be placed in the report queue in order received. Those reports marked to be listed, will appear in the weekly published Modules-In-Process listing posted on the CMVP web site. The listing and the definition of the five stages of the Modules-In-Process listing is found at: http://csrc.nist.gov/groups/STM/cmvp/inprocess.html

During the COORDINATION phase the CST laboratory will address each CMVP comment and update any applicable files as necessary in addition to providing a response and additional clarification as necessary in the CMVP comments document. The laboratory will re-submit the report in its entirety as above (i.e. full report submission) including the updated CMVP comments file.

6. **CMVP Comments** <DOC> or <DOCX>

4.4 Submission Scenarios

A full submission is currently the only type of submission that can be currently submitted. The full submission is currently defined as:

- Full Submission (5FS): A new module is submitted for validation as is modifications made to hardware, software, or firmware components that do not meet revalidation criteria, then the cryptographic module **shall** be considered a new module and **shall** undergo a full validation testing by a CST laboratory.

Other scenarios are needed to aid CMVP in the management of changes to existing validations that are significantly less effort for vendor, lab, or CMVP than a full submission. While the scenario is defined for new submissions, details are yet to be defined for revalidation categories. Combining submission scenarios is not yet determined. To date the remaining categories are:

- Vendor Info (1VI): Change of vendor or contact information that does not affect any security relevant items; post validation, approved security relevant functions or services for which testing was not available at the time of validation or not tested during the original validation which are now being included as approved security services.
- OE Addition (1OEA): Add an additional tested OE to the Module that does not affect any security relevant items; post validation, approved security relevant functions or services for which testing was not available at the time of validation or not tested during the original validation which are now being included as approved security services.
- Vendor Affirm (1VA): Change to SP to add vendor affirmed OEs that does not affect any security relevant items; post validation, approved security relevant functions or services for which testing was not available at the time of validation or not tested during the original validation which are now being included as approved security services.
- Update SP (1UP): Update SP beyond above scenarios, especially to update procedures or references, that does not affect any security relevant items; post validation, approved security relevant functions or services for which testing was not available at the time of validation or not tested during the original validation which are now being included as approved security services.
- New Algorithm Update (1AU): Replace vendor affirmed algorithm with Validated Certificates without affecting any security relevant items; post validation, approved security relevant functions or services for which 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 tested and are being submitted for inclusion as approved functions or security services.
- OEM (1OEM): Modifications are made to hardware, software or firmware components that do not affect any security relevant items. If there are no modifications to a module and the new module is a re-branding of an already validated OEM module.
- Sunset change (2SC): Used to extend the module's sunset date when a module has not changed. The module meets all of the latest standards, implementation guidance and algorithm testing in effect at the time the module revalidation package is submitted unless there is an implementation guidance transition that affects reports that have been submitted.
- Maintenance Update (1MU): Modifications are made to hardware, software or firmware components that affect some security relevant items. An updated cryptographic module can be considered in this scenario if it is similar to the original module with only minor changes in the security policy and FSM, and less than 30% of the modules security relevant features. Can be submitted for up to 1 year post validation.

- Minor Changes (3MC): Modifications are made to hardware, software or firmware components that affect some security relevant items. An updated cryptographic module can be considered in this scenario if it is similar to the original module with only minor changes in the security policy and FSM, and less than 30% of the modules security relevant features. Submitted after 1 year of being validated.
- Security Issue (3CVE): Expedited assessment of changes to address CVE related modifications.
- Physical Change (4PSC): Modifications are made only to the physical enclosure of the cryptographic module that provides its protection and involves no operational changes to the module.

Fees charged by NIST as part of the cost recovery program are shown below in Table 2. The current chart shows fees for FY 2020.

Scenario	**Base fee:**	**Extended fee:**
FIPS 140-3 Scenarios 1VI, 1OEA, 1VA, 1UP, 1AU, 2SC, 1MU, 3CVE and 4PSC	N/A	$1,000
FIPS140-3 Scenario 1OEM	$2,000	$1,000
FIPS 140-3 Scenario 3MC	$4,000	$1,500
FIPS 140-3 Scenario 5FS		
Security Level 1:	$8,000	$3,000
Security Level 2:	$10,000	$4,000
Security Level 3:	$10,000	$4,000
Security Level 4:	$10,000	$4,000

Table 2- Scenario Cost Recovery Fees

4.5 Validation Submission Queue Processing

4.5.1 Initial Validation

Modules submitted for initial validation will be queued and addressed on a first-come, first-serve basis. The internal review disposition of a module report is left to the sole discretion of the NIST and CCCS CMVP program managers. Reports will not be marked as FULL or RE-VALIDATION on the MIP list, or ordered differently as currently posted.

4.5.2 Re-validations not requiring a new certificate

Change letters will be required along with the requisite documentation. As these are typically quickly handled and are considered maintenance of the validations, they are have a separate queue. See section 4.4 above for a listing of these scenarios.

4.5.3 HOLD Status for Cryptographic Modules on the Modules In Process

A CST laboratory can request that a module that is in the CMVP queue be officially moved to HOLD status.

1. A reason for the HOLD does not need to be conveyed or provided to the CMVP.
2. The request can be made at any time. However, once a final draft certificate has been approved by the CST laboratory, a module can no longer be placed on HOLD. The module will proceed to validation and posting on the CMVP web site.
3. A module officially requested to be placed in HOLD status will move to the IUT stage while it has this status.
4. Modules that were in the REVIEW PENDING stage when placed on HOLD will move to the back of the CMVP queue. When they are removed from HOLD, they will not return to the position they held prior to being placed on HOLD.
5. Modules that were in the IN REVIEW stage or a later stage when placed on HOLD will return to their former position in the CMVP queue (when they are removed from HOLD).

If a module test report is sent incomplete or is determined to be incomplete once the module has moved to the IN REVIEW stage, the module will be placed on HOLD and the NIST Extended Cost Recovery Fee will apply.

When the incomplete items are received by the CMVP, the module will return to its former position in the CMVP queue in the REVIEW PENDING stage.

If a non-compliance issue is discovered during module IN REVIEW or COORDINATION, the module will be placed on HOLD and NIST Extended Fee will apply. When or if the updated test report with the revised module is received, the module will return to the CMVP queue in the same Modules In Process state it was placed on HOLD and to its former position in the CMVP queue.

If CMVP comments are sent to the lab and the lab has not responded within 90 days, the module will be placed on HOLD and removed from the MIP list until the CST laboratory provides a response.

4.5.4 Validation Deadline

Effective January 1, 2018, CMVP will drop modules that have not completed the validation process within 2 years of report submission or request for an invoice. 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.

4.5.5 Resubmission while in Review Pending

An updated submission may be provided to CMVP while in review pending. The updated submission will replace the previous submission and will keep its place in queue. This is not to be used as a placeholder until testing is completed, and penalties may be applied if misused.

4.6 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. 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).

4.6.1 International Traffic in Arms Regulations Policy

If a CMVP test report is received from a CST laboratory 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.

4.6.1.1 CMVP ITAR Guidance

1. Report submission as specified in **Section 4.3: Preparation and Submission of the Validation Submission** applies with the following changes:
    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 Section 7.5), the test report must include PDF images (front and back) of each of the cryptographic algorithm validation certificates. The algorithm web site will not have any detailed information, and this must be provided for the NIST CMVP reviewers.
    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 is allocated for the CCCS TID. A CCCS TID will not be provided.
    e. Actual module names, version numbers, and vendor information will be provided. This information will not be masked by dummy information.

[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.

2. Report review
   a. Each ITAR report will be reviewed by two 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, Module Type, Embodiment, Validation Date, Sunset Date and Overall Level.
   d. The official certificate will be scanned and emailed to the CST laboratory for presentation to the vendor.
4. Re-validation
   a. All re-validation changes will result in a new certificate sent to the CST laboratory 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 found in 7.8Annex B.

4.7 NIST Cost Recovery[2]

4.7.1 NIST Payment Policy

NIST CMVP maintains the billing information for each CST laboratory. If the CST laboratory's information needs to be updated, contact NIST CMVP. Upon receipt of the CST laboratory's submission or a request for an invoice, NIST billing prepares an invoice and submits it to the identified payee. Only CST laboratories with an active CRADA agreement will be invoiced by NIST billing. Review of submissions will not begin until NIST CMVP receives confirmation from NIST Receivables that the invoice has been paid. If the module is dropped prior to the IN REVIEW stage, then any payment can be refunded.

The NIST CMVP fee schedule is published under **CMVP Notices** at https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Notices. For questions about methods of payments and associated handling fees contact NIST Billing Information: 301-975-3880.

Cost recovery (CR) is a fee charged to the CST laboratory by NIST CMVP to offset the cost of the validation authority activities performed by NIST CMVP. The fee is designed to directly support the resources necessary to perform test report reviews and validations. The fee is applied to new module submissions, modified module submissions, and for report reviews that require additional time due to complexity or quality.

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

4.7.2 Invoice for a Report Submission

NIST Cost Recovery (CR) is currently levied on all 1OEM, 3MC and 5FS submissions. 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 be initiated before the report submission. In order to initiate the CR process before the report submission. The lab **shall** send an IUTA 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 Implementation Under Test (IUT) list. The IUTA must be successfully processed by the NIST CMVP automated system. (This includes 1OEM submission types.) 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.

o If the lab sends an IUTB for a 1OEM, a CR applies.
o 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.*"
    ▪ Only unpaid invoices can be cancelled.
o No files are required for an IUTB or IUTC. Only a properly formatted subject line is required.

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 Modules In Process (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.

4.7.3 Extended Cost Recovery Fee

An extended cost recovery (ECR) fee is applicable when a report submission requires significant additional review effort by the validators. The extended fee may be applied to all report submission scenarios. The CMVP will review the rationale for the application of the extended cost recovery fee with the CST laboratory before determination of its applicability. The extended cost recovery fee is billed separately from the CR fee, if applicable, and must be remitted prior to validation. The ECR fee varies by submission type and security level. See https://csrc.nist.gov/Projects/cryptographic-module-validation-program/notices for the current fees.

A number of factors may lead to an extended cost recovery fee.

Complexity

Typically, a report submitted by the CST laboratory 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; the review time will exceed the average and ECR will be applied or the report may be rejected and the number of modules per report reduced.

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 CST laboratories submission package or following correct process can cause a significant effort by CMVP to identify and work with the CST laboratory to discover and correct; ECR will be applied.

During CMVP review and coordination, the CMVP generates many comments and comment 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. This leads to significant and sometimes specialized effort by CMVP to resolve; ECR will be applied.

During CMVP review and coordination it may be discovered that the module is not conformant to FIPS 140 or CMVP Implementation Guidance and this was not discovered by the CST laboratory during the testing process. The determination leads to significant and sometimes specialized effort by CMVP to assess what is necessary to complete the testing; ECR will be applied.

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 CST laboratory 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.

4.8 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 CST laboratory 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 CST laboratory's proficiency.

The diagram found in Annex B: Flaw Assessment Process describes the flaw discovery handling process in detail. There are several ways for a flaw to be identified including a security-relevant CVE from the NVD database.

4.9 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 CST laboratory 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 be annotated with "revoked" and appear on the *CMVP Historical Validation List*.

4.10 CMVP Webpage Update

This section provides information about the CMVP website.

4.10.1 Official CMVP Website

The official CMVP website with all current publicly-available information on the Cryptographic Module Validation Program is https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program.

4.10.2 Cryptographic Module Validation Lists

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

- *Cryptographic Module Validation List* – a single overall list or a list resulting from a basic search from a combination of vendor, module name, or certificate number.
- *CMVP Historical Validation List* – an advanced search with Validation Status set to "Revoked" or "Historical" will generate a single list of
    - revoked certificates;
    - modules with non-approved algorithms on the approved algorithms list (e.g. due to algorithm transitions); and
    - certificates older than 5 years.
- *Modules In Process*
- *Implementation Under Test*

4.11 CMVP Certificate Page Links

For each certificate there are several links from these pages that may be useful.

4.11.1 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.

4.11.2 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.

4.11.3 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.

4.11.4 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.

4.11.5 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.

4.12 Update Frequency of Validation Lists

Validation lists are updated as required, often several times a day during normal business hours. More specific information is provided below.

4.12.1 Cryptographic Module Validation List

This list is updated when new validation certificates are posted to the web site for a cryptographic module or group of cryptographic modules, when validations are extended to new versions of the cryptographic module through a letter re-validation or when a change is requested in the Vendor information such as the Point of Contact or the Vendor’s Name.

4.12.2 Modules In Process

This list is updated and posted daily. 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.

4.13 Usage of FIPS 140-3 Logos

The FIPS 140-3 logo request form is available from the CMVP web site: http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402LogoForm.pdf. The form includes the terms of use. Completed forms are sent to cmvp@nist.gov. If approved, NIST CMVP will send the artwork to the requestor.

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 CST laboratories 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 CST laboratories as proprietary. The statistical information derived from the collected data is considered to be non-proprietary.

5.3 Collected Metrics

With the update of Cryptik, 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 Documentation Maintenance Processes

This section provides information on the process and timing for updates and maintenance of documents pertinent to the Cryptographic Module Validation Program. Where applicable, the title of the person responsible for the update and/or maintenance of the document is identified.

6.1 FIPS 140-3 Publication (and subsequent Publications)

Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce pursuant 15 USC 278g-3. The standard specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information. FIPS 140-3 directs the CMVP to be a validation authority, utilizing the ISO/IEC 19790:2012, security requirements for cryptographic modules, and ISO/IEC 24759:2017, *Test requirements cryptographic modules*. FIPS are reviewed every 5 years for consideration of update.

Responsible Positions: NIST CMVP and CCCS CMVP Program Managers.

6.2 Cryptographic Module Requirements

ISO/IEC 19790:2012, *Security requirements for cryptographic modules* are developed and managed by the International Organization for Standardization, (ISO), an independent, non-governmental international organization with a membership of 164 national standards bodies. Through its members, it brings together experts to share knowledge and develop voluntary, consensus-based, market relevant International Standards that support innovation and provide solutions to global challenges. The standard is typically reviewed by an ISO committee every three years for consideration of revision.

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

6.3 Derived Test Requirements

ISO/IEC 24759:2017 *Test requirements cryptographic modules* are developed based on the requirements of ISO/IEC 24759:2017 and managed by the International Organization for Standardization, (ISO), an independent, non-governmental international organization with a membership of 164 national standards bodies. Through its members, it brings together experts to share knowledge and develop voluntary, consensus-based, market relevant International Standards that support innovation and provide solutions to global challenges. The standard is typically reviewed by an ISO committee every three years for consideration of revision.

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

6.4 Special Publication 800-140*x*

The CMVP manages the variances allowed in the ISO/IEC 19790:2012 and ISO/IEC 24759:2017 through the SP 800-140x documents. Specifically, the SP 800-140 provides additional evidence and testing that is necessary to meet CMVP cryptographic module requirement evidence, while also providing to ISO/IEC recommended adjustments to the existing standard when next reviewed. The remaining SP 800-140A through SP 800-140F provide additional requirements for vendor evidence, security policy, approved encryption and key management, authentication and non-invasive physical security requirements. Each SP 800-140*x* document will be updated as needed, following the publication of the draft for public comment and resolution by CMVP.

Responsible Positions: NIST CMVP and CCCS CMVP Program Managers.

6.5 Cryptographic Algorithm FIPS and NIST Special Publications

Approved cryptographic algorithms are specified in Federal Information Processing Standards (FIPS) and in NIST Recommendations, which are published as NIST Special Publications (SPs). Both types of publications are periodically reviewed. At any time, including during the official review, the publications may be updated to include new cryptographic algorithms or remove cryptographic algorithms that are no longer considered secure.

Public comments are requested in the Federal Register on publications under review, on any new publications, or on changes to existing publications.

For FIPS publications, any received comments are addressed, and the draft FIPS is submitted to the U.S. Secretary of Commerce for approval and subsequent announcement in the Federal Register. If a FIPS under review has not been modified, it is designated as *Reaffirmed* and assigned a new publication date.

For NIST Recommendations, the NIST Special Publications are posted on the NIST web site (https://csrc.nist.gov/publications/sp800) after the received comments are addressed.

If a cryptographic algorithm is to be revoked, a suitable transition period for the discontinuance of the cryptographic algorithm will be planned, communicated through the Federal Register and the CMVP official websites, and implemented.

FIPS cryptographic algorithm publications and other FIPS standards are posted on https://csrc.nist.gov/publications/fips.

Responsible Positions: Assigned individuals in NIST Cryptographic Technology Group.

6.6 Implementation Guidance

NIST and CCCS draft additions to IG for both technical and policy matters. Often, draft additions are distributed to all the CST laboratories for comment and/or discussed in CST laboratory management meetings before they are posted.

Implementation Guidance is posted on the CMVP website on the web page associated with the FIPS 140-*x* to which it applies.

Responsible Position: NIST CMVP and CCCS CMVP Program Managers.

6.7 FAQ for the CMVP

The FAQ is updated on an as-needed basis, usually in response to a *Request for Guidance* received from the CST laboratory that is assessed as applicable to a particular implementation type of cryptographic module or programmatic situations.

NIST and CCCS draft additions to FAQ for both technical and policy matters. Often, draft additions are distributed to all the CST laboratories for comment and/or discussed in CST Laboratory Management Meetings before they are posted.

FAQ is posted on the CMVP website on the web page associated with the FIPS 140-*x* standard to which it applies.

Responsible Position: NIST CMVP and CCCS CMVP Program Managers.

6.8 Test Tools

6.8.1 CRYPTIK

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 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.

Responsible Individual: NIST CMVP Program Manager.

6.8.2 METRIX Collection Tool

The METRIX tool **shall** be used by the CST laboratories for metrics collection and reporting. For detailed information on the METRIX tool functionality refer to the METRIX_UserGuide.doc document and to the associated METRIX Release Notes document. Information about new features, enhancements, and bug fixes are provided as part of the release process of the new version of the tool.

Suggestions for new features or functionality for the tool are solicited from the CST laboratories and the CMVP Validation Authorities prior to the development of the release. A summary of the changes made for the released version of the METRIX tool accompanies the tool.

Responsible position: CCCS CMVP Program Manager

6.8.3 METRIX Repository Tool

The METRIX Repository tool is used by the CMVP to create queries, load the data collected from the CST laboratories, and create statistical information on the metrics collected. The METRIX Repository tool is not intended to be distributed to the CST laboratories.

Responsible position: CCCS CMVP Program Manager

6.8.4 Suggested Tools for Physical Testing

As indicated in HB 150-17 Section B.6.4.2, a CST Laboratory **shall** meet the minimum hardware and software requirements for physical security testing. The CST Laboratory 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
Dremmel "Type" Rotary Tool (including accessory bits: cutting, grinding, drilling, carving, etc)
Jeweler's screw drivers (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
VOM or 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
Temperature Chamber

Non-Invasive testing equipment – TBD

6.9 CST Laboratory Accreditation Standards

6.9.1 Handbook 150 – Procedures and General Requirements

It is essential for the mutual recognition of NVLAP-accredited laboratories by other laboratory accreditation bodies that NVLAP procedures maintain their consistency with international standards and guidelines. NVLAP signs Mutual Recognition Arrangement (MRA) or Multilateral Recognition Arrangement (MLA) agreements for organizations of laboratory accreditation bodies such as the International Laboratory Accreditation Cooperation (ILAC) group, the Asia Pacific Laboratory Accreditation Cooperation (APLAC) group, the Inter American Laboratory Accreditation Cooperation (IAAC) group, the European co-operation for

Accreditation (EA) association, and the National Cooperation for Laboratory Accreditation (NACLA) group. Specifically, NVLAP procedures must be consistent with in the current version of ISO/IEC 17025: *General Requirements for the Competence of Testing and Calibration Laboratories* and ISO/IEC Guide 58: *Calibration and Testing Laboratory Accreditation Systems* **-** *General Requirements for Operation and Recognition*. Handbook 150 may need to be restructured from time to time so that it conforms to internationally accepted rules for the structure and drafting of standards and similar technical documents and ensure it is easy to understand and use.

Revisions to NIST Handbook 150 must be published in the US Federal Register and officially approved by the office of the U.S. Secretary of Commerce. The Forward of NIST Handbook 150 summarizes the changes made in the current edition of the handbook since the last published edition of the handbook.

NIST Handbook 150, is posted on the NVLAP website at https://www.nist.gov/nvlap/publications-and-forms/nvlap-handbooks-and-lab-bulletins and distributed to the NVLAP-accredited laboratories after publication. Currently the most recent version as of the latest update of this manual is the 2020 Edition.

Responsible Position: Chief of NVLAP.

6.9.2 Handbook 150-17 – Cryptographic and Security Testing

Handbook 150-17, as the program specific handbook for Cryptographic and Security Testing, is revised on a periodic basis. Changes in this handbook are made in recognition of advancements in technology and tools or when a change is made in the general accreditation requirements for a Cryptographic and Security Testing laboratory or requirements for meeting a defined accreditation level.

Lab bulletins are used to inform laboratories of program additions and changes, and to provide clarification of program-specific requirements. Bulletins for Handbook 150-17 should be inserted into the handbook until the handbook is revised. When Handbook 150-17 is revised, any lab bulletins issued for the previous edition of the handbook will be incorporated into the new edition of the handbook.

Revisions to Handbook 150-17 are made by the Program Manager for Information Technology Security Testing. Handbook 150-17 is available on-line: https://www.nist.gov/nvlap/publications-and-forms/nvlap-handbooks-and-lab-bulletins.

Responsible Position: Program Manager, NVLAP Information Technology Security Testing (Common Criteria; Cryptographic Security; Healthcare IT).

6.9.3 Management Manual

The *CMVP Management Manual*, this document, is revised as necessary and posted on the official CMVP website. It will also be reviewed biannually.

Responsible Position: NIST CMVP and CCCS CMVP Program Managers.

7 CMVP General Testing and Reporting Guidance

In order for CMVP to more efficiently manage the program, additional testing requirements are addressed below. The purpose of these requirements is not to impact the cryptographic module requirements of ISO/IEC 19790:2012 nor the testing requirements of ISO/IEC 24759:2017.

7.1 Addition of cryptographic security methods to SP 800-140C and SP 800-140D

7.1.1 CAVP testing

As new security methods are published and approved, the CMVP will occasionally add additional security functions and approved sensitive parameter generation and establishment methods to SP 800-140 C and D. Adding new methods to these SPs will often be accompanied by new testing being available by the CAVP.

Algorithm and component testing will be added to the CAVP ACVTS production server as they become ready, and will not be bundled into releases in the same way as was historically done with CAVS. The CAVP and CMVP also anticipate that algorithm/component testing will be available shortly after, if not before, a standard is finalized and added to the 140 Annexes.

If testing becomes available in a 3 month period, then the transition would occur at the end of the following 3 month period. For example:

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 3- CAVP testing released during these dates are followed by CMVP Transition dates

So, for example, 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 December 31, where after that date vendor affirming to algorithms A, B, or C will be prohibited in submitted reports.

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

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

- only approved methods that have been tested and received a CAVP validation certificate would be allowed. 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 un-tested 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, or the changes are non-security relevant, this change can be submitted under scenario 1AU (see Section 4.4 – *Submission Scenarios*). If the module is changed with security relevant changes, this can be submitted under scenarios 3MC or 5FS as applicable.

Note: To track the algorithms and their transition dates, the CAVP and CMVP keeps an up-to-date table available on their websites (https://csrc.nist.gov/Projects/cryptographic-algorithm-validation-program/cst-lab-transition);

7.1.2 **Vendor Affirmation**

However, if CAVP testing is not available, then the following guidance is applicable.

If new approved methods (e.g. NIST FIPS, Special Publication, etc.) are added to the Annexes which provide a new method that did not exist before (e.g. key establishment), until such time that CAVP testing is available for the new method, the CMVP will:

- if applicable, allow continued implementation of methods as provided by existing guidance (e.g. untested and listed as non-approved but allowed in approved mode).; and
- allow the vendor to implement the new approved method (untested, listed as approved and allowed in approved mode with the caveat “vendor affirmed”). See Annex A for examples of the “vendor affirmed” caveat. A “vendor affirmed” algorithm should implement conditional self-tests unless otherwise covered by existing conditional self-tests or will be considered non-approved should testing be available at a later time.

If new approved methods (e.g. NIST FIPS, Special Publication, etc.) are added to Annexes which provides a new method commensurate with those that currently exist (e.g. a new symmetric key algorithm, RNG, DRBG, hash, digital signature, etc.), until such time that CAVP testing is available for the new method, the CMVP would:

- allow prior approved methods (tested and listed as approved); and
- allow the vendor to implement the new approved method (untested, listed as approved and allowed in approved mode with the caveat vendor affirmed)

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 un-tested and un-validated security functions.

7.2 Testing using Emulators and Simulators

Under certain circumstances it may not be possible to test a module directly. In these cases CMVP has permitted the use of emulators and simulators to model the behavior of the module. 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 many other variables may not be modeled correctly or with certainty.

A simulator exercises the actual module source code (e.g., VHDL code) prior to physical entry into the module (e.g., an FPGA or custom 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 error 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.
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 already allowed 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 by the CST laboratory 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 operational environment 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, **AS2.09** 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.

7.3 Remote Testing of Modules

The testing of a cryptographic module can be performed either by providing the module to the laboratory or preparing it for testing at the vendor's facility. This testing requirement is clear for a hardware module which has self-contained operational environment and can only be physically located either in the laboratory or at the vendor's facility for testing. For a software cryptographic module that relies on an operating environment outside of the module's logical boundary, it is unclear whether it is permissible for the testing to be performed by providing the compiled binary code as a software cryptographic module to the laboratory but preparing its operating environment for testing at the vendor's facility.

Modern day networking enables the testing and deployment of software remotely on a General-Purpose Computer (GPC) that is either not necessary or even not possible to be physically accessible by the human operator. A vendor may have satellite development centers or remotely working developers who test their software on GPCs located elsewhere via the corporation private intranet. Laboratory personnel conducting testing at the vendor's facility may still end up utilizing an operating environment that the tester does not have physical access to and control over. Traveling to the vendor's facility and then performing the test on its remote operating environment not only costs time and money but also does not make a technical difference on the test results in comparison to performing the test on the same remote operating environment directly from the laboratory, as long as the network connection (e.g. VPN connection, SSH connection) between the local test console and the remote test operating environment provides the same level of security as testing onsite. The operational testing requirements of FIPS 140-3 should be able to use these technologies in a way that is practical and secure for all parties involved. The information below addresses the need for testing a software module on a remote operating environment while obtaining the equivalent assurance as if the test were performed at the vendor's facility.

A software cryptographic module **shall** only be tested on a remote operating environment if the following conditions are met:

1. A software cryptographic module is provided by the vendor to the laboratory and its boundary and version is verified on screen against the Security Policy.
2. The network access to a remote test operating environment **shall** be authorized and controlled by the vendor. A 3rdparty cloud system that provides its own operating environment, such as an operating system and hardware upon which the tester has no control (possible examples are: Amazon Web Services, Microsoft Azure, and Google Cloud) **shall** not be used. The tester must have control of the operating environment during testing. The lab's network must be connected to the vendor's network via a secure VPN connection or SSH connection. If a tester wishes to work offsite then the tester 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 must initialize, install, and start-up the module while connected to the remote operating environment.
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 to obtain evidence of test results such as printing out reports, taking screenshots 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 140-3requirements 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 software 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. Entropy can be effectively analyzed, and an entropy report can be generated by the lab.
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 demonstrate 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 must be able to 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.

7.4 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 that cannot be designated as Not Applicable according to the following:

• Section 6.7, Physical Security may be designated as Not Applicable if the cryptographic module is a software-only module and thus has no physical protection mechanisms;

• Section 6.6, Operational Environment may be designated as Not Applicable if the operational environment for the cryptographic module is a limited or non-modifiable operational environment and Section 6.7, Physical Security greater than Security Leve 1 (**AS06.04**);

• Section 6.8, Non-invasive security is Non Applicable as there are currently no requirement 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 Not Applicable.

7.5 PIV References

The PIV card application NPIVP validation is a prerequisite to the module validation. For module validation, the PIV card application **shall** be tested on the module to be validated (i.e. same operational environment). If a PIV card application will be used on different cryptographic module operating environments, the PIV card application **shall** be tested and validated by the NPIVP on each of the unique operating environments employed.

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.

In addition, the PIV card application validation entry **shall** 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 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.

The PIV Certificate number must be referenced on a module validation.

The NPIVP validation entries can be found at:

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

7.6 Module count definition

The CMVP allows multiple modules to be validated on a single certificate. However, the separation of these modules in the report is not always clear.

Determining the module count for a validation depends on the type of report; that is, if it is Software, Hardware, Firmware, or a Hybrid.

Software:

For a software module, its binary package(s) compiled from its source code is the Implementation Under Test (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.

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.

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 and these 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 (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).

- o 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”.

- o 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 (with non-security relevant differences), the module count is “2” to reflect the hardware platforms.

Firmware:

For a firmware module, the firmware package itself **shall** be considered a separate module, regardless of the number of hardware platforms it was tested on.

Examples:

- If a firmware package was validated as firmware version 1.0, and this package was tested on two hardware platforms (e.g. hardwareX version 1.0 and hardwareY version 2.0), the module count is "1".
- If a report includes firmware version 1.0 and firmware version 2.0, then the module count is "2", regardless of the number of hardware platforms these packages were tested on.

Hybrid:

Since hybrid modules (firmware-hybrid or software-hybrid) 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 firmware-hybrid 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 firmware-hybrid 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)

7.7 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 are Category is provided in Table 4.

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 CAVS equivalency criteria for guidance
Programmable Logic Devices	o CPLD, FPGA, PAL

Table 4- 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:

o 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.

o 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:

o The use of some technologies may introduce Security Relevant differences that cannot be predicted by this IG. 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 IG.

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 IG only applies to Operational testing of Hardware modules

- Physical security testing (ISO/IEC 19790:2012, section 7.7) is not addressed in this IG for Security Level 2 and above. In other words, this IG 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 IG. If the CPU is different between modules on the same certificate, then the full Revalidation Regression Test Suite must be run (found under the FIPS 140-3 Resources Tab of the CMVP website).

- 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.

7.8 Revalidation Requirements

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.) There are twelve possible submission Scenarios (1V1, 1OEA, 1VA, 1UP, 1AU, 1OEM, 1MU, 2SC, 3CVE, 3MC, 4PSC, 5FS) All Scenarios must be processed and submitted to the CMVP by a CST Laboratory.

For a description of each scenario and the associated NIST cost recovery fee, please consult the CMVP Resources page at:

https://csrc.nist.gov/Projects/cryptographic-module-validation-program/resources.

Annex A Validation Information Formatting

The CST laboratory **shall** use the CMVP provided Web CRYPTIK tool to document the module test information. The test report information is presented to the CMVP for review and validation as indicated in the Management Manual Section 4.3 - *Preparation and Submission of the Validation Submission*.

The instructions below describe how the information **shall** be formatted to appear on the NIST CMVP validation web page via entry into CRYPTIK.

Laboratory Information

1. **Lab Name** - the name of the CST laboratory. Please include any registration marks or special characters[3]
2. **NVLAP code** [**nnnnnn-n**] - the code assigned by NVLAP to the CST laboratory
3. **Address** - the street, building, post office box, suite, etc. components of the CST Laboratory's address
4. **City** - the city of the CST Laboratory's address
5. **State / Prov** - the state or province of the CST Laboratory's address
6. **Postal Code** - the postal code of the CST Laboratory's address
7. **Country** - the country of the CST Laboratory's address
8. **Signature 1 and Title –** name and position (e.g. approved signatory)
9. **Signature 2 and Title -** name and position (e.g. technical review)
10. **Signature 3 and Title -** name and position (e.g. main tester)

Vendor Information

1. **Vendor Name** - the name of the vendor (including Corp., Inc., Ltd., etc.) that developed the cryptographic module. Please include any registration marks or special characters[1].

   Examples: **AcmeSecurity, Inc.**

   Acmeproducts(R), Ltd.

   AcmeSecurity, Inc. and Acmeproducts(R), Ltd.

   It is desirable that the vendor name be consistent on validation certificates issued for modules from the same vendor. The module listing which includes the Vendor Name can be found at: https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules/Search

2. **Address** - the street, building, post office box, suite, etc. components of the vendor's address
3. **City** - the city of the vendor's address
4. **State / Prov** - the state or province of the vendor's address

[3] The special symbols may not translate to the _vendor.txt properly. The special symbol may be indicated as follows: (R) for ®, (C) for ©, (TM) for ™, etc.

5. **Postal Code** - the postal code of the vendor's address
6. **Country** - the country of the vendor's address
7. **Web Site** - generally the vendor's main URL. Do not include the prefix https://
8. **Product Link** – a URL that may be specific to the module or products which utilize the module. Do not include the prefix https:// or duplicate the Web Site URL.
9. **POC1** - the primary vendor point of contact which may include email, phone number, and fax number.
10. **POC2** - the secondary vendor point of contact which may include email, phone number, and fax number.

Module Information

1. **Lab Internal ID** – the internal ID used and maintained by the CST laboratory.
2. **Tested Date** – the last date in which any form of testing or documentation updates were performed.
3. **CSTL TID** – first two digits represent the CST laboratory ID, and the remaining four characters are assigned by the CST laboratory as a unique identifier.
4. **CSEC TID** – the four characters are assigned by CCCS as a unique identifier
5. **Tester 1** – Primary tester of the module.
6. **Tech Reviewer 1** – CVP ID.
7. **Tester 2** – Secondary tester/reviewer of the module.
8. **Tech Reviewer 2** – CVP ID.
9. **Module Name(s)** - the complete name of the cryptographic module. Do not include the version number with the name unless by vendor choice. The name of the cryptographic module **shall** be consistent with ISO/IEC 24759:2017 **AS02.11** and the name found in the Security Policy and test report. Please include any registration marks or special characters[4].

   Examples: **Crypto Acceleration Token**

   Secure Cryptographic ToolKit™

   Best Crypto©

   If the test report represents multiple modules, list all module names.

   Examples: **Crypto Sensor AM-5000 and AM-5010**

   Crypto 8000 PCI, Crypto 9000 PCI and Crypto Plus++ PCI
10. **FIPS Version** – either FIPS 140-2 or FIPS 140-3.
11. **Module Count** - see the Management Manual Section 7.6 - *Module count definition*.
12. **Module Classification** – choose the most applicable module classification.

[4] The special symbols may not translate to the _vendor.txt properly. The special symbol may be indicated as follows: (R) for ®, (C) for ©, (TM) for ™, etc.

13. **Hardware, Software and Firmware Versioning** - the specific versioning information representative of each of the crypto module's elements. This number **shall** be of sufficient level such that updates/upgrades/changes **shall** be reflected in a new version (see **AS04.32**). For example, version 4 may not be sufficient if the releases are numbered 4.0, 4.1, 4.2, etc. The version number may also include letters, for example, 4.0a, 4.0b, 4.0c, etc. This **shall** include the version numbers for each element; hardware, software, and firmware, if applicable. Each elements version number (e.g. hardware, firmware, software) **shall** be separated by a semi-colon. If a module does not include an element, leave the field blank; do not enter "NA". The version numbers **shall** be the same as the ones found in the Security Policy. For example, hardware version: 4.2; software version: 4.0a.

    If possible, a hardware version of a module **shall** represent all the components of the module, included (**AS02.15**) or excluded (**AS02.14**). If there are any additional components, included (**AS02.15**) or excluded (**AS02.14**), that are inside the module boundary but are not within the scope of the hardware version then the module certificate **shall** list these additional components separately in the hardware version field. Brackets **shall** be used to group hardware versions with their corresponding components. If the module is a collection of different hardware components, included (**AS02.15**) or excluded (**AS02.14**), and does not contain a hardware version, then the module certificate **shall** list all of the components of the module in the hardware version field without referencing any hardware version.

    If there are multiple modules listed on the certificate, or if there are multiple part numbers with different versions of firmware for example, brackets **shall** be used to clearly indicate the pairings between the versioning information and/or the module names.

    Examples: **(Hardware Version: 4.2; Software Version: 4.0a; Hardware)**
    Hardware module with software embedded within it.

    (Hardware Versions[5]: 5.2 and 5.3, Build 3; Firmware Version: 2.45; Hardware)
    Two different hardware modules, each with the same embedded firmware. All of the components in these hardware modules must be considered: included (**AS02.15**) or excluded (**AS02.14**).

    (Hardware Versions: 5.2 [1] and 5.3 [2], Build 3; Firmware Versions: 2.45 [1] and 2.50 [2]; Hardware)
    Two different hardware modules each with the specified version of embedded firmware.

    (Hardware Version: 88X8868; Software Version: 1.0; **Software-Hybrid)**
    Software hybrid module referencing the hardware and disjoint software components.

    (Hardware Version: BN45; Firmware version 1.0; Software Version 2.0; Software-Hybrid)
    Software hybrid module referencing the hardware and disjoint software versions. The hardware component also has firmware embedded within it.

    (Hardware Version: 88X8686; Firmware Version 1.4; Firmware-Hybrid)

[5] Version will be changed to plural during the posting by the CMVP

Firmware hybrid module referencing both the hardware and disjoint firmware versions.

Note the use of the commas, semi-colons and colons.

(Hardware Version: [XYZ1, XYZ2, and XYZ3 with components 1234, 1235, 1236] and [ZYX1, ZYX2 and ZYX3 with components 1234, 5123, 6123]; Firmware Version: 1.0; Hardware)
Hardware module contains multiple hardware versions that have additional corresponding components that are included (**AS02.15**) or excluded (**AS02.14**).

(Hardware Version: P/N 5432, 7654, and 4321; Firmware Version: 1.0; Hardware)
Hardware module that is a collection of hardware components that are included (**AS02.15**) or excluded (**AS02.14**) rather than a versioned hardware module.

14. **Approved Algorithms** - the approved security functions included in the cryptographic module and utilized by the module's callable services or internal functions. The security function is listed and then the applicable algorithm Certificate number in parentheses. Do NOT include the modes or key lengths (e.g., ECB, CBC; 128 bits). All algorithm entries must be separated by semi-colons. The security functions **shall** be listed in alphabetical order using the official CAVP security function name and examples below.

    If a module contains within it or is bound to an already validated cryptographic module, all approved security functions that are used by the module's callable services and internal functions **shall** be annotated on the certificate (e.g. both those within the embedded/bound module and in addition to the embedding/binding module) and included within the Security Policy with a clear distinction on if the algorithms are implemented within the embedding/binding module or the embedded/bound module. Algorithms that are never called **shall not** be listed on the certificate. An algorithm that can only be called by a service that performs the self-tests also **shall not** be listed on the certificate; however, the module's Security Policy **shall** have an entry for the corresponding self-test and explain that this algorithm can only be executed when running a self-test.

    The algorithm **shall** meet all three (3) conditions to be listed as approved:

    1. an approved security function as specified in **SP 800-140C** or **SP 800-140D** and validated by the CAVP or vendor affirmed per CMVP implementation guidance;
    2. meet all requirements of FIPS 140-3 (self-tests, etc.); and
    3. used in at least one approved cryptographic function or service for that cryptographic algorithm in an approved mode of operation.

    Examples: **AES (Cert. #A100);**

    CKG[6] (vendor affirmed);

[6] Cryptographic Key Generation; SP 800-133 and IG D.I.

cSHAKE[7] **(Cert. #A50);**

CVL[8] **(Cert. #A4);**

DRBG[9] **(Cert. #A12);**

DSA[10] **(Cert. #A200);**

ECDSA[11] **(Cert. #A100);**

ENT[12]**;**

HMAC[13] **(Cert. #A23);**

KAS[14] **(Cert. #A33);**

KAS-SSC[15] **(Cert. #A66);**

KAS (KAS-SSC Cert. #A66, KDA Cert. #A11, CVL Cert. #A43);[16]

KAS (KAS-SSC Cert. #A66, CVL Cert. #A153);[17]

KAS-RSA-SSC[18] **(Cert. #A91);**

KAS-RSA (KAS-RSA-SSC Cert. #A91, CVL Certs. #A153 and #A155, CVL Cert. #A41);[19]

Note. Two different CVL certificates, #A153 and #A155 demonstrate the KDF validation testing. The CVL certificate #A41 demonstrates the tested key confirmation functionality. There are several possible reasons for obtaining more than one CVL certificate for KDF testing. As with any other algorithm, the vendor might have performed an algorithm testing in multiple operating environments. The vendor could have also chosen to test different key derivation functions separately and to obtain different certificates. Even when testing the same algorithm (or a CVL function) in the same operating environment, the vendor may decide to test various functionalities and different parameter sets (such as key lengths) separately and have multiple certificates issued by the

[7] Customizable SHAKE function; SP 800-185.

[8] Component Validation List; see CAVP CVL and IG 2.4.B.

[9] Deterministic Random Bit Generator; SP 800-90A.

[10] FIPS 186-2 (for Signature Verification only) or FIPS 186-4.

[11] FIPS 186-2 (for Signature Verification only) or FIPS 186-4.

[12] An entropy source tested to SP 800-90B. No algorithm certificate number is needed.

[13] Includes truncated HMACs per IG C.D.

[14] Key Agreement Scheme; tested to SP 800-56A Rev3.

[15] Tested for a compliance with one or more shared secret computation schemes in Section 6 of SP 800-56A Rev3. The information about the scheme's security strength is documented in the module's Security Policy.

[16] An SP 800-56A Rev3 compliant key agreement scheme, where testing is performed separately for the shared secret computation, an SP 800-56C Rev1 or Rev2 compliant KDF, and a key confirmation.

[17] An SP 800-56A Rev3 compliant key agreement scheme, where testing is performed separately for the shared secret computation and for a KDF compliant with either SP 800-135 Rev1 or RFC 8446. No key confirmation.

[18] Tested for a compliance with the derivation of the shared secret as shown in SP 800-56Br2. The information about the derived shared secret security strength is documented in the module's Security Policy.

[19] An SP 800-56Br2-compliant key agreement scheme, where testing is performed separately for the shared secret computation, for a key derivation function compliant with SP 800-135 Rev1 and/or RFC 8446, and for the key confirmation.

CAVP.

KBKDF[20] **(Cert. #A2);**

KDA[21] **(Cert. #A25);**

Note 1. Obtaining a CVL certificate for a tested TLS 1.3 KDF does not lead to granting the vendor a KDA algorithm certificate; in order to receive a KDA certificate, the implementation's compliance to **SP 800-56C Rev1** or **Rev2** **shall** be tested separately. This testing may include either a one-step key derivation, or a two-step key derivation (shown in Sections 4 and 5 of **SP 800-56C Rev1/Rev2**, respectively), or both.

Note 2. A KDA algorithm certificate obtained by the vendor may also be used to claim the correct implementation of the HKDF key derivation function, but only if the KDA certificate has been issued for testing the two-step key derivation documented in Section 5.1 of **SP 800-56C Rev1/Rev2** using HMAC for the randomness extraction in Step 1, as shown in Figure 1 in **SP 800-56C Rev1/Rev2**. The module's Security Policy **shall** provide the justification for claiming a compliant implementation of the HKDF.

The HKDF key derivation function is documented in the IETF RFC 5869 which references the following paper: https://eprint.iacr.org/2010/264.pdf for the algorithm's details.

KMAC[22] **(Cert. #A25)**

ParallelHash[23] **(Cert. #A25);**

PBKDF[24] **(Cert. #A25);**

RSA[25] **(Cert. #A133);**

SHA-3[26] **(Cert. #A55);**

SHAKE[27] **(Cert. #A50);**

SHS[28] **(Cert. #A23);**

Skipjack[29] **(Cert. #45);**

Triple-DES (Certs. #A78 and #A122);

[20] Key Based Key Derivation Function; SP 800-108.
[21] Key Derivation Algorithm compliant to SP 800-56C Rev1 or Rev2.
[22] KECCAK Message Authentication Code; SP 800-185.
[23] Based on cSHAKE, and thus, on KECCAK; SP 800-185.
[24] Password Based Key Derivation Function; SP 800-132.
[25] FIPS 186-2 (for Signature Verification only) or FIPS 186-4.
[26] FIPS 202.
[27] Extendable output function of SHA-3; FIPS 202.
[28] FIPS 180-4.
[29] Only decryption is approved for Skipjack.

TupleHash[30] (Cert. #A100);

For multiple certificate entries, the term "Cert" **shall** be pluralized (i.e., Certs), an "and" **shall** be placed between the last two certificate numbers and there **shall** be a "#" in front of each number.

Examples: **Triple-DES (Certs. #A118 and #A133);**

SHS (Certs. #A103, #A115 and #A119)

If the module supports symmetric key wrapping, one of the following annotations **shall** be used, depending on the approved wrapping algorithm. In every case, the referenced AES, Triple-DES and/or HMAC certificates **shall** be listed separately on the approved line in addition to the KTS entry. Please refer to NOTE 1 below to determine when the strength caveat applies:

KTS (Triple-DES Cert. #A50; SSP establishment methodology provides 112 bits of encryption strength) – an implementation has been tested for its compliance with three-key Triple-DES TKW and this mode of the Triple-DES is used for key wrapping .

KTS (AES Cert. #A100) – an implementation has been tested for its compliance with AES KW and/or AES KWP and this mode of AES is used for key wrapping.

KTS (AES Cert. #A200) - has been tested for its compliance with AES GCM (or any other authenticated encryption mode) and this mode of AES is used for key wrapping.

KTS (AES Cert. #A300) - has been tested for its compliance with both AES KW and AES GCM and each of these two modes of AES may be used for key wrapping. Each tested AES mode, KW and GCM (and any other) will be shown in the AES algorithm certificate. The Security Policy **shall** explain how each applicable mode of AES is used for key wrapping.

KTS (AES Cert. #A700 and HMAC Cert. #A200) - Example of CAVP testing of disjoint AES encryption and HMAC authentication with appropriate strength.

KTS (AES Cert. #A750 and HMAC Cert. #A250; SSP establishment methodology provides 192 bits of encryption strength) - Example of CAVP testing of disjoint AES encryption and HMAC authentication where an AES wrapping key may be of lower length than wrapped key.

KTS (AES Cert. #A300 and HMAC Cert. #A355; SSP establishment methodology provides 128 or 192 bits of encryption strength) – a combination of AES in any mode and message authentication using HMAC is used for key wrapping. There is a range of AES key lengths.

KTS (AES Cert. #A400 and AES[31] Cert. #A10; SSP establishment

[30] SHA-3-derived hash function; SP 800-185.

[31] When two algorithm names are included in a symmetric-key-based KTS scheme caveat, the first name shows an algorithm used to perform the encryption and the second one – the message authentication.

methodology provides between 128 and 256 bits of encryption strength) - a combination of AES in any mode and message authentication using AES CMAC or GMAC is used for key wrapping.

KTS (AES Certs. #A10, #A20 and #A55 and AES Certs. #A100, #A200, #A300 and #A366; SSP establishment methodology provides 128 or 256 bits of encryption strength) - a combination of an AES in any mode (with the AES algorithm certificates #A10, #A20 and #A55) and message authentication using AES CMAC or GMAC (with the AES algorithm certificates #A100, #A200, #A300 and #A366) is used for key wrapping. An AES encryption/decryption may be performed with the AES key sizes of 128 and 256 bits.

NOTE 1: The AES or the Triple-DES algorithm certificate will provide information on the length of the wrapping key. To make a decision if this length is sufficient to avoid adding a strength caveat, one has to know the range of the possible lengths of the wrapped keys. If the strength of the largest key that can be established by a cryptographic module is greater than the comparable strength of the implemented SSP establishment method, then the module certificate and Security Policy **shall** be annotated with, in addition to the other required caveats, the caveat "**(SSP establishment methodology provides xx bits of encryption strength)**"[32] for that SSP establishment method as explained in IG D.B – *Strength of SSP Establishment Methods*. No strength caveat is required if the wrapping key used in key transport be equal or of greater strength than the wrapped key. This applies to both an approved KTS, or the allowed SSP establishment methods (see section 13 below for allowed SSP establishment methods). A similar caveat is used when a key is established using a key agreement protocol that might cause the resulting cryptographic strength of the key to be less than the key length in bits.

NOTE 2: The strength of an HMAC key and the size of the hash output are not reflected in the computation of the equivalent encryption strength.

If the module supports an RSA-based key encapsulation/un-encapsulation and the vendor obtains an algorithm certificate of compliance with **SP 800-56Br2** then one of the following annotations **shall** be used, depending on the necessity to address the algorithm strength:

KTS-RSA (Cert. #A100)

KTS-RSA (Cert. #A100; SSP establishment methodology provides 112 bits of encryption strength)

KTS-RSA (Cert. #A100; SSP establishment methodology provides between 112 and 150 bits of encryption strength)

NOTE: The module’s validation certificate will not indicate if the approved RSA-based SSP establishment algorithm supports the key encapsulation, key un-encapsulation, or both. This information **shall** be included in the Security Policy.

If the module supports an RSA-based key agreement and the vendor obtains an algorithm certificate of compliance with **SP 800-56Br2** then one of the following annotations **shall** be

[32] While this caveat only has a single encryption strength claimed, other examples included in this Management Manual indicate that the strength caveat may have a range, depending on the key sizes used for the SSP establishment methodology.

used, depending on the necessity to address the algorithm strength:

KAS-RSA (Cert. #A25)

KAS-RSA (Cert. #A25; SSP establishment methodology provides 112 bits of encryption strength)

KAS-RSA (Cert. #A25; SSP establishment methodology provides 112 or 128 bits of encryption strength)

NOTE: The module's validation certificate will not indicate which approved RSA-based SSP establishment algorithms (KAS1 or KAS2, or both) are supported. Neither will the module's certificate specify whether the supported schemes include any form of key confirmation. The information about the key confirmation testing will be found in the KAS-RSA algorithm certificate and **shall** be listed in the module's Security Policy.

If the module implements a key agreement scheme based on the use of the finite field or the elliptic curve technology and the vendor obtains an algorithm certificate of compliance with **SP 800-56A Rev3** then one of the following annotations **shall** be used, depending on the necessity to address the algorithm strength:

KAS (Cert. #A72)

KAS (Cert. #A72; SSP establishment methodology provides 112 bits of encryption strength)

KAS (Cert. #A72; SSP establishment methodology provides between 112 and 256 bits of encryption strength)

NOTE1: This entry indicates compliance with a key agreement scheme from **SP 800-56A Rev3**. It uses a key derivation function compliant with **SP 800-56C Rev1** or **Rev2**.

NOTE2: The module's validation certificate will not indicate the presence of the CVL certificate for testing of the key confirmation portion of a key agreement scheme. The information about the key confirmation testing will be found in the KAS algorithm certificate and **shall** be listed in the module's Security Policy.

15. **Allowed algorithms** - cryptographic algorithms that are not approved but are allowed to be used in an approved mode of operation.

All allowed algorithms **shall** be identified in the Security Policy and listed on the validation certificate. Allowed algorithms **shall** be listed in alphabetical order on the certificate.

Examples: **AES[33] (Cert. #A300, key unwrapping);**

Diffie-Hellman[34] (shared secret computation);

[33] This is an allowed but non-SP-800-38F-compliant key unwrapping, where the key used in key transport is of equal or greater strength than the unwrapped key and therefore the strength caveat is not required.

[34] A shared secret computation compliant to IG D.F Scenario 3 (and IG C.A) with no claim of compliance with SP 800-56A Rev3. This entry **shall** be accompanied with an approved SP 800-56A Rev3 method using at least one NIST-recommended curve as required by IG D.F Scenario 3 (c).

RSA[35] (key unwrapping);

RSA[36] (key wrapping);

RSA[37] (CVL Cert. #A10, key wrapping);

Triple-DES[38] (Cert. #A200, key unwrapping);

For the non-approved SSP establishment schemes refer to IG's D.F and D.G.

All non-approved and not allowed algorithms **shall** be listed in the Security Policy but NOT on the certificate. A non-approved implementation may exist for what appears to be an approved algorithm where a CAVP validation or the requirements of FIPS 140-3 (e.g. self-test) are not met. These non-approved implementations are considered non-approved and non-compliant and **shall** be described in the Security Policy as "*non-compliant*" so that it is clear the algorithm implementation **shall** not be used in an approved mode of operation.

NOTE: Encryption strengths represented on a validation entry are based on algorithm key sizes in bits *only*. As indicated above the calculation of the encryption strength based on key size is performed per IG D.B. The effective encryption strength may be less depending upon the amount of available entropy. See IG 9.3.A, IG D.J and this guidance for additional guidance and applicable caveats.

In the following SSP establishment examples, the strength caveat *does* apply (i.e., the security strength of the SSP establishment scheme implemented by the module **can be** less than that of the agreed or wrapped key).

If the module supports, for a particular SSP establishment method, a single strength, then the caveat **shall** state the strength provided by the keys.

Examples: **RSA (key wrapping; SSP establishment methodology provides 112 bits of encryption strength)**

RSA[39] (key unwrapping; SSP establishment methodology provides 112 bits of encryption strength)

EC MQV[40] (shared secret computation provides 192 bits of encryption

[35] The module does not support RSA key wrapping but does employ RSA key unwrapping that uses a PKCS#1-v1.5 padding scheme with no claim of compliance with any testable component of SP 800-56B Rev2.

[36] Uses an RSA-based PKCS#1-v1.5 padding scheme with no claim of compliance with any testable component of SP 800-56B Rev2. If the module supports both RSA key wrapping and unwrapping in this way, or just key wrapping alone, the certificate **shall** only include a "key wrapping" entry without a separate "key unwrapping" entry.

[37] The RSADP component of an RSA-based PKCS#1-v1.5 padding scheme is tested by CAVP for its compliance with SP 800-56B Rev2. The module supports both the wrapping and the unwrapping of the cryptographic keys using RSA, hence the annotation in this example states "key wrapping", even though the listed RSADP CVL certificate applies only to the key unwrapping schemes. This CVL certificate **shall** be referenced as shown here if the implemented key transport scheme does utilize this component. Note: the RSA entry **shall not** reference the KDF CVLs, as these are not directly part of RSA key transport scheme.

[38] This is an allowed but non-SP-800-38F-compliant key unwrapping, where the key used in key transport is of equal or greater strength than the unwrapped key and therefore the strength caveat is not required.

[39] The module does not support RSA key wrapping but does employ RSA key unwrapping with 2048-bit modulus.

[40] This entry reflects Scenario 3 of IG D.F.

strength)

If a module *only* implements two specific key sizes for RSA, then:

RSA (key wrapping; SSP establishment methodology provides 112 or 128 bits of encryption strength)

If a module implements a SSP establishment scheme with several key sizes for Diffie-Hellman, MQV, RSA, EC Diffie-Hellman or EC MQV then only the range end points are indicated:

MQV (shared secret computation provides between 112 and 256 bits of encryption strength)

RSA (key wrapping; SSP establishment methodology provides between 128 and 256 bits of encryption strength)

If a module implements a SSP establishment scheme of several key sizes and also less than 112 bits of strength, then only the approved range end points are indicated.

Diffie-Hellman (shared secret computation provides between 112 and 256 bits of encryption strength)

If the module supports the key unwrapping algorithms that are not compliant with **SP 800-38F** then this **shall** be annotated in the certificate. For example:

AES (Cert. #A300, key unwrapping; SSP establishment methodology provides 128 or 192 bits of encryption strength)

Triple-DES (Cert. #A114, key unwrapping; SSP establishment methodology provides 112 bits of encryption strength)

Note: In all cases, the CMVP report reviewer must ascertain the correctness of the added caveat(s) and the most accurate wording and the best interpretation to give to the Federal users.

If the Allowed algorithms field is not applicable, mark the field as N/A.

For non-approved algorithms that have names similar to approved security functions, they are considered non-approved and non-compliant and **shall** be listed in the Security Policy but NOT on the certificate. They **shall** be described as "non-compliant" in the Security Policy so that it is clear the algorithm implementation **shall not** be used in the approved mode of operation.

16. **Module Part Number –** N/A.
17. **Module Description –** Vendor provided short description of the module.
18. **Module Embodiment** - the cryptographic module **shall** be specified as one of the three types: **Single-Chip, Multi-Chip Embedded,** or **Multi-Chip Standalone** (see ISO/IEC 19790:2012 Section 7.7.1 for examples of each).
19. **Type -** the module type is one of the following: **Software, Hardware, Firmware, Software-Hybrid** or **Firmware-Hybrid**. If a module is hardware with embedded software and/or firmware, the module's type is simply labeled Hardware.

20. **Section Level** - for each of the 12 areas, select the specific level. For ISO/IEC 19790:2012, the Software/Firmware Security (Section 7.5), Operational Environment (Section 7.6), Physical Security (Section 7.7), Non-Invasive Security (Section 7.8), and Mitigation of Other Attacks (Section 7.12) may not be applicable[41] and if so, **shall** be marked as N/A.
21. **Overall Level [n] –** the overall level of the crypto module. This value is the *lowest* value of the individual levels. Section Level 1 **shall** be set to the overall level.
22. **Submission Type –** select the submission type. See Management Manual Section 4.4 - *Submission Scenarios* for more information.
23. **Flags –** select if the module is tested with a maintenance role, bypass role and/or identity authentication.
24. **Administrative Flags** - select if the module is ITAR, should be added to the MIP List, and/or Cost Recovery is applicable.
25. **Certificate Caveat** - This caveat may be modified or expanded by the CMVP during the validation process. Cryptographic modules may not have a caveat if the module only has a single approved mode of operation.

    Examples: <no caveat>

    The module can only be installed and operated in an approved mode of operation.

    When operated in approved mode
    The module can be installed or operated in either an approved or non-approved mode of operation.

    When installed, initialized and configured as specified in Section [section number] of the Security Policy
    The module can be installed, initialized and/or configured in order to be considered a FIPS 140-3 recognized module. Without this configuration, the module is not considered a FIPS-validated module. After this configuration, a module may run in approved mode or non-approved mode (if supported) which may require additional configuration and/or procedural guidance to invoke.

    The <tamper evident seals> and <security devices> installed as indicated in the Security Policy
    Installation of the referenced components required for the module to operate in an approved mode of operation.

    When operated in approved mode and initialized to overall level 2 per Security Policy

[41] Software/Firmware Security is N/A if the module is hardware-only without firmware or software; Operational Environment is N/A if the Security Level of Section 7.7 is greater than 1; Physical Security is N/A if the module is software-only; Non-Invasive Security is N/A until non-invasive requirements are defined; Mitigation of Other Attacks may apply if the module has been *purposely* designed, built and publicly documented to mitigate one or more specific attacks not defined within FIPS 140-3.

The module can be initialized to operate at different overall levels.

> Example: A module can be initialized to either support level 2 role-based authentication or initialized to support only level 3 identity-based authentication.

When operated in approved mode with module [module name] validated to FIPS 140-3 under Cert. #xxxx operating in approved mode
The module's validation is bound to another validated cryptographic module.

> **Example:** A software cryptographic module which requires services from another validated software cryptographic module operating in the same operational environment. Application services are available from either module.

This module contains the embedded module [module name] validated to FIPS 140-3 under Cert. #xxxx operating in approved mode
If the module incorporates an embedded validated cryptographic module.

> **Example:** A software cryptographic module which is compiled with a privately linked validated software cryptographic module operating in the same operational environment. Application services are only available from the module indicated on the certificate.
>
> **Example:** A hardware cryptographic module which has embedded within its physical boundary a validated cryptographic module.

This validation entry is a non-security-relevant modification to Cert. #nnnn

If the lab submits a revalidation under scenario 1OEM. Please refer to Management Manual Section 4.4 – Submission Scenarios.

When utilizing a Trusted Channel as specified in the Security Policy

If the use of the Trusted Channel is claimed to meet the FIPS 140-3 compliance requirements of ISO/IEC 19790:2012 Section 7.3.4. Please refer to IGs 3.4.A and 9.5.A.

The module generates SSPs whose strengths are modified by available entropy
Please refer to IG 9.3.A.

The module generates random strings whose strengths are modified by available entropy
Please refer to IG 9.3.A.

The module generates SSPs and random strings whose strengths are modified by available entropy
Please refer to IG 9.3.A.

No assurance of the minimum strength of generated SSPs
Please refer to IG 9.3.A.

When entropy is externally loaded, no assurance of the minimum strength of generated SSPs
Please refer to IG 9.3.A.

The output of the DRBG may not be used to generate SSPs

If the module implements a DRBG where the module does not meet the requirements for the entropy source explained in IGs 9.3.A, D.J and D.K.

The protocol(s) <TLS, SSH, …> shall not be used when operated in approved mode

If the module implements a KDF from NIST SP 800-135rev1 and this KDF has not been validated by the CAVP. Please refer to IG D.C.

26. **Operational Environment** - the specific operational environment(s) or configuration(s) that was employed during testing by the CST laboratory **shall** be specified for all module types. (e.g. software, firmware, hardware and hybrid). This **shall** match the information in the test report in **AS02.15**. The operational environment includes the operating system(s), the tested platform(s), and the processor(s).

For Java applets, the Java environment (JRE, JVM) version **shall** be specified for all security levels. For multiple operating environment entries, separate each with a semi-colon; do not use "and".

Examples: **Microsoft Windows XP with SP2 running on a Dell Optiplex Model 4567 with an Intel i7-8550U;**

Sun Solaris Version 2.6SE running on a Sun Ultra SPARC-1 workstation with an Intel Xeon X5670;

Microsoft Windows XP with SP2 running on an HP Pavilon 4.5 with an AMD A8-3850;

HP-UX 11.23 running on an IBM RISC 6000RB2 with an Intel Xeon E3-1230

The following example for a *firmware* cryptographic module;

Example: **BlackBerry® 7230 with BlackBerry OS® Versions 3.8, 4.0 and 4.1 with Qualcomm Snapdragon S4 Plus**

If the *firmware* module's physical security meets ISO/IEC 19790:2012 Section 7.7 levels 2, 3 or 4, the hardware platform **shall** include applicable specific versioning information.

Example: **Little OS® Version 3.7b running on a Crypto Unit (Hardware Version:**

1.0) with AMD Duron 800

The following example for a *software-hybrid* cryptographic module;

Example: **Debian GNU/Linux 4.0 (Linux kernel 2.6.17.13) running on a 4402-A ViPr Desktop Terminal with Intel i7-8550U**

The following example for a *firmware-hybrid* cryptographic module; the certificate **shall** specify the operating environment (operating system and hardware platform with processor) that was used for testing.

Example: **BlackBerry OS Version 4.2 running on a BlackBerry 8700c with Qualcomm Snapdragon S4 Plus**

The operational environment includes the operating system(s) the tested platform(s) and the processor(s). The operating system may also represent virtual environments. Virtual environments are run by computer software, firmware or hardware called a hypervisor. Native hypervisors run directly on the host computer. Hosted hypervisors run on a conventional operating system.

- For a Type 1 (or native) hypervisor, the OE listing **shall** include the platform, guest OS, hypervisor and processor using the following format:

  Operational Environment: **<*Guest OS*>** on **<*hypervisor*>** running on **<*platform*>** with <***processor***>

  An example is: Windows 10 on VMWare ESX 5 running on a Dell Optiplex 5460 with an Intel Core i5

- For a Type 2 (or hosted) hypervisor, the OE listing **shall** include the platform, guest OS, hypervisor, host OS and processor using the following format:

  Operational Environment: **<*Guest OS*>** on **<*hypervisor*>** on **<*Host OS*>** running on **<*platform*>** with <***processor***>

  An example is: Windows 10 on Oracle VM VirtualBox on Oracle Solaris 11 running on a HP Model 20 with Intel Xeon E5-2670v3

The tested platform itself may be procured with a single processor or several different processors. As shown above, the processor(s) on which the module was tested on **shall** be listed on the CMVP certificate, Security Policy and test report.

Example: **Wind River Linux 6.0 running on a Xerox Explorer 60 with Intel Atom E3800**

SEPOS running on Apple TV 4K with Apple A10X Fusion

Tintri OS 4.5 running on a EC6030 with Intel Xeon E5-2609

If this field is not applicable, mark the field as N/A.

27. **PIV Certificate [#nnnn]** - When a module implements a validated PIV application, the application validation certificate type and number **shall** be included. Additional information

relating to PIV versioning can be found in the Management Manual Section 7.5 - *PIV References*.

28. **Validation Certificate –** blank unless the validation has been completed and assigned a certificate number.
29. **Revalidation Cert Number –** applicable for any revalidation submission.
30. **Special Instructions –** Special considerations for reviewer’s information.

Annex B CMVP Convention for Correspondence

This section is still in DRAFT

In order to accomplish uniformity and support CMVP communication and database automation, all FIPS 140-3 report transactions to the CMVP **shall** follow the conventions specified below.

Annex B.1 Acronyms

CST laboratory	Cryptographic and Security Testing Laboratory
CVC	Consolidated Validation Certificate
ITAR	International Traffic in Arms Reduction
IUT	Implementation Under Test
LC	Laboratory Code
NCR	NIST Cost Recovery
NECR	NIST Extended Cost Recovery
TID	Tracking IDentification

Annex B.2 e-mail Subject Line format:

TID-<**Field1**>-<**Field2**>-<**Field3**>-<**Field4**>-<**Field5**>-<**Field6**>-<**Field7**>-<**Field8**>

NOTE: All fields **shall** be delimited by hyphens "-"

The CRYPTIK tool, which is provided to the accredited CST Laboratories, includes an automated Email function that will generate the correct subject line syntax based on the selected options. This is found under ***FILE I/O and EMAIL***

Field1 – LC-nnnn **CST laboratory TID**

[2-digit LC]-[4-digit *alphanumeric* (A-Z, a-z, 0-9) assigned by the CST laboratory]

The 2-digit LC designations are as follows:

LC	CST Laboratory	LC	CST Laboratory
01	UL	18	DEKRA
02	CEAL	19	ITSC
03	~~DOMUS~~	20	~~CSC~~
04	COACT	21	~~UL~~
05	~~SAIC - VA~~	22	~~BAE Systems AI~~
06	EWA	23	~~CGI~~

07	~~LogicaCMG~~	24	BAH
08	~~BT~~	25	ADS
09	TÜViT	26	~~UL Transaction Security~~
10	~~Aspect~~	27	Penumbra
11	atsec	28	Gossamer
12	~~ICSA~~	29	Acumen Security
13	Leidos	30	Asia Pacific IT Lab, TUV Nord
14	~~ACTL~~	31	Serma
15	Ægisolve	32	Lightship Security
16	~~TTC~~	33	
17	ECSEC	34	Cyber Security Malaysia

Table 5 - Annex A. CST Laboratory Codes

Field2 – nnnn **CCCS TID**

[4-digit *numeric* (0-9) assigned by CCCS (0000 if not assigned)] *or* [ITAR (for ITAR reports not reviewed by CCCS)]

Field3 – nnnn **e-mail Transaction TAG**

[4-digit character email tag as defined below]

Pre-validation Activities:

IUTA[42] – Add report to IUT list

IUTB – Request an invoice from NIST for Cost Recovery before report submission

IUTC – Cancel a request for an invoice from NIST for Cost Recovery - only available if the invoice has not been paid

IUTR – Remove report from the IUT list

IUTM[3] – Modify an existing IUT entry

Report Submission (FIPS 140-3 Scenario: s = 1V1, 1OEA, 1VA, 1UP, 1AU, 1OEM, 1MU, 2SC, 3CVE, 3MC, 4PSC, 5FS):

XXXX[3] – Report Submission Scenario (see Section 4.4 for descriptions)

[42] **Shall** include file attachment

HLD	– Place report on HOLD
NSn[3]	– NIST comments
CSn[3]	– CCCS comments
CMn[3]	– CMVP comments or returned CST laboratory addressed comments
CRVn[3]	– CMVP (int) review w/ OK comments & draft certificate
NCRn[5]	– NIST (cert) review response to draft certificate
CCRn[5]	– CCCS (cert) review response to draft certificate
n=0	[if comments not sent to CST laboratory] **OR**
n=1+	[nth time CMVP comments sent to the CST laboratory]

Finalization Activities:

FAOK[3]	– All OK comments w/draft certificate for CST laboratory review and moves MIP reporting to Finalization
FCLC[43]	– CST laboratory review response to draft certificate
FRCN	– Request certificate number assignment
FVCN	– Assignment of validation certificate number
FWPH	– Posting of validation entry on NIST web site
FCVC[3]	– Consolidated Validation Certificate
FMOD[2]	– Modification of posted validation entry

Miscellaneous:

ASSG	– CCCS assigned TID
DRPT	– CST laboratory request to DROP report
RQFG	– CST laboratory request for guidance
ALOR	– Internal Assignment of NIST or CCCS report reviewer
STAT	– Query report status
OTHR	– Other

Billing:

NECN[44]	– NIST Extended Cost Recovery Notification to CST laboratory
NECR[6]	– NIST Extended Cost Recovery CST laboratory Response

Field4 – Vendor Name

[1 to10-digit *alphanumeric* characters maximum]

[43] May include an updated vendor.txt file where the only updates are for vendor contact information.

[44] **Shall** include file attachment

Field5 – Date of Transaction

[6-digit *numeric* date of transaction (format: yymmdd)]

Field6 – Vn Version Number

n [nth transaction]

Example: If a replacement for the same report is sent a 3rd time then Field6 = V3

Field7 – Certificate Number

[Newly Assigned Certificate Number (FVCN)], or MULT (if more than one certificate)

Field8 – Report Review or Draft Certificate Review Completed

[**OK –** NIST, CCCS or CST laboratory review completed with no further comments]

Note - If the OK is not included on the subject line, there will be another round of comments

TO: and CC: minimum requirements:

1. All transactions from a CST Lab to the CMVP **shall** be sent:

   TO: cmvp@nist.gov; cmvp@cyber.gc.ca

2. All transactions from CCCS to a CST Lab **shall** be sent:

   TO: <CST Lab>
   CC: cmvp@cyber.gc.ca; cmvp@nist.gov

3. All transactions from NIST CMVP to a CST Lab **shall** be sent:

   TO: <CST Lab>
   CC: cmvp@cyber.gc.ca

4. All transactions from CCCS to the NIST CMVP **shall** be sent:

   TO: cmvp@nist.gov
   CC: cmvp@cyber.gc.ca

5. All transactions from NIST CMVP to CCCS **shall** be sent:

   TO: cmvp@cyber.gc.ca

6. All ITAR transactions from a CST Lab to NIST CMVP **shall** be sent:

   TO: cmvpitar@nist.gov

7. All ITAR transactions from NIST CMVP to a CST Lab **shall** be sent:

   TO: <CST Lab>

Annex B.3 File attachment naming convention:

In order to maintain a correspondence between the submitted e-mail and the attachment for tracking purposes, only one attachment will be allowed per email transmittal. The **file attachment shall** be a Zip file. The entire e-mail attachment **shall** be encrypted with PGP. The Zip file **shall** contain one or more attachments. The names of the Zip file and all of the individual files **shall** have the exact same <ZIP FILE NAME>.

The files within the Zip files **shall** be named as follows:

1. *Security Policy*:

   s(scenario) = 1OEM, 3MC, or 5FS <ZIP FILE NAME>**_140sp.pdf**

   s = 1VI, 1OEA, 1VA, 1UP, 1AU, 2SC, 1MU, 3CVE and 4PSC[45]
   <ZIP FILE NAME>**_140sp**<CertNo>**.pdf**

   (one security policy for *each* certificate number referenced)

2. *CRYPTIK Assessment Reports*:

   s = 3MC <ZIP FILE NAME>**_report.pdf**

   Signed Signature Page || General Vendor/Module Information || Revalidation Report with Assessments (including list of changes) || Full Report || Physical Test Report (Section 4.5 Levels 2, 3 and 4)

   s = 4PSC <ZIP FILE NAME>**_report.pdf**

   Physical Test Report (Section 4.5 Levels 2, 3 and 4)

   s = 5FS <ZIP FILE NAME>**_report.pdf**

   Signed Signature Page || General Vendor/Module Information || Full Report with Assessments || Physical Test Report (Section 4.5 Levels 2, 3 and 4)

3. *CRYPTIK Vendor Text File*:

   s = *all* <ZIP FILE NAME>**_vendor.txt**[46]

4. *CRYPTIK Draft Certificate*:

   s = 1OEM, 3MC, or 5FS <ZIP FILE NAME>**_140crt.doc**

5. *CMVP Comments*:

   s = *all* <ZIP FILE NAME>.doc

[45] Only required if the modifications cause changes to the Security Policy.

[46] If **s = 1** and multiple module validations are referenced, the _vendor.txt **shall** represent the composite group. For example, the CRYPTIK module name field specified as "Multiple Acme Modules". Versioning, algorithms, module description, Certificate Caveat and other module specific fields in CRYPTIK should be marked NA. The CRYPTIK Reval Ref Certs field **shall** include all referenced module validations to be changed.

6. *Change Request Letter* [47]:

s = 1VI, 1OEA, 1VA, 1UP, 1AU, 2SC, 1MU, 3CVE and 4PSC

Non-image <ZIP FILE NAME>**_letter_unsigned.pdf**
Signed image <ZIP FILE NAME>**_letter_signed.pdf**

Current Cert. #1000	**Change Requested Cert. #1000**
Software Version 3.1	Software Versions 3.1 and 3.2
AES (Cert. #333); DSA (Cert. ~~#111~~)	AES (Cert**s**. #333 **and #555**); DSA (Cert. #**666**)
Acme ~~Incorporated, LTD~~	Acme **and Forrester Co.**
POC2 Name:	**Joe Diffie**
POC2 email:	**Joe.diffie@acmeforr.com**
Current Cert. #1050	**Change Requested Cert. #1050**
Acme ~~Incorporated, LTD~~	Acme **and Forrester Co.**

Table 6 - Annex A. Current vs. Change Table to be submitted with a change request

[47] The change request letter **shall** provide a "Current" verses "Change Requested" table representing the requested validation information changes for each certificate. The "Current" text for removal **shall** be marked as strike-through and the "Change Requested" or added text **shall** be hi-lighted and bolded as shown above.

Annex B.4 Submission Files sent between CST laboratory and CMVP

Submission Scenarios	CST laboratory to CMVP	File Content	CMVP to CST laboratory
5FS	_vendor.txt	Cryptik	
	_140sp.pdf	Security Policy	
	_report.pdf	Test Report	
	_140crt.doc, .docx, .rtf	Draft Certificate	doc, .docx, .rtf[48]
	.doc, .docx, .rtf[49]	CMVP Comments with CST laboratory Resolutions	doc, .docx, .rtf
4PSC	_vendor.txt	Cryptik	
	_letter_unsigned.pdf	Change Request Letter	
	_letter_signed.pdf	Change Request Letter – signed	
	_140sp<CertNo>.pdf	Security Policy[50]	
	_report.pdf	Test Report[51]	
	.doc, docx, .rtf[1]	CMVP Comments with CST laboratory Resolutions	.doc, .docx, .rtf
3MC, 1MU	_vendor.txt	Cryptik	
	_140sp.pdf	Security Policy	
	_report.pdf	Test Report	
	_140crt.doc, docx, .rtf	Draft Certificate	doc, .docx,. rtf[2]

[48] The draft certificate is sent when in FINALIZATION.

[49] The CMVP Comments file is not included with the initial submission.

[50] The Security Policy is required if the modifications cause changes to the Security Poliy.

[51] Physical Security Test Report.

	doc, .docx, .rtf[1]	CMVP Comments with CST laboratory Resolutions	.doc, .docx, .rtf
3CVE	_vendor.txt	Cryptik	
	_140sp.pdf	Security Policy	
	_report.pdf	Test Report	
	_140crt.doc, docx, .rtf	Draft Certificate	doc, .docx,. rtf[2]
	doc, .docx, .rtf[1]	CMVP Comments with CST laboratory Resolutions	.doc, .docx, .rtf
	_letter_unsigned.pdf	Change Request Letter	
	_letter_signed.pdf	Change Request Letter – signed	
1OEA, 1VA, 1AU, or 1OEM	_vendor.txt	Cryptik	
	_letter_unsigned.pdf	Change Request Letter	
	_letter_signed.pdf	Change Request Letter – signed	
	_140sp.pdf	Security Policy for 1A or 1B	
	_140sp<CertNo>.pdf	Security Policy[3]	
	_140cert.doc, .docx, .rtf	Draft Certificate for 1OEM	doc, .docx, .rtf[52]
	.doc, .docx, .rtf[1]	CMVP comments with CST laboratory resolutions	.doc, .docx, .rtf

Table 7 - Annex A. Submission files to be included

Based on the above field descriptions, some example ***subject line*** formats would be:

[52] The draft certificate is sent when in FINALIZATION.

Annex B.5 Report Submission Examples

Example 1: TID-06-0001-0000-**1MU**-Motorola_S-100802-V1

Lab assigned TID number of 06-0001, CCCS TID number not yet assigned, submitted by EWA – revalidation report submission under Scenario 1 - vendor Motorola Solutions, Inc. – sent on August 02, 2010 and version 1

Example 2: TID-16-0001-0000-**1MU**-Motorola_S-100921-V1

Lab assigned TID number of 16-0001, CCCS TID number not yet assigned, submitted by TTC – revalidation report submission under Scenario 1 - vendor Motorola Solutions, Inc. – sent on September 21, 2010 and version 1

Example 3: TID-06-0001-0000-**3MC**-IBM_Corpor-080802-V1-1024

Lab assigned TID number of 06-0001, CCCS TID number not yet assigned, submitted by EWA – revalidation report submission under Scenario 3 - vendor IBM Corporation – sent on August 02, 2008 and Cert. #1024 is the revalidation reference certificate number

Example 4: TID-03-0003-0000-**5FS**-Entrust_In-081031-V1

Lab assigned TID number of 03-0003, CCCS assigned TID number not yet assigned, submitted by DOMUS – full report submission under Scenario 5 - vendor Entrust, Inc. – sent on October 31, 2008 and version 1

Example 5: TID-03-0003-0023-**HLD**-Entrust_In-081115-V1

Lab assigned TID number of 03-0003, CCCS assigned TID number of 0023, submitted by DOMUS – request report submission under Scenario 5 to be put on HOLD - vendor Entrust, Inc. – sent on November 15, 2008 and version 1

Example 6: TID-03-0003-0023-**5FS**-Entrust_In-090118-V2

Lab assigned TID number of 03-0003, CCCS assigned TID number of 0023, submitted by DOMUS – full replacement report submission under Scenario 5 - vendor Entrust, Inc. – sent on January 18, 2009 and version 2

Annex B.6 Typical COORDINATION set of comment rounds

First set of CMVP comments sent to the CST laboratory:

Example 7a: TID-05-0004-0024-CM1-Cisco_Syst-100115-V1-1024

Lab assigned TID number 05-0004, CCCS assigned TID number of 0024, submitted by Atlan – revalidation submission under Scenario 3 – 1st set of CMVP comments - vendor Cisco Systems, Inc. – sent on January 15, 2010, version 1 and Cert. #1024 is the revalidation reference certificate number

CST laboratory returns responses to the first set of CMVP comments a few days later:

Example 7b: TID-05-0004-0024-3CM1-Cisco_Syst-100121-V1-1024

Lab assigned TID number 05-0004, CCCS assigned TID number of 0024, submitted by SAIC - revalidation submission under Scenario 3 – 1st set of CST laboratory response comments - vendor Cisco Systems, Inc. – sent on January 21, 2010, version 1 and Cert. #1024 is the revalidation reference certificate number

Second set of CMVP comments sent to the CST laboratory:

Example 7c: TID-05-0004-0024-3CM2-Cisco_Syst-100123-V1-1024

Lab assigned TID number 05-0004, CCCS assigned TID number of 0024, submitted by SAIC – revalidation submission under Scenario 3 – 2nd set of CMVP comments - vendor Cisco Systems, Inc. – sent on January 23, 2010, version 1 and Cert. #1024 is the revalidation reference certificate number

CST laboratory returns responses to the second set of CMVP comments on same day:

Example 7d: TID-05-0004-0024-3CM2-Cisco_Syst-100123-V2-1024

Lab assigned TID number 05-0004, CCCS assigned TID number of 0024, submitted by SAIC - revalidation submission under Scenario 3 – 2nd set of CST laboratory response comments - vendor Cisco Systems, Inc. – sent on January 23, 2010, version 2 and Cert. #1024 is the revalidation reference certificate number

Example 8: TID-04-0005-**ITAR**-NS1-Attachmate-080520-V1

Lab assigned TID number 04-0005, ITAR report, submitted by COACT - report submission under Scenario 5 - NIST only comments - vendor Attachmate – sent on May 20, 2008, version 1 – NIST comments

Example 9: TID-04-0005-2012-**5CM1**-Attachmate-080520-V1

Lab assigned TID number 04-0005, CCCS assigned TID number of 2012, submitted by COACT - report submission under Scenario 5 – CST laboratory responses to CMVP comments - vendor Attachmate – sent on May 20, 2008, version 1

Example 10a: TID-04-0005-2012-**FAOK**-Attachmate-120520-V1

Lab assigned TID number 04-0005, CCCS assigned TID number of 2012, submitted by COACT - report submission under Scenario 3 or 5 - CMVP Final All OK comments to the CST laboratory - vendor Attachmate – sent on May 20, 2012, version 1

If the **FAOK** is sent a 2nd time (or more) due to changes, then the new transaction version would be V2 (or incremented +1 for each new transmission).

Example 10b: TID-04-0005-**ITAR**-FAOK-Attachmate-080520-V1

Lab assigned TID number 04-0005, ITAR report, submitted by COACT - report submission under Scenario 3 or 5 – NIST-only Final All OK comments to the CST laboratory - vendor Attachmate – sent on May 20, 2008, version 1

Example 11: TID-12-3555-**RQFG**-090510

Since a request for guidance is more general in nature, only the following fields are required in the **subject line**: TID-**Field1**-**Field3**-**Field5**

Lab assigned TID number 3555, CCCS assigned TID number of 3555, submitted by ICSA, sent on May 10, 2009

Example 12: TID-**FCVC**-120520-V1

Sending Consolidated Validation Certificate to CCCS for signature

Example 13: TID-04-0005-2012-**FWPH**-Attachmate-120520-V1

The validation entry for Cert. #nnnn will be posted on the NIST CMVP web site.

Example 14: TID-04-0005-2012-**FCLC**-Attachmate-120520-V1-OK

The CST lab has reviewed the final draft certificate and found it OK to proceed with validation.

Example 15: TID-04-0005-2012-**FMOD**-Attachmate-120520-V1

The validation entry for Cert. #nnnn has … *or*

The validation entries for Certs. #nnnn, #nnnn and #nnnn have …

been modified and the NIST CMVP web site will be posted

Example 16: TID-04-0005-2012-**ALOR**-Attachmate-120520-V1

The subject report has been assigned to you.

Example 17: TID-04-0005-2012-**STAT**-Attachmate-120520-V1

Please provide status for this report

Example 18: TID-04-0005-**NECN**-Attachmate-120520-V1

NIST CMVP sent to CST Lab:

Please see attachment notification for verification of NIST Extended Cost Recovery.

Example 19: TID-01-2078-0000-**IUTB**-Thales_e-S-160510

Request for NIST to send an invoice to the lab before the lab submits the test report/submission package.

Example 20: TID-01-2078-0000-**IUTC**-Thales_e-S-160511

Request to cancel an unpaid invoice. Only unpaid invoices can be cancelled.

Example 21: TID-23-0005-0000-**IUTA**- Attachmate-110531-V1

IUT Add request: Lab assigned TID number 23-0005, CCCS TID number not yet assigned, submitted by CGI – IUT Add Request, vendor Attachmate – sent on May 31, 2011, version 1
The attached Zip file would include the _vendor.txt file

Example 22: TID-23-0006-0000-**IUTR**-Cisco_Syst-150203-V1

Lab assigned TID number 23-0006, CCCS TID number not yet assigned, submitted by CGI – IUT Remove Request, Vendor Cisco Systems, Inc. - Sent on February 3, 2015. Version 1.

Example 23: TID-04-0006-0000-**IUTM**-Cisco_Syst-150204-V1

Lab assigned TID number 04-0006, CCCS TID number not yet assigned, submitted by COACT – IUT Modify Request, Vendor Cisco Systems, Inc. - Sent on February 4, 2015, Version 1

The attached Zip file would include the _vendor.txt file

Annex B.7 File attachment examples

The attached file names would be named as follows:

TID-23-0005-0000-**IUTA**-Attachmate-110531-V1.zip

TID-16-0001-0000-**1VI**-Motorola-100802-V1**.**zip

TID-05-0004-0024-**CM2**-Cisco-100123-V2-1024.zip

TID-04-0005-**ITAR**-**NS1**-Attachmate-080520-V1.zip

TID-12-3555-**RQFG**-090510.zip

Annex C CMVP Validation Issue Assessment Process

Annex C.1 Addressing Security Relevant Issues

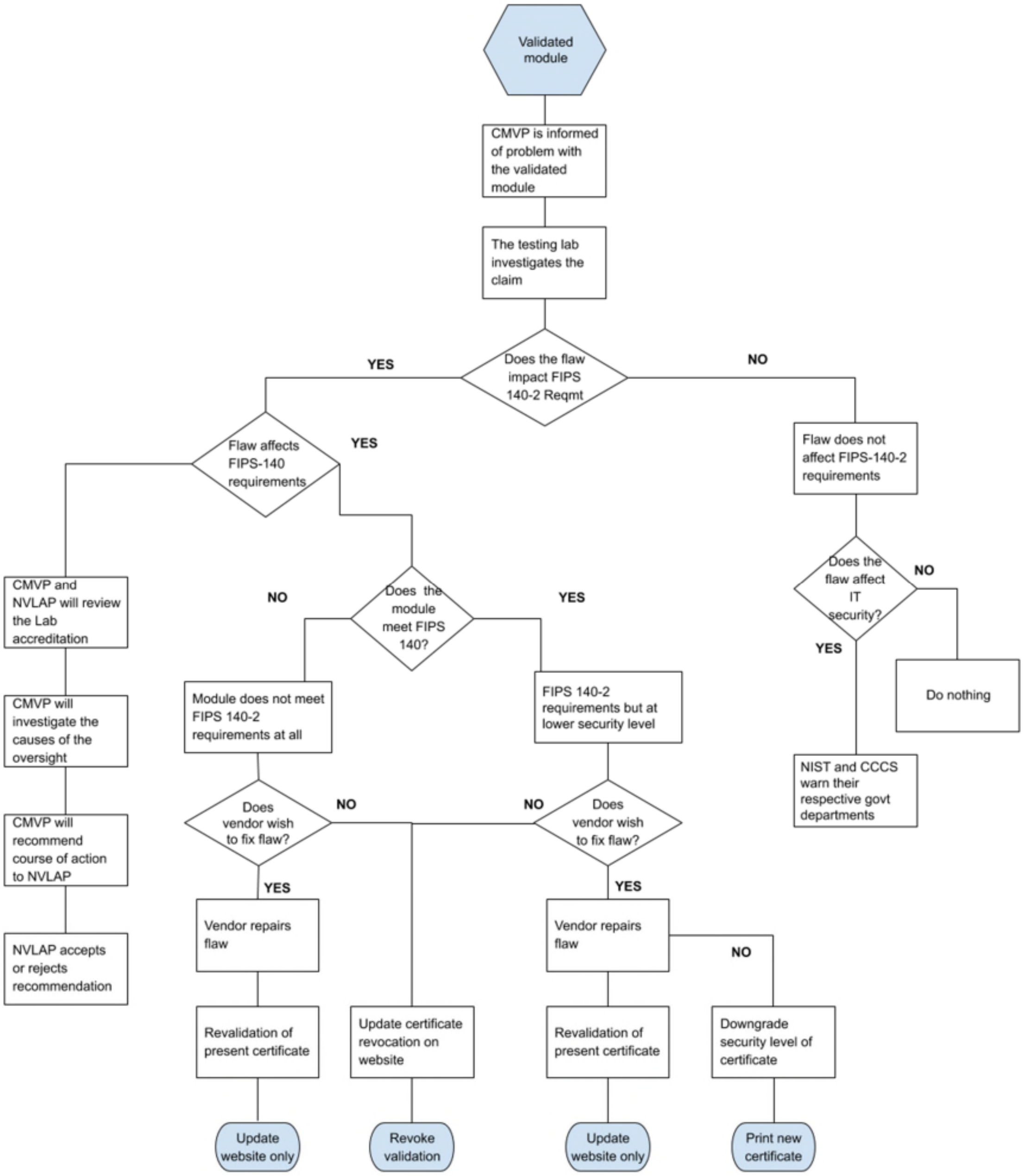
Validated module
CMVP is informed of problem with the validated module
The testing lab investigates the claim
Does the flaw impact FIPS 140-2 Reqmt
YES
NO
Flaw affects FIPS-140 requirements
YES
Flaw does not affect FIPS-140-2 requirements
CMVP and NVLAP will review the Lab accreditation
NO
Does the module meet FIPS 140?
YES
Does the flaw affect IT security?
NO
YES
CMVP will investigate the causes of the oversight
Module does not meet FIPS 140-2 requirements at all
FIPS 140-2 requirements but at lower security level
Do nothing
NIST and CCCS warn their respective govt departments
CMVP will recommend course of action to NVLAP
Does vendor wish to fix flaw?
NO
NO
Does vendor wish to fix flaw?
YES
YES
NVLAP accepts or rejects recommendation
Vendor repairs flaw
Vendor repairs flaw
NO
Revalidation of present certificate
Update certificate revocation on website
Revalidation of present certificate
Downgrade security level of certificate
Update website only
Revoke validation
Update website only
Print new certificate

Figure 4 – Annex B. Validation Issue Assessment Process

Annex C.2 Addressing CVE Relevant Vulnerabilities

The list of CVEs (Common Vulnerability and Exposures) are maintained by NIST in the National Vulnerability Database (NVD) at https://nvd.nist.gov/. The purpose of the Scenario 1CVE revalidation (described in the paragraph 4.4) 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 standard.

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/.

ACRONYMS

ACVP	Automated Cryptographic Validation Program
AES	Advanced Encryption Standard
AESAVS	Advanced Encryption Standard Algorithm Validation System
ANSI	American National Standards Institute
APLAC	Asia Pacific Laboratory Accreditation Cooperation
AS	Assertion
CAN-P	Canadian Publication
CAPS	Communications-Electronics Security Group Assisted Products Scheme
CAVP	Cryptographic Algorithm Validation Program
CAVS	Cryptographic Algorithm Validation System
CBC	Cipher Block Chaining
CC	Common Criteria
CCM	Counter with Cipher Block Chaining-Message Authentication Code
CCVMS	Counter with Cipher Block Chaining-Message Authentication Code Validation System
CCCS	Canadian Centre for CyberSecurity
Cert	Certificate
CESG	Communications-Electronics Security Group
CMVP	Cryptographic Module Validation Program
CST	Cryptographic and Security Testing
CTCPEC	Canadian Trusted Computer Product Evaluation Criteria
DES	Data Encryption Standard
DOC	Word document
DSA	Digital Signature Algorithm
DSAVS	Digital Signature Algorithm System
DTR	Derived Test Requirements
EA	European cooperation of Accreditation
EAL2	Evaluation Assurance Level 2
ECB	Electronic Code Book
ECDSA	Elliptic Curve Digital Signature Algorithm
ECDSAVS	Elliptic Curve Digital Signature Algorithm Validation System

FAQ	Frequently Asked Questions
FAX	Facsimile
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FSM	Finite State Model
GC	Government of Canada
GPC	General Purpose Computer
HB	Handbook
HMAC	Keyed-Hash Authentication Code
HMACVS	Keyed-Hash Message Authentication Code Validation System
IAAC	InterAmerican Accreditation Cooperation
IAF	International Accreditation Forum
ID	Identification
IG	Implementation Guidance
ILAC	International Laboratory Accreditation Cooperation
ISO	International Organization for Standardization
ITAR	International Traffic in Arms Regulation
ITSEC	Information Technology Security Evaluation Criteria
ITSET	Information Technology Security Evaluation and Test
IUT	Implementation Under Test
MAC	Message Authentication Code
MD5	Message Digest 5
MLA	Multilateral Recognition Arrangement
MMT	Multi-block Message Test
MOU	Memorandum of Understanding
MRA	Mutual Recognition Arrangement
N/A	Not Applicable
NACLA	National Cooperation for Laboratory Accreditation
NDA	Non-Disclosure Agreement
NIST	National Institute of Standards and Technology
NSTISSP	National Security Telecommunications and Information Systems Security Policy
NVLAP	National Voluntary Laboratory Accreditation Program

OS	Operating System
PALCAN	Program for the Accreditation of Laboratories – Canada
PDF	Portable Document Format
PKCS	Public Key Cryptography Standard
PP	Protection Profile
PUB	Publication
RC4	Rivest Cipher 4
RFG	Request for Guidance
RNG	Random Number Generator
RNGVS	Random Number Generator Validation System
RSA	Rivest Shamir Adleman Cryptographic System
RTF	Rich Text Format
SBU	Sensitive But Unclassified
SHA	Secure Hash Algorithm
SHAVS	Secure Hash Algorithm Validation System
SHS	Secure Hash Standard
SoC	Secretary of Commerce
SP	Special Publication
TCSE	Trusted Computer Systems Evaluation Criteria
TDES	Triple Data Encryption Standard
TID	Tracking Identification Number
TM	Trademark
URL	Uniform Resource Locator