FIPS 140-2
Cryptographic Module Validation Program Management Manual

(Date 9/9/2021)

Version 1.5

National Institute of Standards and Technology and
Canadian Centre for CyberSecurity

Revision History

Version	Date	Comment
1.0	15 April 2009	Initial publication of the CMVP Management Manual
1.1	05 Jun 2014	Updated NIST CMVP Fee information
1.2	28 Oct 2016	Updated document
1.3	7 Mar 2017	Updated NIST CMVP Fee information, coordination deadline, added validation deadline
1.4	20 May 2020	Major revision
1.5	9 Sep 2021	Adds entropy submissions, updated submission files, and RFG formatting

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 Authorities, 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.

1.5 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.

Note: As of September 22, 2026, all FIPS 140-2 validated module will move to the historical list. No new systems should consider the use of validated modules on the historical list.

1.6 CMVP Management Manual Structure

This manual is organized into the following sections:

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

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

Section 3 – 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.

1.7 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 encompassing security and testing requirements that must be satisfied by a cryptographic module. CMVP also works with NVLAP to address CST accreditation requirements. These documents are identified below.

1.7.1 FIPS 140-2

FIPS 140-2 (2001) supersedes FIPS 140-1. The 11 areas of requirements are: cryptographic module specification; cryptographic module ports and interfaces; roles, services, and authentication; finite state model; physical security; operation environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks.

The document is available on-line on the official Cryptographic Module Validation Program website at https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Standards.

1.7.2 Derived Test Requirements

The Derived Test Requirements (DTR) describes the methods that are to be used by accredited CST laboratories to test the conformance of a cryptographic module to the requirements of FIPS 140-2. 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.

The DTR contains the security requirements from FIPS 140-2, 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 FIPS 140-2. 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 supplied as results of the required tests performed 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.

The document is available on-line on the official Cryptographic Module Validation Program website at https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Standards.

1.7.3 Implementation Guidance

Implementation Guidance is issued to provide clarification and guidance with respect to a particular assertion or group of assertions found in FIPS 140-2 and the DTR. 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/Standards.

1.7.4 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 (2016), *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.

1.7.5 Other Documents on the CMVP Website

The CMVP website contains 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 cryptographic modules validated to FIPS 140-1 and FIPS 140-2.

5. Modules in Process (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 under FIPS 140-2 where the test report has been submitted to the CMVP for validation. (The listing is voluntary where vendors may choose to have their module included on this list). For more information regarding a specific module, please contact the vendor.

6. Implementation Under Test (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 under FIPS 140-2 but have not yet been submitted to the CMVP. (The listing is voluntary where vendors may choose to have their module included on this list.) The CMVP does not have information regarding the status of these modules or whether a test report will be submitted to the CMVP. 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.

2 Program Management

2.1 Introduction

The purpose of this section is to describe the overarching 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 testing to FIPS 140-2, 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:

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 and CAVP

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 FIPS 140-2 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 carbon copied. 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 a FIPS 140-2 test 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. If the request is related to an existing report in the CMVP queue, please submit this request using the email subject line outlined in the CMVP Management Manual, Annex B which includes the TID number.

If the RQFG is not related to an existing report in the queue, please use:

<Lab code>-FIPS 140-2 RQFG-<submission date>

as the email subject line. These questions must be submitted to all points of contact.

2.4.1 Format for Request for Guidance

A Request for Guidance will result in a response from the CMVP that will state current policy or interpretations. This format provides the CMVP a clear understanding of the question. Preferably, questions should be non-proprietary, as their response may be distributed to ALL CST laboratories. Distribution may be restricted on a case-by-case basis. 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 FIPS 140-2,

4. Applicable assertion(s) from the FIPS 140-2 DTR,

5. Applicable required test procedure(s) from the FIPS 140-2 DTR,

6. Applicable statements from FIPS 140-2 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 FIPS 140-2 target security level. All of this will enable a more efficient and timely resolution of FIPS 140 related questions 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 or the IGs. Note that general questions may still be submitted, but these questions should be identified as not being associated with a particular validation effort.

2.4.2 Informal Request

Informal requests are considered as ad hoc questions aimed at clarifying issues about the FIPS 140-2 and other aspects of the CMVP and CAVP. 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. The submission should follow the format outlined in 2.4.1

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

2.4.3 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 in 2.4.1. 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.

2.4.4 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 of FIPS 140-2 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 non-proprietary and not prevent further distribution by the CMVP.

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

Following its review of the official request regarding the module, the CSTL will state its position on whether the official request:

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

The CMVP will review the CSTLs 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 below in ANNEX B: CMVP Validation Issue Assessment Process for the flow diagram for 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 Roles, Responsibilities, and Output in the CMVP Process

below.

Who	Vendor	CSTL	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 FIPS (e.g. FIPS 140-2) and NIST Special Publications. Amongst 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 laboratory 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 different module which is not validated and therefore a new validation or revalidation effort would need to be on the updated 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. The requirements levied on the cryptographic module are specified in FIPS 140 and tested in accordance with the DTR 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 FIPS 140, the Derived Test Requirements, 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, User Guidance and Crypto Officer 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 consolidate or reformat 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 as required by IG G.9. 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 with FIPS 140-2, 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 review of the management system manual, conducting of the proficiency exam, on-site assessment and 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 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 validated version number of a cryptographic module is also specified on the *Validated FIPS 140 Cryptographic Modules* list 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 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:

- CMVP team status
- 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 NIST, CCCS, a CST laboratory's accreditation, vendor, or the program.

As required by the CST laboratory accreditation standards listed in Handbook 150-17 Section 4.2, 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 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 and Risk Mitigation 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 Process

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 (2016) 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: CST Laboratory Accreditation Process. All steps in the accreditation process are sequential and must be completed in the order shown.

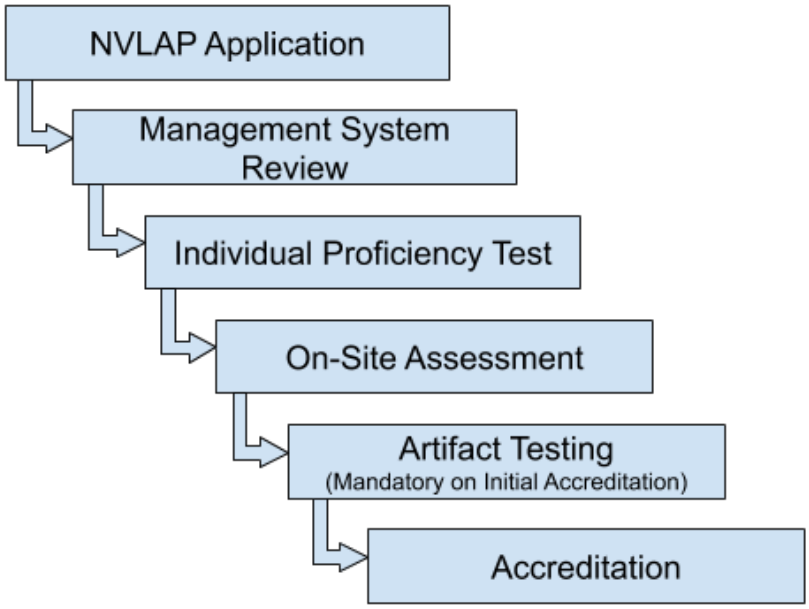

Figure 2 CST Laboratory Accreditation Process

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 manual to NVLAP prior to the assessment process. Upon notification by NVLAP of an acceptable application, an assessment team is selected. This team is typically comprised of one or more technical assessors 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

A CST Proficiency Examination will be administered to the applicant laboratory's testing and signatory personnel. The written examination consists of questions relating to various aspects of CST laboratory activities, FIPS 140, 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
  - Programmatic guidance and specifically 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
  - Single operator mode
  - 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
  - Default Entry Point (DEP)
  - 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
  - Level 3 and above 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
  - EMI/EMC
  - Ports and Interfaces
  - Design Assurance – Security Levels 1to 4

The exam is graded by the third-party testing organization, and the results are provided to the CMVP. Testers are required to pass the CVP Certified Tester exam with 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 reduced to account for new technical requirements.

Each CST laboratory shall retain a minimum of two CVP certified tests to maintain laboratory accreditation. All signatories of validation submissions must be CVP certified.

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 to NVLAP concerning resolution of deficiencies within thirty days of notification.

3.1.2.5 Artifact Testing (Mandatory for initial accreditation)

Following the on-site assessment, the assessment team will leave 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 of application. Once completed, the applicant laboratory must submit the test report to the assessment team for their review. The team will then assess the competency of the laboratory using the responses provided in the test report.

3.1.2.6 Accreditation Decision

The assessment team 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

The renewal period is one year after initial accreditation and two years thereafter. 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 initial 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 CRYPTIK. The CMVP and CAVP will also issue the latest programmatic directives and policies, and internal guidance and documentation, including use of CAVP ACVTS.

3.1.2.9 Cryptographic Testing Program Cooperative Research and Development Agreement (CRADA)

All accredited CST Laboratories must have an executed 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 from October 1, 2021 to October 30, 2026 unless modified. The agreement is reviewed and revised as needed. 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 still 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 3.2 of NIST Handbook 150. The re-accreditation process is the same as illustrated in Figure 2 CST Laboratory Accreditation Process and described above in Section 3.1.2. 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 that a CST laboratory changes ownership, the accreditation body and the CMVP Validation Authorities must be informed within thirty working days in accordance with Annex C of the NVLAP Handbook 150 (2016) of the identity of the new owner of the laboratory and the effective date of the change.

3.2.4 Relocation of a CST Laboratory

In the event that 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 will conduct a monitoring visit after the relocation is completed to ensure all accreditation requirements continue to be met. The laboratory must also submit an update to the Quality Manual to NVLAP showing the new location information.

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 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 FIPS 140-2 testing will be suspended until a remediation plan is approved and executed.

ECR points are levied as follows:

0 points - Excessive number of modules in one report

1 point - Scenarios 1, 2, and 4 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 its 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), 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.

4.1.1 General Overview

Figure 3 Cryptographic Module Testing and Validation Process shows the general flow of testing and validation of a cryptographic module to the FIPS 140-2 standard.

NO
NO

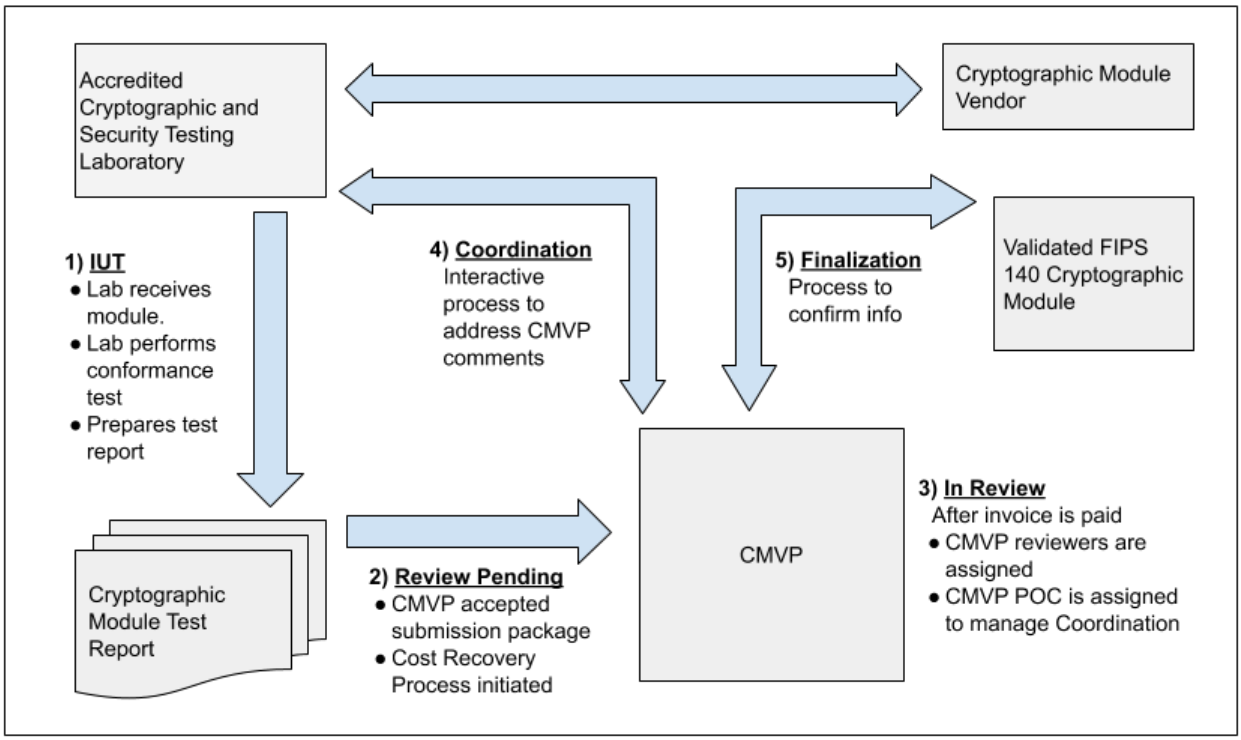

Figure 3 Cryptographic Module Testing and Validation Process

The steps for the cryptographic module validation life cycle include:

Step 1. **IUT** Accredited CST laboratory receives the cryptographic module for testing as part of a contractual agreement with the vendor. Cryptographic module validation testing is performed using the Derived Test Requirements (DTR) for FIPS 140-2, *Security Requirements for Cryptographic Modules*. 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 the *Implementation Guidance for FIPS 140-2 and the Cryptographic Module Validation Program G.1*. Once all the testing requirements have been completed, a

validation submission is prepared.

Step 2. **Review Pending** CMVP accepts the validation submission from the CST laboratory. NIST initiates Cost Recovery process.

Step 3. **In Review** After cost recovery is paid, 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.

Step 4. **Coordination** The coordination process begins with CMVP submitting comments to the CST laboratory and will continue until all comments and/or questions have been satisfactorily addressed.

Step 5. **Finalization** CMVP will perform a final review and confirm the lab has no additional changes. The validation information is posted to the *Validated FIPS 140 Cryptographic Module 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 an accredited CST laboratory (Step 1) to perform the FIPS 140-2 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 may notify 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 whether this information is to appear in the *IUT list*.

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, FIPS 140-2, *Security Requirements for Cryptographic Modules* remain the definitive reference for whether or not the cryptographic module meets the requirements of the standard. The 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 (see section 2.4) from CCCS and NIST in determining how to apply the FIPS 140 standard to the particular

cryptographic module.

The FIPS 140-2 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 (Step 1a). Section 4.3: Preparation and Submission of the Validation Submission describes what must be submitted by the laboratory for the FIPS 140-2 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 via email. 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 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

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 NIST and CCCS, as the Validation Authorities, issue a certificate number which is added to the database, along with the validation information. Each entry includes the version number of the validated cryptographic module and benchmark configuration of the original validation testing. Instructions for completing a FIPS 140 validation certificate are found at *Implementation Guidance for FIPS 140-2 and the Cryptographic Module Validation Program G.13.* The web-based search tool for the database can be found at https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules/Search.

At the end of each month, the Validation Authorities sign a consolidated validation certificate which lists all modules that were validated during the month.

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. As described in the

Implementation Guidance for FIPS 140-2 and the Cryptographic Module Validation Program G.8, 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 FIPS 140-2 Implementation Under Test (IUT) and Modules In Process (MIP) Lists* are provided for information purposes only. Participation on the IUT 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 choose not to list the module on the MIP list, the module will be anonymously reflected at the end of the list in the "Not Displayed" row. Posting on either 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 sections describe the requirements or activities that take place during each stage of the FIPS 140-2 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 other information (see IG G.2).
    - 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.
   - Testing documents updated based on resolutions and submitted to NIST and CCCS.
   - 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 FIPS 140-2 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 to the web site: 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 policy statements have been excerpted from the *Implementation Guidance for FIPS 140-2 and the Cryptographic Module Validation Program* G.2.

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 A**: *CMVP Convention for E-mail 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. For additional information or requirements, please refer to the FIPS 140-2 DTR and IG 14.1.
2. **CRYPTIK v9.0c (or higher) reports in PDF**. 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

4.4 Validation Submission Queue Processing

4.4.1 Initial Validation

No full validation or re validation submission (Scenario 5 and 3 under FIPS 140-2 IG G.8) will be accepted after Sept 22, 2021 unless lab was contracted prior to June 14, 2021 and CMVP has approved the petition for late submission. All full validations and re-validations must be submitted on or before March 31, 2022. Modules submitted for initial validation will be queued and addressed on a first-come, first-served 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.

4.4.2 Non-security Relevant Re-validation

Non-security relevant change letters as described in the Implementation Guidance for FIPS 140-

2 and the Cryptographic Module Validation Program G.8 will be handled upon receipt.

4.4.3 HOLD Status for Cryptographic Modules on the Modules In Process List

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. If prepayment is made in accordance with IG G.16, and the test report is not received within 90 days, the module will be moved to on HOLD and removed from the IUT list.
5. 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.
6. 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 and the ECR is paid, 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.

4.4.4 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, per IG G.16. 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 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).

4.5.1 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.

4.5.1.1 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 FIPS 140-2 IG 1.4, 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.
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

---

[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.

marked as: Not Applicable – ITAR.

c. The NIST CMVP web page will only post the following information: Certificate number, Vendor (null), Cryptographic Module (validated to FIPS 140-2), Module Type, Validation Date, and Level/Description.

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 under the *Implementation Guidance for FIPS 140-2 and the Cryptographic Module Validation Program G.8* 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 requirements stated in *the Implementation Guidance for FIPS 140-2 and the Cryptographic Module Validation Program G.8*.

4.6 NIST Cost Recovery[2]

The NIST CMVP fee schedule is published under **CMVP Notices** at

https://csrc.nist.gov/Projects/cryptographic-module-validation-program/nist-cost-recovery-fees.

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.

4.6.1 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 change scenarios under FIPS 140-2 IG G.8. 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/nist-cost-recovery-fees 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

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

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 a failure to follow correct process can cause a significant effort by CMVP to identify and work with the CST laboratory to discover and correct; ECR is likely to 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 FIPS 140-2 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.

4.6.2 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 (see IG G.16), 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.

For questions about methods of payments and associated handling fees contact NIST Billing Information: 301-975-3880.

4.7 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 for the validation in the *FIPS 140-1 and FIPS 140-2 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 *FIPS 140 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 140-2 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 FIPS 140-2 Cryptographic Module Validation Lists

The official CMVP website can generate the following lists related to the validation of cryptographic modules to FIPS 140-2:

- *FIPS 140-2 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 FIPS approved algorithms list (e.g. due to algorithm transitions); and
  - certificates older than 5 years.
- *FIPS 140-2 Modules In Process*
- *FIPS 140-2 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 on the CAVP website for those wishing to know more details of the specific testing performed.

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 FIPS 140-2 Cryptographic Module Validation List

This list is updated when new FIPS 140-2 validation certificates are posted to the web site for a cryptographic module or group of cryptographic modules, when FIPS 140-2 validations are extended to new versions of the cryptographic module through a letter re-validation request as described in the *Implementation Guidance for FIPS 140-2 and the Cryptographic Module Validation Program G.8* or when a change is requested in the web entry information such as the Point of Contact or the Vendor's Name.

4.12.2 FIPS 140-2 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 140-2 Logos

Information about the use of FIPS 140-2 logo and phrases is available from the CMVP web site: https://csrc.nist.gov/Projects/cryptographic-module-validation-program/use-of-fips-140-2-logo-and-phrases. Completed forms are sent to cmvp@nist.gov. If approved, NIST CMVP will send the artwork to the requestor.

5 CMVP and CAVP programmatic metrics collection

Programmatic Metrics is not currently being collected for FIPS 140-2 program.

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 140-2 Publication (and subsequent Publications)

FIPS 140-2 defines the security requirements for cryptographic modules and covers 11 areas related to their design and implementation. As with all FIPS publications, the FIPS 140 series is subject to periodic review and updates as necessary. The publication is ratified by the U.S. Secretary of Commerce.

Responsible Positions: CMVP Validation Authorities.

6.2 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.

6.3 Derived Test Requirements

The Derived Test Requirements for a particular FIPS 140-*x* publication are developed at the same time as requirements are added and/or revised for the new version of FIPS 140-*x*. This development is done by the CMVP Validation Authorities with input from the CST laboratories.

Responsible Positions: NIST CMVP and CCCS CMVP Program Managers.

6.4 Implementation Guidance

The IG is updated on a quarterly basis

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.

6.5 Programmatic Transitions for the CMVP

The programmatic transition webpage lists dates for transitions to algorithm testing and acceptance for incorporation into modules. This webpage is available at: https://csrc.nist.gov/Projects/cryptographic-module-validation-program/programmatic-transitions . Current and historical information is provided.

Responsible Position: NIST CAVP, NIST CMVP and CCCS CMVP Program Managers.

6.6 CST Laboratory Accreditation Standards

6.6.1 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 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.

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.

Responsible Position: Chief of NVLAP.

6.6.2 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, Information Technology Security Testing (Common Criteria; Cryptographic Security; Healthcare IT).

6.6.3 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 Test Tools

CST Labs are required to use the CMVP provided tools listed below. In order to aid the Lab in their testing a list of suggested tools is also provided.

7.1 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.

7.2 Suggested Tools for Laboratory 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)

Level 4 equipment:

Variable Power Supply
Digital Storage Oscilloscope
Formal Model Text
Temperature Chamber

Annex A CMVP Convention for Programmatic Correspondence

In order to accomplish uniformity and support CMVP e-mail and database automation, all e-mail report transactions to the CMVP **shall** follow the conventions specified below.

Annex A.1 Acronyms

CSTL	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 A.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 **CSTL TID**

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

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 2 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[3] – 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

[3] **Shall** include file attachment

Report Submission (FIPS 140-2 IG G.8 Scenario: s = 1[4], 3[5][6], 4 or 5[7]):

sSUB[3] – Report Submission (FIPS 140-2 IG G.2)

sHLD – Place report on HOLD

sNSn[3] – NIST comments

sCSn[3] – CCCS comments

sCMn[3] – CMVP comments or returned CSTL addressed comments

CRVn[3] – CMVP (int) review w/ OK comments & draft certificate

NCRn[6] – NIST (cert) review response to draft certificate

CCRn[6] – CCCS (cert) review response to draft certificate

n=0 [if comments not sent to CSTL] **OR**

n=1+ [nth time CMVP comments sent to the CSTL]

Finalization Activities:

FAOK[3] – All OK comments w/draft certificate for CSTL review and moves MIP reporting to Finalization

FCLC[8] – CSTL 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[3] – Modification of posted validation entry

Miscellaneous:

ASSG – CCCS assigned TID

DRPT – CSTL request to DROP report

RQFG – CSTL request for guidance

ALOR – Internal Assignment of NIST or CCCS report reviewer

---

[4] If the revalidation is a combination of a 1SUB and a 4SUB, the higher number always takes precedent in the submission designation. In this case it would be a 4SUB.

[5] A scenario 3A or 3B submission is submitted as a 3SUB

[6] No re validation submission (Scenario 3 under FIPS 140-2 IG G.8) will be accepted after Sept 22, 2021 unless lab was contracted prior to June 14, 2021 and CMVP has approved the petition for late submission. All Full Validations and Re-Validations must be submitted on or before March 31, 2022.

[7] No full validation submission (Scenario 5 under FIPS 140-2 IG G.8) will be accepted after Sept 22, 2021 unless lab was contracted prior to June 14, 2021 and CMVP has approved the petition for late submission. All Full Validations and Re-Validations must be submitted on or before March 31, 2022.

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

STAT – Query report status

OTHR – Other

Billing:

NECN – NIST Extended Cost Recovery Notification to CSTL

NECR[9] – NIST Extended Cost Recovery CSTL Response

Field4 – Vendor Name

[1 to10-digit *alphanumeric* characters maximum]

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 CSTL 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@cse-cst.gc.ca

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

   TO: <CST Lab>
   CC: cmvp@cse-cst.gc.ca; cmvp@nist.gov

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

   TO: <CST Lab>
   CC: cmvp@cse-cst.gc.ca

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

   TO: cmvp@nist.gov
   CC: cmvp@cse-cst.gc.ca

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

[9] **Shall** include file attachment, vendor.txt that contains the billing address

TO: cmvp@cse-cst.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>

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, with 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>.

NOTE: Following includes the full complement of files that are addressed in **IG G.2:**

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

1. *Security Policy*:

   s(scenario) = 1A, 1B, 3 or 5 <ZIP FILE NAME>**_140sp.pdf**

   s = 1[10] or 4[7] <ZIP FILE NAME>**_140sp**<CertNo>**.pdf**

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

2. *CRYPTIK Assessment Reports (IG G.2 and IG G.8 minimum requirements)*:

   s = 3 <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 = 4 <ZIP FILE NAME>**_report.pdf**

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

   s = 5 <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 = 1, 3, 4, or 5 <ZIP FILE NAME>**_vendor.txt**[11]

4. *CRYPTIK Draft Certificate*:

[10] Only required if the modifications cause changes to the areas in FIPS 140-2 Appendix C.

[11] 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.

s = 1A, 1B, 3, or 5 <ZIP FILE NAME>**_140crt.doc**

5. *CMVP Comments*:

s = 1, 3, 4, or 5 <ZIP FILE NAME>.doc

6. *Change Request Letter* [12]:

s = 1 or 4

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 Version**s** 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 3 Annex A. Current vs. Change Table to be submitted with a change request

[12] The change request letter shall provide a "Current" vs. "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 A.3 Submission Files sent between CSTL and CMVP

Submission Scenarios	CSTL to CMVP	File Content	CMVP to CSTL
5	_vendor.txt	Cryptik	
	_140sp.pdf	Security Policy	
	_report.pdf	Test Report	
	_entropy_report.pdf	Entropy Report	
	_140crt.doc, .docx, .rtf	Draft Certificate	doc, .docx, .rtf[13]
	.doc, .docx, .rtf[14]	CMVP Comments with CSTL Resolutions	doc, .docx, .rtf
4	_vendor.txt	Cryptik	
	_letter_unsigned.pdf	Change Request Letter	
	_letter_signed.pdf	Change Request Letter – signed	
	_140sp<CertNo>.pdf	Security Policy[15]	
	_report.pdf	Test Report[16]	
	.doc, docx, .rtf[1]	CMVP Comments with CSTL Resolutions	.doc, docx, .rtf
3	_vendor.txt	Cryptik	
	_140sp.pdf	Security Policy	
	_report.pdf	Test Report	
	_entropy_report.pdf	Entropy Report	
	_140crt.doc, docx, .rtf	Draft Certificate	doc, .docx,. rtf[2]
	doc, .docx, .rtf[1]	CMVP Comments with CSTL Resolutions	.doc, .docx, .rtf

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

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

[15] The Security Policy is required if the modifications cause changes to the areas in FIPS 140-2 Appendix C.

[16] Physical Security Test Report.

3A or 3B	_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 CSTL Resolutions	.doc, .docx, .rtf
	_letter_unsigned.pdf	Change Request Letter	
	_letter_signed.pdf	Change Request Letter – signed	
2[17]	_vendor.txt	Cryptik	
	_140sp.pdf	Security Policy	
	_report.pdf	Test Report	
	_entropy_report.pdf	Entropy Report	
	_140crt.doc, docx, .rtf	Draft Certificate	doc, .docx,. rtf[2]
	doc, .docx, .rtf[1]	CMVP Comments with CSTL Resolutions	.doc, .docx, .rtf
	_letter_unsigned.pdf	Change Request Letter	
	_letter_signed.pdf	Change Request Letter – signed	
1 *or* **1A**	_vendor.txt	Cryptik	
	_letter_unsigned.pdf	Change Request Letter	
	_letter_signed.pdf	Change Request Letter – signed	

[17] Scenario 2 will not be available beginning October 1, 2021.

	_140sp.pdf	Security Policy for 1A or 1B	
	_140sp<CertNo>.pdf	Security Policy[3] for 1SUB	
	_140cert.doc, .docx, .rtf	Draft Certificate for 1A or 1B	doc, .docx, .rtf[18]
	.doc, .docx, .rtf[1]	CMVP comments with CSTL resolutions	.doc, .docx, .rtf

Table 4 Annex A. Submission files to be included

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

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

Annex B ANNEX B: CMVP Validation Issue Assessment Process

Annex B.1 Addressing Security Relevant Issues

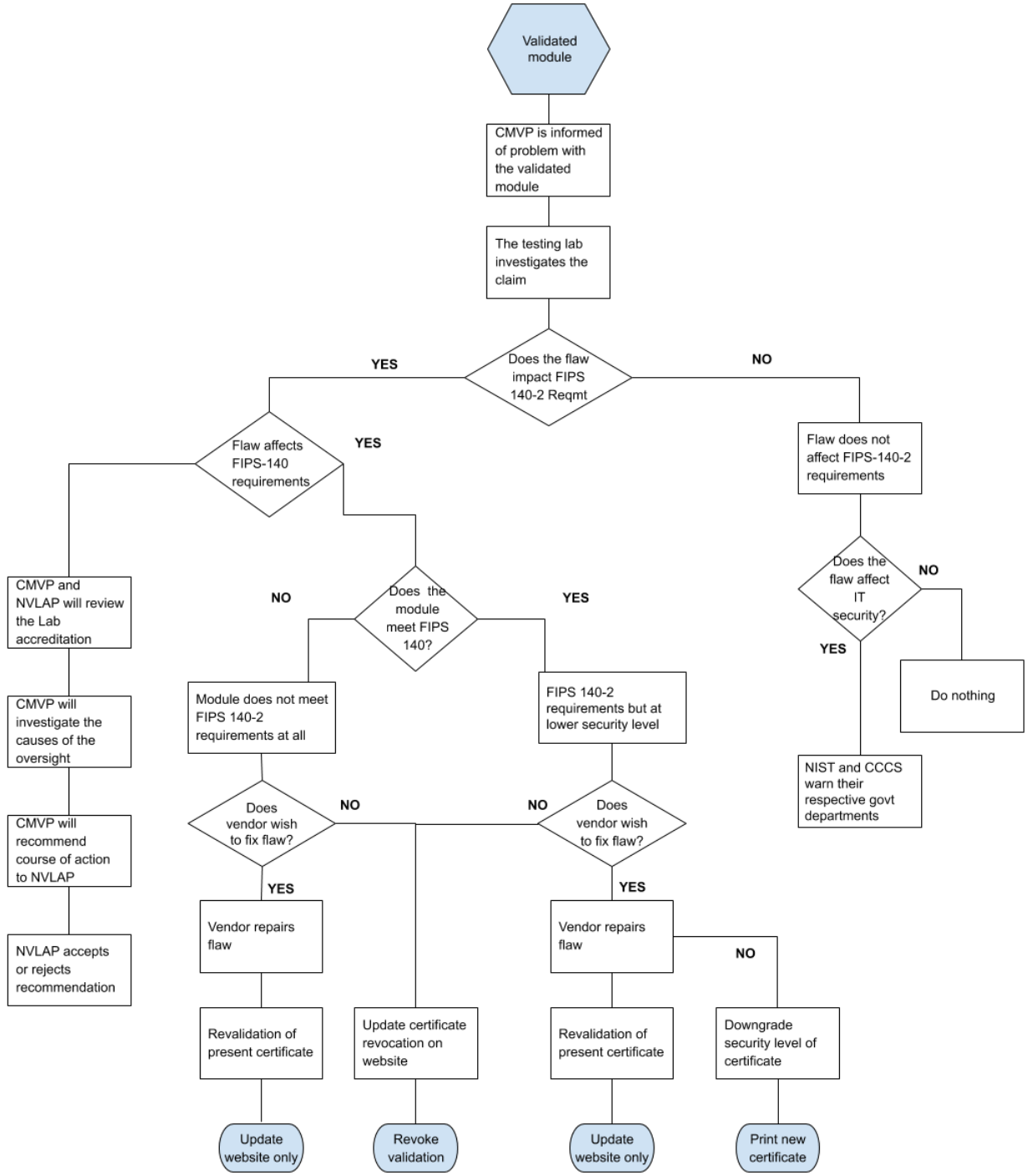

Figure 4 Annex B. Validation Issue Assessment Process

Annex B.2 Addressing CVE Relevant Vulnerabilities

The list of CVEs (Common Vulnerability and Exposures) is maintained by NIST in the National Vulnerability Database (NVD) at https://nvd.nist.gov/. The purpose of the Scenario 3A revalidation (described in the CMVP IG G.8) is to provide the vendor a means to quickly fix, test and revalidate a module that is subject to a security-relevant CVE, while at the same time providing assurance that the module still meets the current FIPS 140 standards.

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

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

For more information about CVEs please also refer to https://cve.mitre.org/.

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
CVE	Common Vulnerability and Exposures
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