



Cryptographic Module Validation Program Management Manual

DRAFT
(Version 1.0)

**National Institute of Standards and Technology
and
Communications Security Establishment Canada**

Initial release: 15 April 2009
Last update: _____

This page left blank intentionally.

Revision History

Version	Date	Comment
1.0	15 April 2009	Initial publication of the CMVP Management Manual

Table of Contents

1	INTRODUCTION	1
1.1	Background.....	1
1.2	Purpose of the CMVP Management Manual	1
1.3	Applicability and Scope	1
1.4	Purpose of the Cryptographic Module Validation Program	1
1.5	Use of Validated Products	1
1.6	CMVP Management Manual Structure	2
1.7	CMVP Related Documents.....	2
	1.7.1 FIPS 140-1.....	2
	1.7.2 Implementation Guidance for FIPS 140-1 and the CMVP.....	2
	1.7.3 FIPS 140-2.....	3
	1.7.4 Derived Test Requirements for FIPS 140-2	3
	1.7.5 Implementation Guidance for FIPS 140-2 and the CMVP.....	3
	1.7.6 CST Laboratory Accreditation Standards	4
	1.7.7 Other Documents on the CMVP Website.....	4
2	CMVP MANAGEMENT	6
2.1	Introduction.....	6
2.2	Validation Authorities.....	6
2.3	CMVP Points of Contact	6
2.4	Roles and Responsibilities of Program Participants	6
	2.4.1 Vendor	7
	2.4.2 CST Laboratory	7
	2.4.3 CMVP Validation Authorities.....	7
	2.4.4 User	8
2.5	Management of the CMVP.....	8
	2.5.1 CMVP Meetings.....	8
	2.5.2 CST Laboratory Manager Meetings.....	8
	2.5.3 Language of Correspondence	9
2.6	Confidentiality of Information.....	9
2.7	Agreements between Validation Authority Organizations	9
2.8	Relationship between Vendors, CST Laboratories, and NIST and CSEC.....	9
2.9	Programmatic Directives and Policies, and Internal Guidance and Documentation	10
3	CST LABORATORY PROCESSES.....	11

3.1	Accreditation of CST Laboratories	11
3.1.1	Recognized Standards and Standard Accreditation Body	11
3.1.2	Accreditation Process	11
3.2	Maintenance of CST Laboratory Accreditation.....	13
3.2.1	Proficiency of CST Laboratory	13
3.2.2	Renewal of Accreditation	13
3.2.3	Ownership of a CST Laboratory	14
3.2.4	Relocation of a CST Laboratory.....	14
3.2.5	Change of Approved Signatories.....	14
3.2.6	Change of Key Laboratory Testing Staff	14
3.2.7	Monitoring Visits	14
3.2.8	Suspension, Denial and Revocation of Accreditation	14
3.2.9	Voluntary Termination of the CST Laboratory.....	15
3.3	Confidentiality of Proprietary Information	15
3.3.1	Confidentiality of Proprietary Information Exchanged between NIST, CSEC and the CST Laboratory	15
3.3.2	Non-Disclosure Agreement for Current and Former Employees	15
3.4	Code of Ethics for CST Laboratories.....	15
3.5	Management of CMVP and CAVP Test Tools.....	16
3.6	Assistance CMT Laboratories may Provide to Vendors.....	16
3.6.1	Design and Testing of Cryptographic Modules.....	16
3.6.2	Finite State Model, Security Policy, User Guidance and Security Officer Guidance Documentation	17
4	CRYPTOGRAPHIC MODULE VALIDATION PROGRAM PROCESSES	18
4.1	Cryptographic Module Validation Process Overview	18
4.1.1	General Overview.....	18
4.1.2	Testing of the Cryptographic Module	19
4.1.3	Validation Report Review	20
4.1.4	Validation Certificate	20
4.1.5	CRYPTIK Tool	21
4.2	Modules in Process	21
4.2.1	Implementation Under Test (IUT).....	21
4.2.2	Review Pending.....	21
4.2.3	In Review	21
4.2.4	Coordination.....	22

4.2.5	Finalization.....	22
4.3	Preparation and Submission of the Validation Submission	22
4.4	Validation Submission Queue Processing	23
4.4.1	Initial Validation.....	23
4.4.2	Re-validation	23
4.4.3	Non-security Relevant Re-validation	24
4.4.4	HOLD Status for Cryptographic Modules on the Modules In Process	24
4.4.5	Queue Re-prioritizations	24
4.5	Validation when Test Reports are not Reviewed by both Validation Authorities	24
4.5.1	International Traffic in Arms Regulations Policy	25
4.6	NIST Cost Recovery	26
4.6.1	Validation Fee	27
4.6.2	Extended Fee	27
4.6.3	CMVP Payment Policy	28
4.7	Partial Validation	28
4.8	Maintaining Validation	28
4.8.1	Vendor	29
4.8.2	Users.....	30
4.9	Re-Validation of Cryptographic Modules	30
4.9.1	Modifications to Components that Do Not Affect FIPS 140-1 or FIPS 140-2 Components.....	31
4.9.2	No Modifications to the Cryptographic Module	32
4.9.3	Limited Modifications to FIPS 140-2 Assertions.....	32
4.9.4	Modifications to the Physical Enclosure	33
4.9.5	New Module	34
4.10	Requests for Guidance to NIST and CSEC	34
4.11	Request for Transition Period Extension	35
4.12	Flaw Discovery Handling Process	36
4.13	Validation Revocation	36
4.14	CMVP Webpage Update	36
4.14.1	Official CMVP Website	36
4.14.2	FIPS 140-1 and FIPS 140-2 Cryptographic Module Validation Lists.....	37
4.14.3	CMVP Vendor Product Link.....	37
4.14.4	Changes to Vendor, Module Name or Version Information	37
4.14.5	Security Policy Updates	37

4.14.6	Update Frequency of Validation Lists.....	37
4.15	Usage of FIPS 140-1 and FIPS 140-2 Logos.....	38
5	CMVP AND CAVP PROGRAMMATIC METRICS COLLECTION.....	40
5.1	Overview.....	40
5.2	Confidentiality of the Collected Metrics Data.....	40
5.3	Collected Metrics.....	40
5.4	Reported Metrics.....	41
5.5	Metrics Reporting.....	41
5.6	Reporting Deferral.....	41
5.7	Metrics Submission.....	42
5.8	Metrics Retention and Audit.....	42
5.9	METRIX Collection Tool.....	42
5.10	METRIX Repository Tool.....	42
6	DOCUMENTATION MAINTENANCE PROCESSES.....	43
6.1	FIPS 140-2 Publication (and subsequent Publication).....	43
6.2	Cryptographic Algorithm FIPS and NIST Special Publications.....	43
6.3	Derived Test Requirements.....	44
6.4	Implementation Guidance.....	44
6.5	FAQ for the CMVP.....	44
6.6	Test Tools.....	45
6.6.1	CRYPTIK.....	45
6.6.2	METRIX Collection Tool.....	45
6.6.3	METRIX Repository Tool.....	45
6.7	CST Laboratory Accreditation Standards.....	46
6.7.1	Handbook 150 – Procedures and General Requirements.....	46
6.7.2	Handbook 150-17 – Cryptographic and Security Testing.....	46
6.7.3	CAN-P-4E – General Requirements for the Competence of Testing and Calibration Laboratories.....	46
6.7.4	CAN-P-1591B – Guidelines for the Accreditation of Information Technology Security Evaluation and Testing Facilities.....	47
6.7.5	CAN-P-1621 – Requirements for the Accreditation of Cryptographic Module and Algorithm Testing Facilities.....	47
6.8	Management Manual.....	48
ANNEX A:	CODE CONVENTION (TRACKING IDENTIFICATION NUMBERS).....	49
ANNEX B:	REGRESSION TESTS FOR FIPS 140-2 VALIDATED CRYPTOGRAPHIC MODULES.....	51
ANNEX C:	FLAW DISCOVERY HANDLING PROCESS DIAGRAM.....	54

ANNEX D: GUIDELINES FOR THE USE OF THE FIPS 140-1 LOGO.....55
ANNEX E: GUIDELINES FOR THE USE OF THE FIPS 140-2 LOGO.....56
ANNEX F: GLOSSARY57

Figures

Figure 2-1: Roles and Responsibilities in the CMVP 6
Figure 3-1: CST Laboratory Accreditation Process..... 11
Figure 4-1: Cryptographic Module Testing and Validation Process..... 18

Tables

Table 4-1: Cost Recovery Fee Schedule.....27

1 Introduction

1.1 Background

The Communications Security Establishment Canada (CSEC) 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) 140-2, NIST-recommended standards, and other cryptography-based standards. The CMVP is a government validation program that is jointly managed by NIST and CSEC. Products or modules validated as conforming to FIPS 140-2 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) or Standard Council of Canada (SCC) 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 CSEC, 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. Guidance for these matters should be sought in the technical manuals of the standard, refer to [Section 1.7 CMVP Related Documents](#).

1.4 Purpose of the Cryptographic Module Validation Program

The purpose of the Cryptographic Module Validation Program is to ensure the availability and assurance of secure cryptographic modules for the protection of information through the conformance testing of cryptographic modules to FIPS 140-2 by independent accredited third-party CST laboratories and the validation of the results by the Validation Authorities for 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 140-2 for the protection of sensitive information. However, this standard has only been formally accepted by the Government of the United States of America and the Government of Canada (GC). As specified under FISMA of 2002, U.S. federal departments and agencies are required to use cryptographic modules validated to either FIPS 140-1 or FIPS 140-2 for the protection of sensitive information where cryptography is required. Similarly, the Communications Security Establishment Canada recommends that GC departments and agencies use those validated cryptographic modules for the protection of Protected information.

FIPS 140-2 is also used in other areas such as:

- Several Common Criteria (CC) Protection Profiles (PP) require FIPS 140-1 or FIPS 140-2 validated cryptographic modules. These PPs have been developed by many organizations throughout the world.
- The National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11 requires that products used for the protection of U.S. national information be, amongst other requirements, validated to FIPS 140-1 or FIPS 140-2 if the product implements cryptography.
- Many private sector organizations enforce the use of cryptographic modules validated to FIPS 140-1 or FIPS 140-2 in order to conform to a minimum baseline of security functionality and assurance.

A list of FIPS 140-1 and FIPS 140-2 validated cryptographic modules is located at the following NIST web site: <http://csrc.nist.gov/groups/STM/cmvp/validation.html> and at the following CSEC web site: <http://www.cse-cst.gc.ca/services/industrial-services/cmvp-val-products-e.html>.

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

1.7.1 FIPS 140-1

FIPS 140-1 (1994) 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 standard has been superseded by FIPS 140-2. Validations to FIPS 140-1 are still recognized by both governments. The document is available on-line on the official Cryptographic Module Validation Program websites at <http://csrc.nist.gov/publications/fips/fips140-1/fips1401.pdf> and <http://www.cse-cst.gc.ca/cmvp/>.

1.7.2 Implementation Guidance for FIPS 140-1 and the CMVP

Implementation Guidance for FIPS 140-1 and the CMVP is issued to provide clarification and guidance with respect to a particular assertion or group of assertions found in FIPS 140-1 and its Derived Test

Requirements (DTR). Even though FIPS 140-1 has been withdrawn, many of its guidance entries are still valid and applied to FIPS 140-2.

1.7.3 FIPS 140-2

FIPS 140-2 (2001) supersedes FIPS 140-1. The document specifies the security requirements for a cryptographic module utilized within a security system protecting sensitive information in computer and telecommunication systems, including voice systems. This standard specifies the security requirements that must be satisfied by a cryptographic module. The standard provides four increasing, qualitative levels of security intended to cover a wide range of potential applications and environments. The security requirements cover areas related to the secure design and implementation of a cryptographic module. These areas include cryptographic module specification; cryptographic module ports and interfaces; roles, services, and authentication; finite state model; physical security; operational 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 <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>.

1.7.4 Derived Test Requirements for FIPS 140-2

The Derived Test Requirements (DTR) for FIPS 140-2 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 FIPS PUB 140-2 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 PUB 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 PUB 140-2. Following each assertion is a set of information requirements that must be fulfilled by the vendor (VE). These requirements 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 requirements that must be applied by the tester of the cryptographic module (TE). These test requirements instruct the tester as to what they must do in order to test the cryptographic module with respect to the given assertion. The DTR is available on-line on the official Cryptographic Module Validation Program website at <http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/fips1402DTR.pdf>

1.7.5 Implementation Guidance for FIPS 140-2 and the CMVP

Implementation Guidance for FIPS 140-2 and the CMVP is issued to provide clarification and guidance with respect to a particular assertion or group of assertions found in FIPS 140-2 and its DTR. Often, implementation guidance is issued to assist CST laboratories and vendors to apply the requirements of FIPS 140-2 to a particular type of cryptographic module implementation or technology. Implementation guidance is also based on responses issued by NIST and CSEC to questions posed by the CST laboratories, vendors, and other interested parties.

The following CMVP programmatic implementation information previously found in the General section of *Implementation Guidance for FIPS 140-2* and the CMVP has been incorporated into this document:

- G.1 – Request for Guidance from the CMVP
- G.2 – Completion of a test report: Information that must be provided to NIST and CSEC

- G.4 – Design and testing of cryptographic modules
- G.7 – Relationships among Vendors, Laboratories, and NIST and CSEC
- G.8 – Revalidation Requirements
- G.9 – FSM, Security Policy, User Guidance and Security Officer Guidance Documentation
- G.10 – Physical Security Testing for Revalidation from FIPS 140-1 to FIPS 140-2
- G.12 – Post-validation Inquiries

The document is available on-line on the official Cryptographic Module Validation Program website at <http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402IG.pdf>

1.7.6 CST Laboratory Accreditation Standards

NIST laboratory accreditation standards applicable to the NVLAP accreditation of CST laboratories are published on the NVLAP website at <http://ts.nist.gov/Standards/214.cfm>. Links to these standards are also provided on the official CMVP website http://www.csrc.nist.gov/groups/STM/testing_labs/index.html#details and the testing laboratories website http://www.csrc.nist.gov/groups/STM/testing_labs/index.html.

NIST laboratory accreditation standards relevant to the NVLAP accreditation of CST laboratories are:

1. NIST Handbook 150 (2006), *NVLAP Procedures and General Requirements*, <http://ts.nist.gov/Standards/Accreditation/upload/nist-handbook-150.pdf>; and
2. NIST Handbook 150-17 (2008), *NVLAP Cryptographic and Security Testing*, Document available on-line at http://csrc.nist.gov/groups/STM/testing_labs/hnbk-17.pdf.

Standards Council of Canada (SCC) laboratory accreditation standards that can be applied to the accreditation of Canadian CST laboratories are published on the SCC website at <http://www.scc.ca/en/publications/criteria/labs/index.shtml> and include:

1. CAN-P-4E, *General Requirements for the Competence of Testing and Calibration Laboratories*;
2. CAN-P-1591B, *Guidelines for the Accreditation of Information Technology Security Evaluation and Testing Facilities* http://www.scc.ca/Asset/iu_files/criteria/1591b_e.pdf; and
3. CAN-P-1621, *Requirements for the Accreditation of Cryptographic Module and Algorithm Testing Facilities* http://www.scc.ca/Asset/iu_files/criteria/1621_e.pdf.

1.7.7 Other Documents on the CMVP Website

The CMVP website hosts several other links and documents that provide information about the program:

1. Announcements (<http://csrc.nist.gov/groups/STM/cmvp/announcements.html>) contains information on changes made to documents or test tools pertinent to the Cryptographic Module Validation Program.
2. Notices (<http://csrc.nist.gov/groups/STM/cmvp/notices.html>) 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 <http://csrc.nist.gov/groups/STM/cmvp/faqs.html> contains questions and answers to several issues pertaining to the CMVP.
4. Validation Lists (<http://csrc.nist.gov/groups/STM/cmvp/validation.html>) contains the most current information about cryptographic modules validated to FIPS 140-1 and FIPS 140-2.

5. Modules in Process (<http://csrc.nist.gov/groups/STM/cmvp/inprocess.html>) contains information provided by the CST laboratories about cryptographic modules undergoing testing under FIPS 140-2. (The listing is voluntary where vendors may choose to have their module listed on this list).
6. List of Accredited CST Laboratories (http://csrc.nist.gov/groups/STM/testing_labs/index.html) contains 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 CMVP 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 Communications Security Establishment Canada 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 CSEC. 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.

Section 4.10: Requests for Guidance to NIST and CSEC describes the process by which vendors and CST laboratories can formally submit questions to the CMVP.

The name, telephone number and email address for the NIST CMVP Director and CSEC Head – CMVP are:

NIST

Randall J. Easter
 Director CMVP
 Security Testing & Metrics Group
 (301) 975-4641
reaster@nist.gov

CSEC

Jean Campbell
 Head – CMVP
 Industry Program Group
 (613) 991-8121
jean.campbell@cse-cst.gc.ca

A complete list of all CMVP points of contact can be found on the CMVP website at:
<http://csrc.nist.gov/groups/STM/cmvp/contacts.html>.

2.4 Roles and Responsibilities of Program Participants

The various roles and responsibilities of the participants in the CMVP are illustrated in **Figure 2-1: Roles and Responsibilities in the CMVP** below.

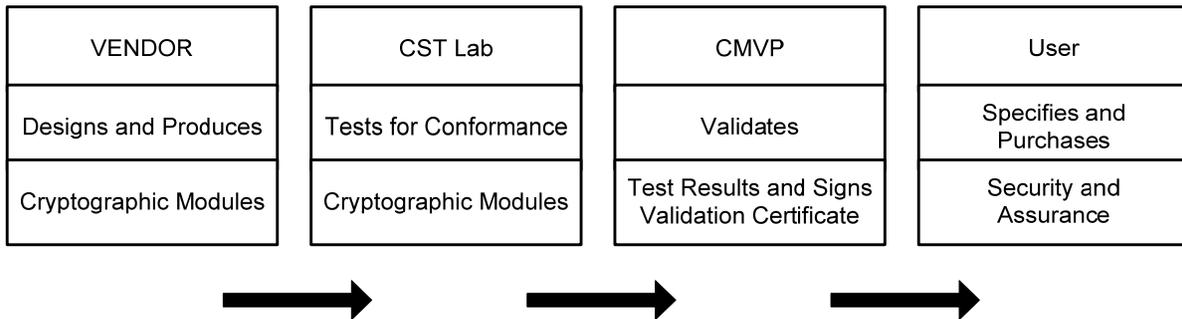


Figure 2-1: Roles and Responsibilities in the CMVP

2.4.1 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 laboratories of its choice.

After the cryptographic module has been validated, the vendor can not change the validated version of the module. Any change to the validated version will result in a new module which is not validated and therefore a new validation test effort would need to be performed on the new module.

2.4.2 CST Laboratory

The role of the CST laboratory is to independently test the cryptographic module to the appropriate FIPS 140-2 security level and embodiment, and produce a written test report for the CMVP Validation Authorities based on its findings. The CST laboratory conducts the algorithmic testing, reviews the cryptographic module's documentation and source code, and performs the operational and physical testing of the module. The requirements levied on the cryptographic module are specified in FIPS PUB 140-2 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 (subject to the specific limitations described in **Section** Error! Reference source not found.**Error!** Reference source not found.) to resolve all discrepancies prior to submitting the validation package to the Validation Authorities.

CST laboratories must exercise due diligence when performing their conformance testing, as well as abide by the policies and procedures outlined in this manual.

A list of accredited CST laboratories is available at (http://csrc.nist.gov/groups/STM/testing_labs/index.html) under the Testing Laboratories menu tab or from the CSEC website at <http://www.cse-cst.gc.ca/services/industrial-services/nvlap-e.html>. The accreditation process for CST laboratories is briefly described in **Section 3: CST Laboratory Processes** of this manual.

2.4.3 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 Communications Security Establishment Canada 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, to the CST laboratory accreditation process which includes the review of the management system manual, the conduct of the proficiency exam, the on-site assessment and the oversight of the artifact testing.

2.4.4 User

The user verifies that a cryptographic module that they are considering procuring has been validated and meets their requirements. The listing of validated cryptographic modules is located at <http://csrc.nist.gov/groups/STM/cmvp/validation.html> and from CSEC website at <http://www.cse-cst.gc.ca/services/industrial-services/cmvp-val-products-e.html>. A non-proprietary security policy is posted on the aforementioned list for each validated cryptographic module so that a potential user can determine if the validated cryptographic module provides the cryptographic services and protection required for the particular application and threat environment. NIST Special Publication 800-21, *Guidelines for Implementing Cryptography in the Federal Government*, on the official NIST Computer Security Division website at http://csrc.nist.gov/publications/nistpubs/800-21-1/sp800-21-1_Dec2005.pdf is a good reference on the use of cryptography for U.S. Federal Government departments and agencies, and also provides valuable guidance for any user of FIPS validated cryptography.

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 listed on the listing of validated cryptographic modules provided on the CMVP website.

Users can also develop product or system specifications that include the requirements for FIPS 140-2 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.

2.5 Management of the CMVP

The CMVP is jointly managed by NIST and CSEC. Decisions are made jointly by both organizations with the NIST Director CMVP and the CSEC Head – CMVP communicating regularly.

2.5.1 CMVP Meetings

CSEC 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.

2.5.2 CST Laboratory Manager Meetings

NIST and CSEC organize semi-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 minutes are taken, filed, and distributed to the CST laboratories 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.

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

2.5.3 Language of Correspondence

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

2.6 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, CSEC, and the CST laboratories to protect against unauthorized disclosure of vendors' proprietary information. Any potential or actual breach of confidentiality could have an adverse effect on the NIST, CSEC, a CST laboratory's accreditation, or the program.

As required by the CST laboratory accreditation standards listed in **Section 1.7.6: CST Laboratory Accreditation Standards**, 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 CSEC.

NIST, CSEC, 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.

2.7 Agreements between Validation Authority Organizations

The CMVP is jointly managed by NIST and CSEC. NIST and CSEC 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 Industry Program Group at CSEC and by the Computer Security Division at NIST.

2.8 Relationship between Vendors, CST Laboratories, and NIST and CSEC

The following policy statements have been excerpted from the *Implementation Guidance for FIPS 140-2* Section G.7 – Relationships among Vendors, Laboratories, and NIST and CSEC.

The CST laboratories are accredited by NVLAP or SCC to perform cryptographic module validation testing to determine compliance with FIPS 140-2 and other cryptographic algorithm FIPS and NIST Special Publications. NIST and CSEC rely on the CST laboratories to use their extensive validation testing experience and expertise to make sound, correct, and independent decisions based on FIPS 140-2, the Derived Test Requirements for FIPS 140-2 *Security Requirements for Cryptographic Modules*, the *Implementation Guidance for FIPS 140-2*, and other testing tools. Once a vendor is under contract with a laboratory, NIST and CSEC will only provide official guidance and clarification for the vendor's module through the point of contact at the CST laboratory.

In a situation where the vendor and CST laboratory reach an impasse over a testing issue, the vendor may ask for clarification/resolution directly from NIST and CSEC. The vendor should use the format required by **Section 4.10: Requests for Guidance to NIST and CSEC**. The point of contact at the CST laboratory must be copied on all correspondence. All correspondence from NIST and CSEC to the vendor regarding any such issues will be provided through the CST laboratory point of contact.

2.9 Programmatic Directives and Policies, and Internal Guidance and Documentation

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

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

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

3 CST Laboratory Processes

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

3.1 Accreditation of CST Laboratories

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

Note: This section describes the process used by NVLAP. The process followed by SCC is very similar.

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:

1. NIST Handbook 150 (2007) and Handbook 150-17 (2008) under the NVLAP of the Government of the United States of America; and
2. CAN-P-4E (2005-11-01), CAN-P-1591B (2006-11) and CAN-P-1621 (2006-11) under the Standards Council of Canada of the Government of Canada.

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 3-1: CST Laboratory Accreditation Process**. All steps in the accreditation process are sequential and must be completed in the order shown.

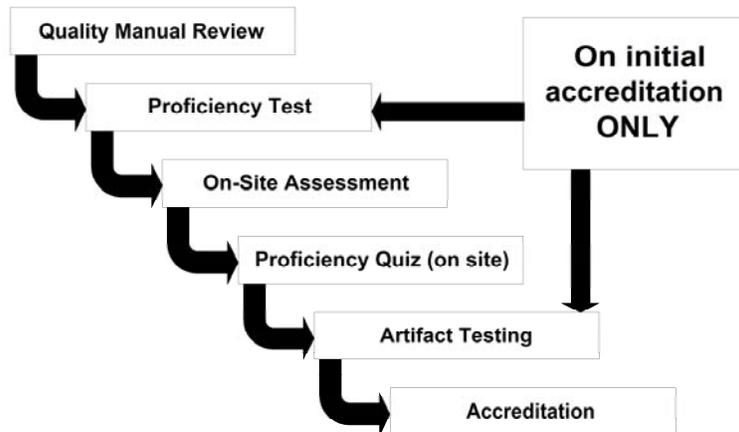


Figure 3-1: CST Laboratory Accreditation Process

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 conditions for accreditation, and provide their quality manual to NVLAP prior to the assessment process. Upon receipt of an application by NVLAP, an assessment team is selected mainly from the CMVP. This team is typically comprised of two representatives from NIST and one representative from CSEC. 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 Quality Manual Review

The assessment team will review the Quality Manual 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. The examination consists of approximately thirty questions relating to various aspects of CST laboratory activities, FIPS 140-2, and cryptographic algorithm implementation testing. The applicant laboratory is provided seven (7) days to complete the exam. The assessing team will grade the exam and determine if the laboratory is competent.

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. An assessment typically takes two (2) business days to perform. The activities performed during an assessment are described in Section 3.2 Assessment of NIST Handbook 150 or in Section 4 Demonstrating Technical Competence of CAN-P-1621.

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 (30) days of notification.

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

3.1.2.5 Proficiency Quiz

During the on-site assessment, the assessment team will conduct a proficiency quiz with all of the applicant laboratory staff to determine the level of knowledge of the team and to evaluate how the group interacts when addressing a problem.

3.1.2.6 Artifact Testing

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 a year. 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.

3.1.2.7 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

3.1.2.8 Granting Accreditation

Once the approval has been granted to accredit the CST laboratory for CST 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. 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.

3.1.2.9 CMVP and CAVP Test Tools

Once accreditation has been granted and the CMVP and CAVP are advised by NVLAP that the applicant laboratory has been accredited, the CMVP and CAVP will issue to the newly accredited CST laboratory the latest version of the CRYPTIK, CAVS and METRIX tools. The CMVP and CAVP will also issue the latest programmatic directives and policies, and internal guidance and documentation.

3.2 Maintenance of CST Laboratory Accreditation

3.2.1 Proficiency of CST Laboratory

CST laboratories must submit at least one validation test report during their accreditation cycle 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 will perform a new on-site assessment, monitoring visit, and/or proficiency test of the laboratory.

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 <http://ts.nist.gov/Standards/Accreditation/feesch.cfm>. 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 3-1: CST Laboratory Accreditation Process** and described in **Section 3.1.2**, except that the Proficiency Examination and the Artifact Testing steps are not performed. 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 (30) days of notification.

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 ten (10) working days of the identity of the new owner of the laboratory and the effective date of the change. The laboratory must also submit an update to the Quality Manual to NVLAP showing the new owner information.

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 ten (10) working days of the new signatories and the effective date of the change. The laboratory must also submit, if necessary, an update to the Quality Manual to NVLAP showing the new signatory information.

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 ten (10) working days. The laboratory must also submit, if necessary, an update to the Quality Manual to NVLAP showing the 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.

Discovery of serious violations such as breach of information confidentiality will result in an immediate recommendation by the CMVP Heads to the accreditation body to suspend the CST laboratory's accreditation while an investigation is conducted and 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.

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, CSEC and the CST Laboratory

The confidentiality of the proprietary information exchanged between NIST, CSEC 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

This Code of Ethics is largely based on the IEEE Code of Ethics (August 1990) and the Advanced Card Technology Association of Canada's (ACT Canada) Code of Professional Ethics.

WE, as testers, reviewers, managers, and directors in accredited Cryptographic and Security Testing Laboratories, in recognition of our responsibility to the Cryptographic Module Validation Program and the Cryptographic Algorithm Validation Program, to our colleagues, and to our clients, do hereby commit ourselves to the highest ethical and professional conduct and agree to the following precepts:

- 1. to accept responsibility for making decisions consistent with the requirements of the standards to which we conduct testing and with the requirements of the Cryptographic Module Validation Program, the Cryptographic Algorithm Validation Program and the standards to which the laboratory of which we are a member is accredited;*
- 2. to be honest, objective, and accurate in presenting evidence in support of meeting a requirement;*
- 3. to seek, accept, and offer honest criticism of technical work, to acknowledge and correct errors, and to credit properly the contributions of others;*
- 4. to maintain and improve our technical competence and to undertake technological tasks for others only if qualified by training or experience, or after full disclosure of pertinent limitations;*
- 5. to avoid real or perceived conflicts of interest whenever possible, and to disclose them to all affected parties when they do exist;*
- 6. to reject bribery in all its forms;*
- 7. to treat others with dignity and professional courtesy;*

8. *to avoid injuring others, their property, reputation, or employment by false or malicious action; and*
9. *to assist co-workers in their professional development and to support them in abiding by this code of ethics.*

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 CSEC 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, provided that they are used within the CST laboratory facilities. Test tools include all versions of CRYPTIK, the Cryptographic Algorithm Validation System (CAVS), the METRIX tools and any other tools developed by NIST and CSEC for use by the CMVP and CAVP. Violation of this policy may be considered cause for suspension of the CST laboratory's accreditation.

3.6 Assistance CMT Laboratories may Provide to Vendors

The following policy statements have been excerpted from the *Implementation Guidance for FIPS 140-2* Sections G.4 – Design and Testing of Crypto Module and G.9 – FSM, Security Policy, User Guidance, and Security Officer Guidance Document. They describe documentation development activities allowed by the CMVP.

3.6.1 Design and Testing of Cryptographic Modules

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 CST 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 140-2, the Derived Test Requirements, and other associated documents at any time during the life cycle of the module, including:
 - a. documents developed by the CMVP staff for the Cryptographic and Security Testing program (e.g., Implementation Guidance, CMVP Policy, Handbook 150-17, Cryptographic and Security Testing); and

- b. Implementation Guidance and policy associated with FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*.

3.6.2 Finite State Model, Security Policy, User Guidance and Security Officer Guidance Documentation

A CST laboratory may take 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. If this occurs, NIST and CSEC shall be notified of this documentation when the validation report is submitted. Additional details for the individual documents are provided below.

3.6.2.1 Finite State Model Guidance

The vendor-provided documentation must readily provide a finite set of states, a finite set of inputs, a finite set of outputs, a mapping from the sets of inputs and states into the set of states (i.e., state transitions), and a mapping from the sets of inputs and states onto the set of outputs (i.e., an output function).

3.6.2.2 Security Policy Guidance

The vendor-provided documentation must readily provide a precise specification of the security rules under which a cryptographic module must operate, including the security rules derived from the requirements of FIPS 140-2 and the additional security rules imposed by the vendor.

In addition, a CST laboratory must be able to show a mapping from the consolidated or reformatted FSM and/or Security Policy back to the original vendor source documentation. The laboratory must maintain the mapping(s) as part of the validation records.

Consolidating and reformatting are defined as follows:

1. The original source documents were prepared by the vendor (or a subcontractor to the vendor) and submitted to the laboratory with the cryptographic module.
2. The laboratory extracts applicable technical statements from the original source documentation to be used in the FSM and/or Security Policy. The technical statements may only be reformatted to improve readability of the FSM and/or Security Policy. The content of the technical statements must not be altered.
3. The laboratory may develop transitional statements in the FSM and/or Security Policy to improve readability. These transitional statements shall be specified as developed by the laboratory in the mapping.

3.6.2.3 User Guidance and Security Officer Guidance

A CST laboratory may create User Guidance, Security Officer Guidance and other non-design related documentation for an existing cryptographic module (post-design and post-development). If this occurs, NIST and CSEC shall be notified of this documentation when the validation report is submitted.

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 4-1: Cryptographic Module Testing and Validation Process shows the general flow of testing and validation of a cryptographic module to the FIPS 140-2 standard.

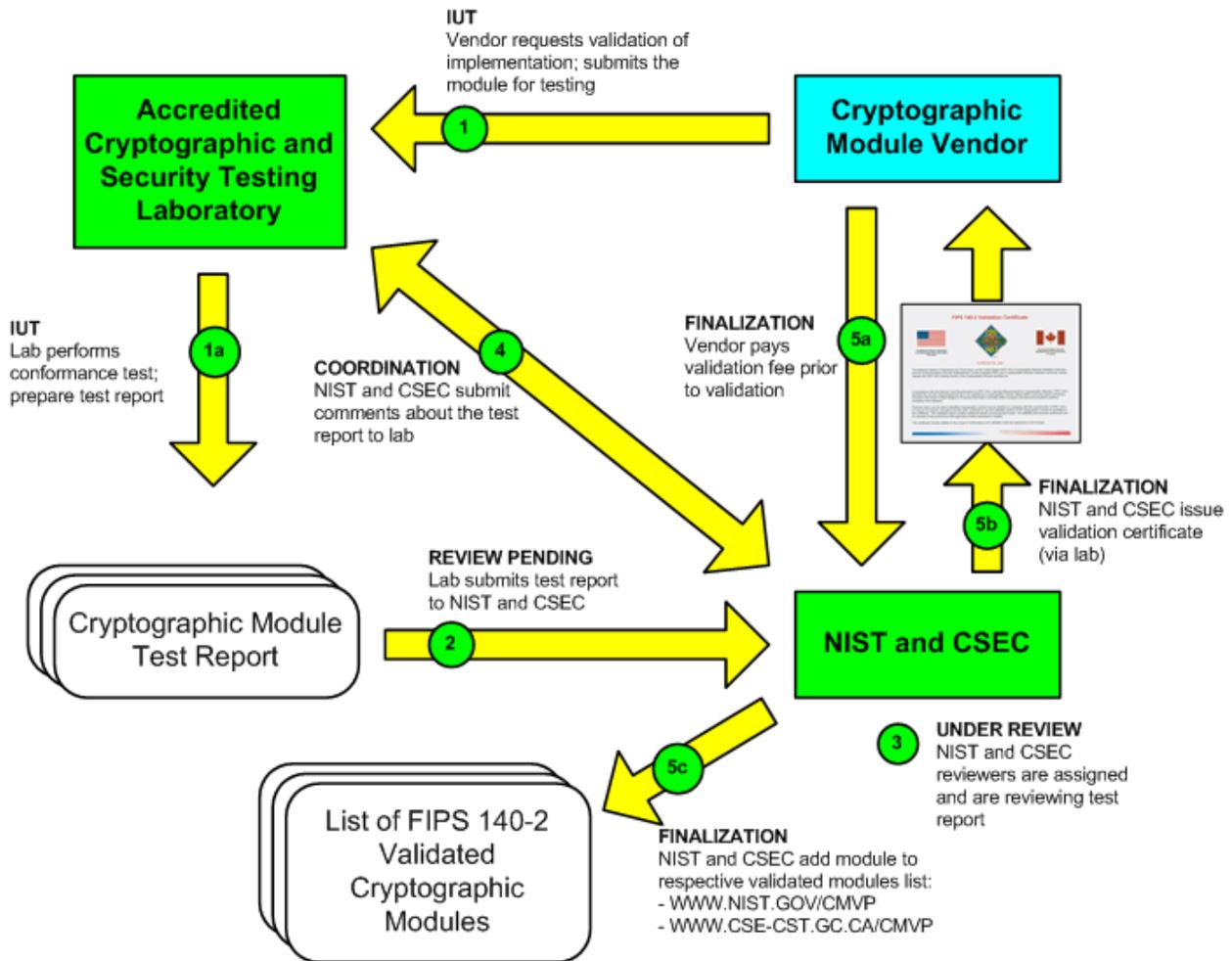


Figure 4-1: Cryptographic Module Testing and Validation Process

The steps for the cryptographic module validation life cycle include:

Step 1. The vendor submits the cryptographic module for testing to an accredited CST laboratory under a contractual agreement. Cryptographic module validation testing is performed using the Derived Test Requirements (DTR) for FIPS PUB 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 CSEC as described in **Section 4.10: Requests for Guidance to NIST and CSEC**.

- Step 2. Once all the testing requirements have been completed, a validation submission is prepared and submitted to NIST and CSEC for validation.
- Step 3. A reviewer from NIST and a reviewer from CSEC are assigned to review the validation report, the non-proprietary security policy, and other supporting documents.
- Step 4. During the review process, NIST and CSEC will combine, as required, their comments on the validation report and will submit them to the CST laboratory for action. This process will continue until all comments and/or questions have been satisfactorily addressed.
- Step 5. Once the cryptographic module has been validated, NIST and CSEC will issue a certificate through the CST laboratory to the vendor. The new validated cryptographic module will be given an entry in the *FIPS 140-1 and FIPS 140-2 Cryptographic Module Validation List* at the NIST website: <http://csrc.nist.gov/groups/STM/cmvp/validation.html> and CSEC website: <http://www.cse-cst.gc.ca/services/industrial-services/cmvp-val-products-e.html>.

4.1.2 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 notifies the primary contacts at NIST and CSEC 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 *FIPS 140-1 and FIPS 140-2 Modules In Process*. 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 CSEC provides the last set of four digits upon submission of the validation submission. The CSEC TID portion is to be appended to the six lab-assigned digits, as described in **Annex A: Code Convention (Tracking Identification Numbers) Section 1 Submission Number**. 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 PUB 140-2, *Security Requirements for Cryptographic Modules* and enters all assessments for the testing in the CRYPTIK tool. Although testing requirements are in the DTR, FIPS PUB 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 140-2 validation testing. Please refer to **Section 4.1: Cryptographic Module Validation Process Overview** for more information.

At any point in the testing the CST laboratory may wish to request guidance from CSEC and NIST in determining how to apply the FIPS 140-2 standard to the particular cryptographic algorithm module. For more details on this process, refer to **Section 4.10: Requests for Guidance to NIST and CSEC**.

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 140-2, the laboratory prepares the validation test report and the rest of the validation test submission and sends it to NIST and CSEC 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.

4.1.3 Validation Report Review

All FIPS 140-2 validation submissions are examined by the CMVP. Validation submissions are referenced by a CMVP Tracking Identification Number (TID) that is a number composed from both a Laboratory TID and a CSEC TID as described in **Annex A: Code Convention (Tracking Identification Numbers) Section 1 Submission Number**. When CMVP reviewers are assigned to a cryptographic module validation submission, the cryptographic module is moved to the IN REVIEW stage of the Modules In Process described in [Section 4.2 Modules in Process](#). When the CMVP reviewers have completed their review of the validation submission and provided comments, the CSEC or NIST CMVP administrator sends the encrypted comment sheet 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 Test Report Submission](#). The CSEC and NIST reviewers examine the responses, and if found acceptable, the cryptographic module is moved to the FINALIZATION stage. The *CMVP FIPS 140-1 and FIPS 140-2 Modules In Process* is updated as needed by the NIST CMVP administrator.

4.1.4 Validation Certificate

At the end of the validation process NIST and CSEC, as the Validation Authorities, issue a certificate that includes the version number of the validated cryptographic module and benchmark configuration of the original validation testing. Instructions for completing a FIPS 140-2 validation certificate are found at *Implementation Guidance for FIPS 140-2 Section G.13*.

When NIST and CSEC are satisfied with the test report, CSEC sends the finalized comment sheet and the electronic version of the draft validation certificate to the CST laboratory. The CST laboratory must review and confirm or correct the information on the certificate. Once the information is confirmed, CSEC will issue a certificate number to the laboratory and the certificate is processed and signed by the Validation Authorities. After both Validation Authorities have signed the validation certificate, the certificate number and the cryptographic module information are posted on the website and the certificate is sent to the laboratory for furtherance to the vendor (**Figure 4-1: Cryptographic Module Testing and Validation Process**, steps 5 and 5a).

The information on the certificate pertains to the module at the time of its validation. During its life cycle the module information for that particular validation may change. As described in **Section 4.9: Re-Validation of Cryptographic Modules**, the module's validation will be updated on the website but a new validation certificate will not be issued. Therefore, users should only use the information about a particular certificate that is presented on the NIST or CSEC website. Depending of the nature or extent of the change to module, a new validation certificate may be issued.

Module certificate numbers are not assigned and certificates are not issued unless the signature page is received from the CST laboratory.

4.1.5 CRYPTIK Tool

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 140-2 validation test report and draft certificate. Information about new features, enhancements, and bug fixes are provided with each release of the tool.

4.2 Modules in Process

The *CMVP FIPS 140-1 and FIPS 140-2 Modules In Process List* is provided for information purposes only. Participation on the list is *voluntary* and is a joint decision by the vendor and the CST laboratory. Modules are listed alphabetically by name. Blank entries indicate Modules In Process but a decision has been made by the vendor not to post the name of the module. Posting on the list does not imply or guarantee FIPS 140-2 validation. The Modules In Process list is available on the NIST web site <http://csrc.nist.gov/groups/STM/cmvp/inprocess.html>.

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.

4.2.1 Implementation Under Test (IUT)

1. There exists a viable contract between the vendor and the CST laboratory for the testing of the cryptographic module.
2. The cryptographic module is resident at the CST laboratory or is ready for testing at the vendor's facilities.
3. All of the required documentation is resident at the CST laboratory or is ready for testing at the vendor's facilities. 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.

4.2.2 Review Pending

1. Complete validation submission has been submitted to NIST and CSEC for review. The submission includes: draft certificate, summary module description, detailed test report, non-proprietary security policy, and website information. In addition, some modules may require a separate physical security testing report.
2. Signed letter recommending the validation of the module from laboratory has been received by NIST and CSEC.
3. The validation submission has entered the First-In-First-Out queue waiting for available reviewers from NIST and CSEC.

4.2.3 In Review

1. CMVP reviewers have been assigned.
2. CMVP may perform a preliminary review of the test documents.
3. CMVP performs a review of the test documents.
4. Comments coordinated by CMVP reviewers and combined set of comments sent to the CST laboratory.

4.2.4 Coordination

This phase of the process may be iterative.

1. Comments have been received by the CST laboratory from NIST and CSEC for resolution.
2. Additional testing (if required).
3. Additional documentation (if required).
4. Comments resolution developed for resubmission to NIST and CSEC.
5. Testing documents updated for resubmission to NIST and CSEC.
6. Responses to comments and revised test documents submitted to NIST and CSEC.
7. NIST and CSEC perform a review of the re-submitted test documents.
8. Comments coordinated by NIST and CSEC reviewers and combined set of comments sent to the CST laboratory.

4.2.5 Finalization

1. Final resolution of In Review comments submitted to NIST and CSEC.
2. Testing documents updated based on resolutions and submitted to NIST and CSEC.
3. A final draft of the certificate is reviewed by CSEC.
4. After CSEC final review, CSEC sends a copy to NIST and the CST laboratory for a final review.
5. Once NIST and the CST laboratory review and OK the final draft, CSEC prints and signs the hard copy certificate.
6. After signing the certificate, CSEC scans the certificate and saves the image to their electronic file folders. The original hard copy of the certificate is sent to NIST by mail.
7. When NIST receives the original hard copy certificate from CSEC in the mail, they will sign it. A color image of the certificate will be created in PDF format and the image will be posted on the website at <http://csrc.nist.gov/groups/STM/cmvp/validation.html>
8. NIST will mail the signed hard copy certificate with the *Guidelines for the Use of the FIPS 140-2 Logo* page described in **Section 4.15: Usage of FIPS 140-1 and FIPS 140-2 Logos** , and the Vendor Product Link information page to the CST laboratory.

4.3 Preparation and Submission of the Validation Submission

NIST and CSEC as the Validation Authorities may request any or all information used by the CST laboratory to prepare the validation test report, whether or not 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* Section G.2 – Completion of a Test Report: Information that must be provided to NIST and CSEC.

The following information and documentation shall be provided to both NIST and CSEC by the CST laboratory. Also, each submission documents shall be compressed into a single zip file and should follow the naming format indicated in **Annex A: Code Convention (Tracking Identification Numbers) Section 4: ZIP File Naming Format**.

1. **Non-proprietary Security Policy in PDF.** The security policy shall not be marked as proprietary or copyright, and must 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 v7.0b (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. **Billing for Cost Recovery** – PDF do not include if not applicable;
 - d. **Report Overview with Assessments** – PDF;
 - e. **Full Report with Assessments** – PDF; and
 - f. **Definitions / References** (optional) – PDF.
3. **Physical Test Report** (mandatory at Levels 2, 3 and 4) – PDF. The physical testing report must include photos, drawings, etc. as applicable.
4. **Re-validation Change Summary** – PDF, for re-validation.
5. **Section Summaries** (optional) – PDF, briefly describe how the requirements in each section are met.
6. **Certification Documents**
 - a. Draft certificate – DOC format;
 - b. Vendor file – TXT format (certificate information).

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 CSEC. The Report Overview with Assessments and Detailed Report with Assessments shall not include proprietary information. All CRYPTIK PDF submission outputs, including optional section summaries and physical test report must be merged into a single PDF document. 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 CSEC reviewers, and sent to the following NIST and CSEC points of contact:

- NIST: CMVP@nist.gov
- CSEC: CMVP@cse-cst.gc.ca

4.4 Validation Submission Queue Processing

4.4.1 Initial Validation

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 CSEC CMVP Directors. Reports will not be marked as FULL or RE-VALIDATION on the Modules In Process, or ordered differently as currently posted on the Modules In Process.

4.4.2 Re-validation

Modules that are marked as security relevant re-validations as per **Section 4.9.3: Limited Modifications to FIPS 140-2 Assertions**, will be internally placed in a queue separate from the one for the new full

validations. These modules will receive higher review priority and will be reviewed in order received independent and separate of new reports. To expedite this, the cover letter for such report submissions should be clearly marked as being a RE-VALIDATION submission and shall contain a brief summary of the security relevant changes made to the module is recommended.

4.4.3 Non-security Relevant Re-validation

Non-security relevant change letters as described in **Sections 4.9.1: Modifications to Components that Do Not Affect FIPS 140-1 or FIPS 140-2 Components** and **4.9.2: No Modifications to the Cryptographic Module** will be handled upon receipt.

4.4.4 HOLD Status for Cryptographic Modules on the Modules In Process

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

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 on the CMVP Modules In Process while it has this status.
4. Modules that were in the REVIEW PENDING stage when placed on HOLD will move to the back of the CMVP queue (when they are removed from HOLD). They will not return to the position they held prior to being placed on HOLD.
5. Modules that were in the IN REVIEW stage or a later stage when placed on HOLD will return to their former position in the CMVP queue (when they are removed from HOLD).

If a module test report is sent incomplete or is determined to be incomplete once the module has moved to the IN REVIEW stage, the module will be placed on HOLD and the NIST Extended Fee will apply. When the incomplete items are received by the CMVP, the module will return to the CMVP queue in the REVIEW PENDING stage at the top of the queue.

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

4.4.5 Queue Re-prioritizations

A CST laboratory may request the CMVP to change the order of the module submissions the laboratory has submitted for validation. The laboratory must identify the modules affected and the order it wishes to have them. The responsibility of the queue re-prioritization solely rests with the requesting CST laboratory.

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 Regulations¹ (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 CSEC TID. A CSEC 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 CSEC signature field will be marked as: *Not Applicable – ITAR*.
 - c. The certificate will be black and white.
 - d. 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.

¹ EXAMPLE:

Not Releasable to Foreign Persons or Representatives of a Foreign Interest.

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

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

- e. The official certificate will be sent to the CST laboratory for presentation to the vendor.
4. Re-validation
- a. All re-validation changes under **Section 4.9: Re-Validation of Cryptographic Modules** will result in a new certificate printed and 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 **Section 4.9: Re-Validation of Cryptographic Modules**.

4.5.1.2 Canadian Exemptions

The vendor and CST laboratory may review the ITAR regulations in regard to §126.5 Canadian Exemptions (see http://pmddtc.state.gov/docs/ITAR/2007/official_itar/ITAR_Part_126.pdf) to determine its applicability. If applicable, the review of the test report, printing, and signature of the certificate would allow the participation of CSEC. If the exemption is applicable, please state the report is applicable to ITAR with reference to the Canadian exemption. The following will apply for this scenario:

1. Report Submission – instructions in **Section 4.3: Preparation and Submission of the Validation Submission** apply 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 and CSEC CMVP reviewers.
 - d. The test report package is submitted to NIST and CSEC CMVP.
 - e. Actual module names, versions, and vendor information will be provided. This information will not be masked by dummy information.
2. Report Review
 - a. Each ITAR report will be reviewed by NIST and CSEC.
3. Certificate Generation and Posting
 - a. Certificates will be prepared normally by CSEC.
 - b. Certificates will be signed by both NIST and CSEC.
 - c. The NIST CMVP web page will only post the information as above.

4.6 NIST Cost Recovery ²

The fees are based on the overall security level of the validation. The following table lists the Validation and Extended Fees by Security Levels.

² CSEC does not levy any charges for the validation of cryptographic modules.

Overall Security Level	Validation Fee	Extended Fee
Security Level 1	\$2,750 US	\$1,250 US
Security Level 2	\$3,750 US	\$1,750 US
Security Level 3	\$5,250 US	\$2,250 US
Security Level 4	\$7,250 US	\$3,500 US

Table 4-1: Cost Recovery Fee Schedule

4.6.1 Validation Fee

Validations fees are charged by NIST for the validation tasks and the program management responsibilities performed at NIST by the CMVP. This fee is applicable to all validation reports received by NIST where the vendor has contracted with a CST laboratory after July 18, 2002.

Fees are currently not charged for letter revalidations or revalidations with less than 30% of the security-relevant operational requirements modified. See **Section 4.9.3: Limited Modifications to FIPS 140-2 Assertions**.

The vendor billing information must be entered in CRYPTIK by the CST laboratory and submitted to NIST and CSEC with the CMVP validation test report as described in **Section 4.3: Preparation and Submission of the Validation Submission**.

Note: The validation certificates will not be issued if the invoice for the validation fee has not been paid in full.

4.6.2 Extended Fee

The Extended Fee is applicable when a validation report requires significant additional effort by the reviewers.

The application of the Extended Fee is determined by CMVP policy. The Extended Fee is applicable to:

1. Validation test reports received by NIST CMVP under **Section 4.9.5: New Module** where the vendor has contracted with a CST laboratory after July 18, 2002; and
2. All validation test reports received by NIST CMVP under **Section 4.9: Re-Validation of Cryptographic Modules** (all change scenarios) that are in REVIEW PENDING in the NIST CMVP queue as of October 19, 2006.

The following situations will automatically trigger the Extended Fee:

1. If the report review identified at least one non-compliance to the standard that was not identified by the CST laboratory.
2. If the test report was submitted with a known non-compliance to the standard.
3. If the report In Review took more than two review cycles (i.e. greater than two NIST/CSEC comment replies to a CST laboratory) - this measure is intended to encourage open communications.
4. If the CST laboratory signature page is not received within 30 days of an electronic report submission.
5. A module test report that is received by the CMVP that does not include reference to the underlying validated cryptographic algorithm certificates numbers in TE.01.12.01.

6. If a module test report is sent incomplete (see **Section 4.3: Preparation and Submission of the Validation Submission**), and this is determined once the module has moved to IN REVIEW, the module will be placed on HOLD and NIST Extended Fees will apply. When the incomplete items are received, the module will return to the CMVP queue in REVIEW PENDING at the top of the queue.

Additional specific situations may be added at a later date as significant additional CMVP resources expenditures on report review are identified. The CMVP may impose the Extended Fee for a particular report due to other circumstances not listed above.

4.6.3 CMVP Payment Policy

The current policy regarding payment is that the CMVP will not issue a certificate unless all fees associated with the validation have been paid in full. To ensure timely validation all payments must be received on or before the FINALIZATION stage of the module.

4.7 Partial Validation

The following policy statements have been excerpted from the *Implementation Guidance for FIPS 140-2* Section G.3 – Partial Validations and Not Applicable Areas of FIPS 140-2.

NIST and CSEC will not issue a validation certificate unless the cryptographic module meets at least the Security Level 1 requirements for each area in Section 4 of FIPS 140-2 that cannot be designated as Not Applicable according to the following:

- Section 4.5, Physical Security may be designated as Not Applicable if the cryptographic module is a software-only module and thus has no physical protection mechanisms;
- Section 4.6, Operational Environment may be designated as Not Applicable depending on the module implementation (e.g. if the operational environment for the cryptographic module is a limited operational environment);
- Section 4.11, Mitigation of Other Attacks may be designated as Not Applicable if the vendor has made no claim that the cryptographic module provides such protection mechanisms.

The CST laboratory must provide in the validation test report the rationale for marking any of the aforementioned sections as Not Applicable. If a section is Not Applicable, it will be marked N/A on the module validation certificate. If Section 4.6 is N/A, depending on the module implementation, configuration information may still be required on the module validation certificate.

4.8 Maintaining Validation

The following policy statements have been excerpted from the *Implementation Guidance for FIPS 140-2* Section G.5 – Maintaining validation compliance of software or firmware cryptographic modules.

The tested/validated module version, operational environment upon which it was tested, and the originating vendor are stated on the validation certificate. The certificate serves as the benchmark for the module-compliant configuration.

This guidance addresses two separate scenarios: actions a vendor can affirm or change to maintain a module validation and actions a user can affirm to maintain a module's validation.

This guidance is *not applicable* for validated modules when Section 4.5 Physical Security of FIPS 140-2 has been validated at Level 2 or higher.

4.8.1 Vendor

This section describes actions a vendor can take to change or maintain a module's validation.

4.8.1.1 Recompilation without Source Code Modification

A vendor may perform post-validation recompilations of a software or firmware module and affirm the module's continued validation compliance provided the following is maintained.

1. Software modules that do not require any source code modifications such as changes, additions, or deletions of code, to be recompiled and ported to another operational environment must:
 - For **Level 1 Operational Environment**, a software cryptographic module will remain compliant with the FIPS 140-2 validation when operating on any general purpose computer (GPC) provided that the GPC uses the specified single user operating system/mode specified on the validation certificate, or another compatible single user operating system/mode specified on the validation certificate, or another compatible single user operating system, and
 - For **Level 2 Operational Environment**, a software cryptographic module will remain compliant with the FIPS 140-2 validation when operating on any GPC provided that the GPC incorporates the specified CC evaluated EAL2 (or equivalent) operating system/mode/operational settings or another compatible CC evaluated EAL2 (or equivalent) operating system with like mode and operational settings.
2. Firmware modules (i.e. Operational Environment is *not applicable*) modules that do not require any source code modifications (e.g., changes, additions, or deletions of code) to be recompiled and its identified unchanged tested operating system (i.e. same version or revision number) may be ported together from one GPC or platform to another GPC or platform while maintaining the module's validation.

The CMVP allows vendor porting and re-compilation of a validated software and firmware cryptographic module from the OS(s) and/or GPC(s) specified on the validation certificate to an OS(s) and/or GPC(s) which were not included as part of the validation testing. The validation status is maintained on the new OS(s) and/or GPC without re-testing the cryptographic module on the new OS(s) and/or GPC(s). However, the CMVP makes no statement as to the correct operation of the module when ported to an OS(s) and/or GPC(s) not listed on the validation certificate.

The vendor may provide a new security policy for which would affirm and include references to the new operational environment(s), GPC(s) or platform(s).

4.8.1.2 Recompilation with Non-security Source Code Modifications

Software or firmware modules that require non-security relevant source code modifications such as changes, additions, or deletions of code, to be recompiled and ported to another hardware or operational environment must be reviewed by a CST laboratory and revalidated per **Section 4.9.1: Modifications to Components that Do Not Affect FIPS 140-1 or FIPS 140-2 Components** to ensure that the module does not contain any operational environment-specific or hardware environment-specific code dependencies.

4.8.1.3 Addition of New Operational Environment and/or Platform on Validation Certificate

If the new operational environment and/or platform are requested to be updated on the validation certificate, the CST laboratory shall follow the requirements for non-security relevant changes in **Section 4.9.1: Modifications to Components that Do Not Affect FIPS 140-1 or FIPS 140-2 Components**.

Upon re-testing and validation, the CMVP provides the same assurance as the original operational environment(s) and platform(s) as to the correct operation of the module when ported to the newly listed OS(s) and/or platform(s) operational environments which would be added to the modules validation web entry.

The vendor must meet all applicable requirements in FIPS 140-2 Section 4.10 Design Assurance.

This policy only addresses the operational environment under which a software or firmware module executes and does not affect requirements of the other sections of FIPS 140-2. A module must meet all requirements of the level stated. FIPS 140-2 IG 1.3 – Firmware Designation describes the difference in terminology between software and a firmware module.

4.8.2 Users

This section describes actions a user can take to affirm a module's validation. The term *Users* includes third party integrators or any entity that is not the originating vendor as specified on the validation certificate.

A user may not modify a validated module. Any user modifications invalidate a module's validation.³

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

1. For **Level 1 Operational Environment**, a software cryptographic module will remain compliant with the FIPS 140-2 validation when operating on any general purpose computer (GPC) provided that the GPC uses the specified single user operating system/mode specified on the validation certificate, or another compatible single user operating system, and
2. For **Level 2 Operational Environment**, a software cryptographic module will remain compliant with the FIPS 140-2 validation when operating on any GPC provided that the GPC incorporates the specified CC evaluated EAL2 (or equivalent) operating system/mode/operational settings or another compatible CC evaluated EAL2 (or equivalent) operating system with like mode and operational settings.

The CMVP allows user porting of a validated software cryptographic module on an OS(s) and/or GPC(s) which were not included as part of the validation testing. The validation status is maintained on the new OS(s) and/or GPC without re-testing the cryptographic module on the new OS(s) and/or GPC(s). However, the CMVP makes no statement as to the correct operation of the module when executed on an OS(s) and/or GPC(s) not listed on the validation certificate.

4.9 Re-Validation of Cryptographic Modules

The following policy statements have been excerpted from the *Implementation Guidance for FIPS 140-2* Section G.8 – Revalidation Requirements at <http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402IG.pdf>.

An updated version of a previously validated cryptographic module can be considered for a re-validation rather than a full validation depending on the extent of the modifications from the previously validated

³ A user may post-validation recompile a module if the unmodified source code is available and the modules Security Policy provides specific guidance on acceptable recompilation methods to be followed as a specific exception to this guidance. The methods in the Security Policy must be followed without modification to maintain validation under this guidance.

version of the module. The updated version may be, for example, a new version of an existing crypto module or a new model based on an existing model.

There are five possible change scenarios:

1. Modifications to components that do not affect FIPS 140-2 components;
2. No modifications to the cryptographic module;
3. Limited modifications to FIPS 140-2 assertions;
4. Modifications to the physical enclosure; and
5. New module.

A cryptographic module that is changed under change scenarios 1, 2 and 4 above, must meet ALL standards, implementation guidance and algorithm testing that were met at the time of original validation. A module does not need to continue to meet requirements that were removed or added since the time of original validation.

A cryptographic module that is changed under change scenarios 3 and 5 above, must meet ALL standards, implementation guidance and algorithm testing in effect at the time of module report submission to the CMVP. The CST laboratory is responsible for requesting from the vendor all the documentation necessary to determine whether the cryptographic module meets the current standards and IGs. This is particularly important for features/services of the cryptographic module that required a specific ruling from NIST and CSEC.

For example, a cryptographic module may have been validated with an implementation of Triple-DES that has not been tested. If the same cryptographic module is later submitted for revalidation under scenarios 3 or 5, this Triple-DES implementation must be tested and validated against FIPS 46-3, and the cryptographic module must meet the applicable FIPS 140-2 requirements.

The re-validation scenarios are described in the following sections.

4.9.1 Modifications to Components that Do Not Affect FIPS 140-1 or FIPS 140-2 Components

Modifications are made to hardware, software, or firmware components that do not affect any FIPS 140-1 or FIPS 140-2 security relevant items. The vendor is responsible for providing the applicable documentation to the CST laboratory, which identifies the modification(s). Documentation may include a previous validation report, design documentation, source code, etc. The CST laboratory shall review the vendor-supplied documentation and identify any additional documentation requirements. The CST laboratory shall also determine additional testing as required to confirm that FIPS 140-1 or FIPS 140-2 security relevant items have not been affected by the modification. Upon successful review and applicable testing as required, the CST laboratory shall submit a signed explanatory letter to NIST and CSEC that contains a description of the modification(s) and lists the affected TEs and their associated laboratory assessment. The assessment shall include the analysis performed by the laboratory that confirms that no security relevant items were affected. The letter shall also indicate whether the modified cryptographic module replaces the previously validated module or adds to the latter. If new cryptographic algorithm validation certificates were obtained, they shall be listed. Upon a satisfactory review by NIST and CSEC, the updated version or release information will be posted on the *Validated FIPS 140-1 and FIPS 140-2 Cryptographic Module List* web site entry associated with the original cryptographic module. No new certificate will be issued. It is strongly encouraged that a new security policy be provided for posting that updates the module version number with the new version number.

4.9.2 No Modifications to the Cryptographic Module

No modifications are made to any hardware, software, or firmware components of the cryptographic module. All version information is unchanged. Post validation, Approved security relevant functions or services for which testing was available at the time of validation, or security relevant functions or services that were not tested during the original validation, are now tested and are being submitted for inclusion as a FIPS Approved function or service. The CST laboratory is responsible for identifying the documentation that is needed to determine whether a revalidation is sufficient and the vendor is responsible for submitting the requested documentation to the CST laboratory. Documentation may include a previous validation report and applicable NIST and CSEC rulings, design documentation, source code, etc. The CST laboratory shall identify the assertions affected and shall perform the tests associated with those assertions. This will require the CST laboratory to:

1. Review the COMPLETE list of assertions for the module embodiment and security level;
2. Identify, from the previous validation report, the assertions that are newly tested;
3. Identify additional assertions that were previously tested but should now be re-tested; and
4. Review assertions where specific Implementation Guidance (IG) was provided at the time of the original validation to confirm that the IG is still applicable.

The CST laboratory does not need to perform the regression test suite of operational tests since there is no change to the module. The CST laboratory shall document the test results in the associated assessments and all affected TEs shall be annotated as *re-tested*. The CST laboratory shall submit a delta conformance test report describing the modification and highlighting those assertions that have been newly tested and retested (selecting the re-tested option in CRYPTIK). A new security policy shall be provided for posting that updates the new services or functions that are now included in an Approved mode of operation. Upon a satisfactory review by NIST and CSEC, the updated security policy and information will be posted on the [Validated FIPS 140-1 and FIPS 140-2 Cryptographic Module List](#) web site entry associated with the original cryptographic module. If new cryptographic algorithm validation certificates were obtained, they shall be listed. No new certificate will be issued.

4.9.3 Limited Modifications to FIPS 140-2 Assertions

Modifications are made to hardware, software, or firmware components that affect some of the FIPS 140-2 security relevant items. An updated cryptographic module can be considered in this scenario if it is similar to the original module with only minor changes in the security policy and FSM, and less than 30% of the modules security relevant features. The CST laboratory is responsible for identifying the documentation that is needed to determine whether a re-validation is sufficient and the vendor is responsible for submitting the requested documentation to the CST laboratory. Documentation may include a previous validation report and applicable NIST and CSEC rulings, design documentation, source code, etc. The CST laboratory shall identify the assertions affected by the modification and shall perform the tests associated with those assertions. This will require the CST laboratory to:

1. Review the COMPLETE list of assertions for the module embodiment and security level;
2. Identify, from the previous validation report, the assertions that have been affected by the modification;
3. Identify additional assertions that were NOT previously tested but should now be tested due to the modification; and
4. Review assertions where specific Implementation Guidance (IG) was provided to confirm that the IG is still applicable.

For example, a revision to a firmware component that added security functionality may require a change to assertions in Section 1.

In addition to the tests performed against the affected assertions, the CST laboratory shall also perform the regression test suite of operational tests included in **Annex B: Regression Tests for FIPS 140-2 Validated Cryptographic Modules**

When a cryptographic module is tested for revalidation from FIPS 140-1 to FIPS 140-2, the CST laboratory may re-use information contained in the FIPS 140-1 test report for the preparation of the FIPS 140-2 test report. A mapping table available from NIST or CSEC can be used to guide the tester.

Note: Included in the table are the ASs, TEs, VEs (AS2 for FIPS 140-2 and AS1 for FIPS 140-1, etc.), security level(s), single chip (S), multi chip embedded (ME), multi chip standalone (MS), operational test (Op - x is used for the operational tests, r is used for regression test), applicable to FIPS 140-2 (M - match), and comment (describes the applicability of FIPS 140-1 results to FIPS 140-2, and may include info on the FIPS 140-2 requirement). The CST laboratory shall perform all the operational tests (TEs labelled with an x and an r in the Op field).

The CST laboratory shall document the test results in the associated assessments and all affected TEs shall be annotated as “re-tested” The CST laboratory shall submit a Report Overview with Assessments describing the modification and highlighting those assertions that have been modified and re-tested (selecting the re-tested option in CRYPTIK). Upon a satisfactory review by NIST and CSEC, the updated version will be revalidated to FIPS 140-2 and a new certificate will be issued.

4.9.4 Modifications to the Physical Enclosure

Modifications are made only to the physical enclosure of the cryptographic module that provides its protection and involves no operational changes to the module. The CST laboratory is responsible for ensuring that the change only affects the physical enclosure (integrity) and has no operational impact on the module. The CST laboratory must also fully test the physical security features of the new enclosure to ensure its compliance to the relevant requirements of the standard. The CST laboratory must then submit a letter to NIST and CSEC that:

1. Describes the change (pictures may be required);
2. States that it is a security relevant change;
3. Provides sufficient information supporting that the physical only change has no operational impact; and
4. Describes the tests performed by the laboratory that confirm that the modified enclosure still provides the same physical protection attributes as the previously validated module. For security levels 2, 3 and 4, the submission of an updated Physical Security Test Report is mandatory.

Each request will be handled on a case-by-case basis. The CMVP will accept such letters against cryptographic modules already validated to FIPS 140-1 and FIPS 140-2. No new certificates will be reissued.

An example of such a change could be the plastic encapsulation of the Level 2 token which has been reformulated or colored. Therefore the molding or cryptographic boundary has been modified. This change is security relevant as the encapsulation provides the opacity and tamper evidence requirements. But this can be handled as a change scenario 1 with evidence that the new composition has the same physical security relevant attributes as the prior composition.

4.9.5 New Module

If modifications are made to hardware, software, or firmware components that do not meet the above criteria, then the cryptographic module will be considered a new module and must undergo a full validation testing by a CST laboratory.

If the overall Security Level of the cryptographic module changes, or if the physical embodiment changes, such as from multi-chip standalone to multi-chip embedded, then the cryptographic module will be considered a new module and must undergo full validation testing by a CST laboratory.

4.10 Requests for Guidance to NIST and CSEC

The following policy statements have been excerpted from the *Implementation Guidance for FIPS 140-2* Section G.1 – Request for Guidance from the CMVP.

Programmatic Questions: These are questions pertaining to the general operation of the CMVP. The CMVP suggests reviewing the CMVP Frequently Asked Questions (FAQ), Announcements and Notices posted on the CMVP web site first as the answer may be readily available. The information found on the CMVP web site provides the official position of the CMVP.

Test-specific Questions: These are questions concerning specific test issues of the CMVP. These issues may be technology related or related to areas of the standard that may appear to be open to interpretation.

General Guidance: Questions regarding the CMVP can be directed to either NIST or CSEC by contacting the appropriate points of contact listed below. The complete list of NIST and CSEC addressees shall be included on copy for all questions.

Vendors who are under contract with a CST laboratory for FIPS 140-2 testing of a particular module(s) must contact the contracted CST laboratory for any questions concerning the test requirements and how they affect the testing of the module(s). This allows the laboratory representatives to use their expertise in FIPS 140-2 testing to answer those questions, and to act as a filter for NIST and CSEC.

CST laboratories must submit all test-specific questions in the Request for Guidance (RFG) format described below and to all points of contact.

Federal agencies and departments, and vendors not under contract with a CST laboratory who have specific questions about FIPS 140-2 test requirements or any aspect of the CMVP should contact the appropriate NIST and CSEC points of contact listed below.

Questions can either be submitted by email, telephone, facsimile or written (if an electronic document, Microsoft Word document format is preferred).

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. Replies to informal requests by the CMVP are non-binding and subject to change. It is recommended that informal requests be submitted to all points of contact. Every attempt is made to reply to informal request with accurate, consistent, clear replies in a timely manner.

Official Request: If an official response is requested, then an official request must be submitted to the CMVP written in the RFG format described below. An official response requires internal review by both NIST and CSEC, as well as with others as necessary, and may require follow-up questions from the CMVP. Therefore the official response to such requests may not be immediate.

Request for Guidance (RFG) Format: Questions submitted in this format will result in an official response from the CMVP that will state current policy or interpretations. This format provides the CMVP a clear understanding of the question. A 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 cryptographic algorithmic standards,
8. Background information if applicable, including any previous CMVP 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 a detailed and implementation-specific format, rather than an academic or hypothetical format. This information should also include a brief non-proprietary description of the implementation and the FIPS 140-2 target security level. This will enable a more efficient and timely resolution of FIPS 140-2 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 its 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 the Implementation Guidance to FIPS 140-2 and the Cryptographic Module Validation Program. Note that general questions may still be submitted, but these questions should be identified as not being associated with a particular validation effort.

Questions should be non-proprietary, as the response will be distributed to *all* CST laboratories. Distribution may be restricted on a case-by-case basis.

RFGs from CST laboratories are placed in a queue. Responses to the RFGs are coordinated and agreed upon by both CSEC and NIST. RFGs should be addressed to all of the following contacts:

NIST CMVP

Randall J. Easter
(301) 975-4641
reaster@nist.gov

CSEC CMVP

Jean Campbell
(613) 991-8121
jean.campbell@cse-cst.gc.ca

Allen Roginsky

(301) 975-3603
allen.roginsky@nist.gov

Ken Lu

(613) 991-8122
ken.lu@cse-cst.gc.ca

4.11 Request for Transition Period Extension

Some Implementation Guidance is assigned a transition period before compliance to this guidance is required because 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.

4.12 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, CSEC and the CST laboratory will investigate the allegation about the flaw, and determine its impact on the validation;
2. NIST and CSEC will decide whether or not 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 CSEC may advise their respective federal departments of the flaw and its impact; and
4. NIST and CSEC may notify NVLAP about the possible shortfall with the CST laboratory's proficiency.

The diagram found at **Annex C: Flaw Discovery Handling Process Diagram** describes the flaw discovery handling process in detail.

4.13 Validation Revocation

FIPS 140-1 and FIPS 140-2 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 140-1 and FIPS 140-2 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 140-1 or 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.

4.14 CMVP Webpage Update

This section provides information about the CMVP website.

4.14.1 Official CMVP Website

The official CMVP website with all current publicly-available information on the Cryptographic Module Validation Program is <http://csrc.nist.gov/groups/STM/index.html>.

Limited information about the CMVP is provided as part of Industry Program section of CSEC website at <http://www.cse-cst.gc.ca/cmvp>. The CSEC information is not necessarily up-to-date.

4.14.2 FIPS 140-1 and FIPS 140-2 Cryptographic Module Validation Lists

The official CMVP website has the following lists related to the validation of cryptographic modules to FIPS 140-1 and FIPS 140-2:

- *FIPS 140-1 and FIPS 140-2 Cryptographic Module Validation Lists* – a single overall list plus separate lists for validations completed in a specific year or years
- *FIPS 140-1 and FIPS 140-2 Modules In Process*
- *FIPS 140-1 and FIPS 140-2 Vendor List*

4.14.3 CMVP Vendor Product Link

On May 20, 2003, the CMVP instituted an optional web link entry on the *Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules List*. The purpose of this web link is for vendors to provide a concise listing of 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 aid make it easier for potential customers and users to identify products that use cryptographic modules validated at FIPS 140-1 or FIPS 140-2.

The web page at the vendor provided URL is to be 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.

An information sheet on this CMVP Vendor Product Link is provided to the vendor with each issued cryptographic module validation certificate.

4.14.4 Changes to Vendor, Module Name or Version Information

A CST laboratory must send to NIST and CSEC a signed letter requesting vendor name changes, changes to the module name, or changes to any versioning information. This letter must assert that the CST laboratory has verified the legal vendor name change, if a module name change, that the new named module is identically the same as the old named module, and if a versioning change, that the change does not reflect any actual change to the module (e.g. simply a change in the vendor's release and delivery process).

If the vendor's contact information changes, such as address, telephone, fax, or point-of-contact, or the vendor also request changes to the module description field, the vendor or CST laboratory can send an e-mail or a request letter to NIST and CSEC requesting the validation list update.

4.14.5 Security Policy Updates

Any new or updated security policies must be submitted to NIST and CSEC for replacement of the existing posted security policy by a CST laboratory. If functional or technical content is changed, a CST laboratory must review and submit to NIST and CSEC for review and update.

4.14.6 Update Frequency of Validation Lists

4.14.6.1 FIPS 140-1 and FIPS 140-2 Cryptographic Module Validation List

This list is updated when new FIPS 140-2 validation certificates are signed for a cryptographic module or group of cryptographic modules, when FIPS 140-1 or FIPS 140-2 validations are extended to new versions of the cryptographic module through a letter re-validation request as described in **Section 4.9: Re-Validation of Cryptographic Modules**, or when a change is requested in the web entry information

such as the Point of Contact or the Vendor's Name as described in **Section 4.14.4: Changes to Vendor, Module Name or Version Information** .

4.14.6.2 FIPS 140-1 and FIPS 140-2 Modules In Process

This list is updated and posted weekly.

4.14.6.3 FIPS 140-1 and FIPS 140-2 Vendor List

This list is updated when new validation certificates are signed for cryptographic modules or when a name change for a vendor is requested. The update may be just providing links to the new certificates issued for the vendor or adding a vendor and their certificate(s) to the list if this is the first time the vendor has received a validation certificate to FIPS 140-2 for one of their cryptographic modules.

If the vendor's name is changed, the entry for the vendor in the *FIPS 140-1 and FIPS 140-2 Vendor List* will reference the previous name of the vendor and will include links to all the certificates issued for the particular vendor.

4.15 Usage of FIPS 140-1 and FIPS 140-2 Logos

The following are the guidelines for the use of the FIPS 140-1 and 140-2 logos. The phrases *FIPS 140-1 Validated* and *FIPS 140-2 Validated* and the FIPS 140-1 and FIPS 140-2 logos are intended for use in association with cryptographic modules validated by the National Institute of Standards and Technology (NIST) and the Communications Security Establishment Canada (CSEC) as complying with FIPS 140-1 or FIPS 140-2, *Security Requirements for Cryptographic Modules*. Vendors with cryptographic modules that have been validated by NIST and CSEC may use the phrase and logo provided that they agree in writing to the following:

1. The phrases *FIPS 140-1 Validated* and *FIPS 140-2 Validated* and the FIPS 140-1 and FIPS 140-2 Logos are Certification Marks of NIST, which retains exclusive rights to their use.
2. NIST reserves the right to control the quality of the use of the phrases *FIPS 140-1 Validated* and *FIPS 140-2 Validated*, and the logos themselves.
3. Permission for advertising FIPS 140-1 and FIPS 140-2 validation and use of the logos are conditional on and limited to those cryptographic modules validated by NIST and CSEC as complying with FIPS 140-1 or FIPS 140-2.
4. A cryptographic module may either be a component of a product, or a standalone product. Use of the FIPS 140-1 and FIPS 140-2 logos on product reports, letterhead, brochures, marketing material, and product packaging must be accompanied by the following: ***TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S., or Canadian Governments.*** If the cryptographic module is a component of a product, the phrase ***FIPS 140-1 Inside*** or ***FIPS 140-2 Inside*** must accompany the logo.
5. Permission for the use of the phrases *FIPS 140-1 Validated* and *FIPS 140-2 Validated* and the logos may be revoked at the discretion of NIST.
6. Permission to use the phrases *FIPS 140-1 Validated* and *FIPS 140-2 Validated*, and the FIPS 140-1 and FIPS 140-2 logos in no way constitutes or implies product endorsement by NIST or CSEC.
7. Photographic and electronic copies of the logo are available from NIST upon request.

The *Guidelines for the Use of the FIPS 140-1 Logo* or *Guidelines for the Use of the FIPS 140-2 Logo* forms are provided to the vendor by NIST with the cryptographic module validation certificate. See

Annex D: Guidelines for the Use of the FIPS 140-1 Logo and **Annex E: Guidelines for the Use of the FIPS 140-2 Logo** for a copy of these guidelines. The appropriate form must be completed, signed and returned to NIST for each validation certificate issued. Multiple certificate numbers may be included on a single form. Submission of the form by a vendor for one certificate does not allow use of the logos for other certificates that may have been issued.

The FIPS 140-1 and FIPS 140-2 logos can be used on product literature even if the cryptographic module is not a product; however, the phrase ***FIPS 140-1 Inside™*** or ***FIPS 140-2 Inside™*** must be included. There is no assurance that a product is correctly utilizing an embedded validated cryptographic module as this is outside the scope of the FIPS 140-1 or FIPS 140-2 validation.

CST laboratories, subject to their NVLAP accreditation, may use the NVLAP, CMVP, and FIPS 140-1 and 140-2 logos. Use of the logos shall be specified in the *CST Laboratories Quality Manual* documentation. Use of the FIPS 140-1 and FIPS 140-2 logos shall follow the same CMVP logo use guidelines as appropriate and indicated in the CST laboratory quality manual documentation.

5 CMVP and CAVP Programmatic Metrics Collection

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

5.1 Overview

The CMVP Programmatic Metrics Collection process is intended to document the quality performance of the testing and validation processes of the CMVP and to allow the program to evaluate its relevance within the government.

To achieve these objectives various metrics are collected through the testing and validation processes of the CST laboratories and the CMVP. These metrics are intended to identify general programmatic trends and not to measure individual laboratory or vendor performances.

5.2 Confidentiality of the Collected Metrics Data

The CMVP considers the data collected and reported by the individual CST laboratories as proprietary. The statistical information derived from the collected data is considered to be non-proprietary.

5.3 Collected Metrics

The following CMVP metrics will be collected by each CST laboratory for modules that have been validated or re-validated, refer to [Section 4.9 Re-Validation of Cryptographic Modules](#).

- CMVP TID number;
- Vendor and cryptographic module name;
- Certificate number;
- Validation date;
- FIPS 140-2 or FIPS 140-3 validation;
- FIPS 140-2 or FIPS 140-3 overall security level attained;
- Type of validation;
- Type of module;
- Determination whether the vendor already has a validated module;
- Determination whether the module has been modified due to a Physical Security non-conformance;
- Determination whether the module has been modified due to a Key Management non-conformance;
- Determination whether the module has been modified due to a Self-Test non-conformance;
- Determination whether the module has been modified due to other non-conformance; and
- Determination whether the module's overall documentation has been modified, except the Security Policy

The CST laboratory uses the METRIX tool to collect the aforementioned metrics.

5.4 Reported Metrics

While the metrics collected by the CST laboratory pertain to each validation certificate, the information reported to the CMVP does not identify any vendor. The information reported to the CAVP/CMVP is an aggregate result of all cryptographic modules validated during the specified period.

The CST laboratory, using the METRIX tool, provides the following metrics for a specified period:

- The number of cryptographic module validation certificates that were issued
- The number of cryptographic modules with at least one non-conformance, excluding the documentation non-conformances
- The number of modules with documentation non-conformances
- The total number of modules that have been modified due to:
 - Physical Security non-conformances;
 - Key Management non-conformances;
 - Self-Test non-conformances; and
 - Other module non-conformances

5.5 Metrics Reporting

The CST laboratory will provide the required reported metrics to the CMVP semi-annually, typically in May or November, or as required by the CMVP.

The CMVP will provide the laboratory the following information for each query that the laboratory has to execute:

- Query Number;
- Query Type;
- Query Start Date; and
- Query End Date

The laboratory shall use the METRIX tool, perform the queries required by the CMVP and send the reporting data to the CMVP. For each query performed, the laboratory has to send to the CMVP a query file and a signed report in pdf format.

The query file is automatically created by the METRIX tool and the file name has the following structure:

[NVLAP Lab Code]-[QueryNumber]-#[DateWhenQueryWasExecuted]#.qry

The query report is created by the METRIX tool. The report has to be signed by the laboratory Approved signatory and scanned to a pdf format following the following file naming convention:

[NVLAP Lab Code]-[QueryNumber_Report]-#[DateWhenQueryWasExecuted]#.pdf

5.6 Reporting Deferral

The laboratory can choose to export the results of a query or to defer the reporting. For both options: export or defer, the laboratory shall use the METRIX tool, and send to the CMVP the query file(s) and the signed report(s). If the laboratory chooses to defer the submission of the reporting data to the subsequent reporting period, the laboratory has to provide the reason for the deferral. Typically the deferral option

should be used when the laboratory has insufficient data and the laboratory considers that the anonymity of the vendor or cryptographic module can not be preserved.

5.7 Metrics Submission

The CMVP metrics shall be included into a single zip file, encrypted for all NIST and CSEC reviewers, and e-mailed to:

- CMVP@nist.gov
- CMVP@cse-cst.gc.ca

Normally the CMVP will request the laboratory to perform the CAVP and CMVP queries at the same time, and for the same period of time. The CAVP and CMVP metrics shall be included in the same zip file.

5.8 Metrics Retention and Audit

The CST laboratory shall retain the collected metrics. The CST laboratory collection process and data are auditable items during the NVLAP on-site assessment.

5.9 METRIX Collection Tool

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

5.10 METRIX Repository Tool

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

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 Publication)

As with all FIPS, FIPS 140-2 (and subsequent Pub) is to be reviewed every five years.

Review begins with the public request for comments on the current version of the standard. Suggested new requirements for the FIPS 140-2 (and subsequent Pub) are also welcomed. Comments and suggested changes are solicited through a Federal Register publication at URL:

<http://www.gpoaccess.gov/fr/index.html>. As well, a Federal Register publication with a CMVP announcement such as the revision of the FIPS 140-2 publication will also be posted on the official CMVP website under Notices at URL: <http://csrc.nist.gov/groups/STM/cmvp/notices.html>. CST laboratories will be kept apprised through emails and meetings of developments in the revision of the standard.

After the comment period has closed, NIST and CSEC take time to review the comments. A revision of the FIPS 140-2 may be undertaken based upon the following factors:

1. Advancements in technology and security measures;
2. Newly devised attacks on cryptographic technology;
3. Implementation guidance issued on previous version of FIPS 140-1 (and subsequent Pub);
4. Advancements in related standards; and
5. Comments from Validation Authorities, CST laboratories, cryptographic module vendors, cryptographic module users, standards bodies, and other interested parties.

The revised FIPS 140-3 publication (and subsequent Pub) will be thoroughly reviewed and officially ratified by the U.S. Secretary of Commerce. The corresponding Derived Test Requirements for the revised FIPS 140-3 (and subsequent Pub) will be developed by NIST and CSEC.

Responsible Positions: Director NIST CMVP and Head of CSEC CMVP.

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 after the received comments are addressed.

In both cases, the final publication is posted on the CMVP official web site (<http://csrc.nist.gov/groups/STM/cmvp/index.html>) in the appropriate section and on various NIST web sites under the publication type (<http://csrc.nist.gov/publications/index.html>) and the cryptographic algorithm type (<http://csrc.nist.gov/groups/ST/toolkit/>).

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 and CAVP official websites, and implemented.

FIPS cryptographic algorithm publications are posted on the web page for the particular cryptographic algorithm type.

Responsible Positions: Assigned individuals in NIST Security 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 potentially solicited from the CST laboratories.

If there are any inconsistencies with the FIPS 140-x, errors in the DTR, new test methods need to be added or test methods need to be updated, the DTR will be updated in a timely manner. If any Change Notices are issued for the FIPS 140-x, the DTR will be updated as soon as possible. CST laboratories will be notified about the upcoming Change Notices and DTR changes prior to their publication. The CRYPTIK tool will also be updated and released to the CST laboratories in response to changes in the DTR.

The DTR document is designated as *Draft* to allow it to be updated as necessary. The DTR document for the particular FIPS 140-x is published on the same web page as the FIPS 140-x to which it applies.

Responsible Positions: Director NIST CMVP and Head CSEC CMVP.

6.4 Implementation Guidance

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

NIST and CSEC 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.

A new Implementation Guidance document is created and posted when the FIPS 140-3 is promulgated. Implementation Guidance entries from the previous document that are also applicable to the revised FIPS 140-3 are included in this new document.

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

Responsible Position: Director NIST CMVP and Head CSEC CMVP.

6.5 FAQ for the CMVP

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

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

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

Responsible Position: Director NIST CMVP and Head CSEC CMVP.

6.6 Test Tools

6.6.1 CRYPTIK

A major version (primary number changed) of the CRYPTIK test tool is created and released to CST laboratories on an annual basis. Suggestions for new features or functionality for the tool are solicited from the CST laboratories and the CMVP Validation Authorities prior to the development of the release. A major version of the CRYPTIK test tool is created and released to the CST laboratories when a DTR for a new FIPS 140-*x* comes into effect. As well, a minor (decimal number changed) version of the CRYPTIK test tool may be created and released to CST laboratories if the current DTR is modified or an error is discovered in the tool. A summary of the changes made for the released version of the CRYPTIK tool accompany the tool.

New versions of the CRYPTIK tool are to be used immediately for ongoing as well as future FIPS 140-*x* validation projects since database files can be exported from the previous version of the tool and imported into the new version.

Responsible Individual: Director NIST CMVP.

6.6.2 METRIX Collection Tool

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

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

Responsible position: Head CSEC CMVP

6.6.3 METRIX Repository Tool

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

Responsible position: Head CSEC CMVP

6.7 CST Laboratory Accreditation Standards

6.7.1 Handbook 150 – Procedures and General Requirements

It is essential for the mutual recognition of NVLAP-accredited laboratories by other laboratory accreditation bodies that NVLAP procedures maintain their consistency with international standards and guidelines. NVLAP signs Mutual Recognition Arrangement (MRA) or Multilateral Recognition Arrangement (MLA) agreements for organizations of laboratory accreditation bodies such as the International Laboratory Accreditation Cooperation (ILAC) group, the Asia Pacific Laboratory Accreditation Cooperation (APLAC) group, the Inter American Laboratory Accreditation Cooperation (IAAC) group, the European co-operation for Accreditation (EA) association, and the National Cooperation for Laboratory Accreditation (NACLA) group. Specifically, NVLAP procedures must be consistent with in the current version of ISO/IEC 17025: *General Requirements for the Competence of Testing and Calibration Laboratories* and ISO/IEC Guide 58: *Calibration and Testing Laboratory Accreditation Systems - General Requirements for Operation and Recognition*. Since these procedures are contained in Handbook 150, this Handbook must be updated as necessary. Handbook 150 may also 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 <http://ts.nist.gov/Standards/Accreditation/upload/nist-handbook-150.pdf> and distributed to the NVLAP-accredited laboratories after publication.

Responsible Position: Chief of NVLAP.

6.7.2 Handbook 150-17 – Cryptographic and Security Testing

Handbook 150-17, as the program specific handbook for Cryptographic and Security Testing, is revised when there is a perceived need for its update identified by the Director of the NIST CMVP or the Program Manager for Information Technology Security Testing. 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 not available on-line.

Responsible Position: Program Manager, Information Technology Security Testing.

6.7.3 CAN-P-4E – General Requirements for the Competence of Testing and Calibration Laboratories

CAN-P-4E, *General Requirements for the Competence of Testing and Calibration Laboratories* is a verbatim Canadian adoption of ISO/IEC 17025: *General Requirements for the Competence of Testing and Calibration Laboratories*. It is essential for the mutual recognition of Standards Council of Canada (SCC)-accredited laboratories by other laboratory accreditation bodies that SCC procedures maintain their

consistency with international standards and guidelines. SCC has signed Multilateral Recognition Arrangement (MLA) or Mutual Recognition Arrangement (MRA) agreements for organizations of laboratory accreditation bodies such as the International Accreditation Forum, Inc. (IAF), International Laboratory Accreditation Cooperation (ILAC) group, the Asia Pacific Laboratory Accreditation Cooperation (APLAC) group, the Inter American Laboratory Accreditation Cooperation (IAAC) group, and the National Cooperation for Laboratory Accreditation (NACLA) group. SCC is also working to obtain recognition of its laboratory accreditation systems by the European co-operation for Accreditation (EA) association. If ISO/IEC 17025 is updated, CAN-P-4E will also be updated.

Responsible Organizations: Standards Council of Canada Working Group and Communications Security Establishment Canada.

6.7.4 CAN-P-1591B – Guidelines for the Accreditation of Information Technology Security Evaluation and Testing Facilities

CAN-P-1591B, *Guidelines for the Accreditation of Information Technology Security Evaluation and Testing Facilities* has been created by the Standards Council of Canada to be a framework for the accreditation within Canada of ITS Evaluation and Testing (ITSET) facilities. CAN-P-1591B (ITSET) is a specific guideline document that amplifies CAN-P-4E, *General Requirements for the Competence of Testing and Calibration Laboratories*.

The purpose of CAN-P-1591B is to establish requirements, in addition to those specified in CAN-P-4E, for the technical and organizational matters for the SCC accreditation of facilities for performing IT security evaluation and testing. Cryptographic module and cryptographic algorithm testing is one of the IT security specialization areas for ITSET laboratories.

CAN-P-1591B may be revised as new IT security specialization areas are added to the current list of specialization areas in it. CAN-P-1591B is published on the Standards Council of Canada website at http://www.scc.ca/Asset/iu_files/criteria/1591b_e.pdf

Responsible Organizations: Standards Council of Canada Working Group and Communications Security Establishment Canada.

6.7.5 CAN-P-1621 – Requirements for the Accreditation of Cryptographic Module and Algorithm Testing Facilities

CAN-P-1621, *Requirements for the Accreditation of Cryptographic Module and Algorithm Testing Facilities* presents the specific requirements of the Standards Council of Canada for Canadian testing facilities seeking accreditation for the conformance testing of cryptographic modules and cryptographic algorithms to FIPS 140-2 *Security Requirements for Cryptographic Modules*. The generic testing facility requirements specified in Handbook 150 and Handbook 150-17 were identified and mapped to the requirements specified in the PALCAN Handbook, *Program Requirements for Applicants and Accredited Laboratories*, CAN-P-4E, and CAN-P-1591B. The remaining requirements specific to cryptographic module and algorithm testing were grouped in CAN-P-1621. The requirements specified in CAN-P-4E, CAN-P-1591B and CAN-1621 map to all the requirements specified in NIST Handbook 150 and NIST Handbook 150-17.

The purpose of CAN-P-1621 is to establish requirements, in addition to those specified in CAN-P-4E and in CAN-P-1591B, for technical and organizational matters for the SCC accreditation of testing facilities to perform the conformance testing of cryptographic modules to FIPS PUB 140-2, *Security Requirements for Cryptographic Modules* and the conformance testing of the associated cryptographic algorithms. CAN-P-1621 is published on the Standards Council of Canada website at http://www.scc.ca/Asset/iu_files/criteria/1621_e.pdf

Since CAN-P-1621 has requirements that map to NIST Handbook 150-17, it is expected that when a revision is published for NIST Handbook 150-17, CAN-P-1621 will also be revised and published on the Standards Council of Canada website.

Responsible Organizations: Standards Council of Canada Working Group and Communications Security Establishment Canada.

6.8 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: Director NIST CMVP and Head CSEC CMVP.

Annex A: Code Convention (Tracking Identification Numbers)

In order to accomplish uniformity and improve throughput time, all e-mail transmitted to the CMVP pertaining to processing requests must abide by the conventions specified below:

1. Submission Number

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

Field1 – nn-aaaa [7 character field] where
 nn = 2 digit CST Lab code [see assignments below]
 hyphen separator
 aaaa = 4 character alphanumeric [A-Z,a-z,0-9] CST Lab assigned TID

nn	Lab	nn	Lab	nn	Lab	nn	Lab
01	InfoGard	06	EWA	11	Atsec	16	ITSEL
02	CEAL	07	Not in use	12	ICSA Labs	17	ECSEC
03	DOMUS ITSL	08	BT	13	SAIC	18	Epoche & Espri
04	COACT	09	TÜViT	14	Not in use	19	Unassigned
05	Atlan	10	Aspect	15	ÆGISOLVE	20	Unassigned

Field2 – 4 digit CSEC TID number (= 0000 if not assigned)
OR - 4 characters “ITAR” (for ITAR reports not processed by CSEC).

2. Transaction Code

Field3 – 4 character email tag as defined below:

Modules In Process Activities:

- IUTA – Add module to IUT list
- IUTR – Remove module from the IUT list
- IUTM – Modify IUT entry

Report Submission: (Scenarios 1,2,3,4 or 5 – s=scenario number) See Table below.

- sSUB – Initial submission
- sHLD – Place module HOLD
- sNSn – NIST comments (n=number of times CMVP comments sent to the CST Lab, n=0 if not sent to Lab)
- sCSn – CSEC comments (n=number of times CMVP comments sent to the CST Lab, n=0 if not sent to the Lab)
- sCMn – nth set of CMVP comments (n=3, NIST ECR Applies)

s	Scenario Description	Paragraph
1	Letter Re-validation	4.9.1
2	Test Report – No Modification	4.9.2
3	Re-validation	4.9.3
4	Letter Re-validation – Physical	4.9.4
5	New Submission	4.9.5

Finalization Activities:

- FAOK – Transmittal of All OK and draft certificate
- FCLC – Lab response to certificate generation
- FECT – Transmittal of electronic certificate
- FNCS – NIST response to certificate generation
- FVCN – Assignment of validation certificate number
- FWPE – Web posting of electronic certificate
- FWPH – Web posting of hard copy certificate

Miscellaneous:

- ASSG – Assigned CSEC ID
- DRPT – Drop Report
- RQFG – Request for Guidance
- OTHR – Other cases

3. Miscellaneous Fields

- Field4** – vendor name (10 alphanumeric character maximum)
- Field5** – 6 character date of request submittal (format: yymmdd)
- Field6** – Vn - Version number – where n is incremented each time the contents of the file is modified
- Field7** – Certificate number for Scenarios 1, 2, or 4
- Field8** - optional field (OK for OK comments, AOK for All OK comments)

Instituting this convention for email transmittal, will allow the CMVP to forward the request to the appropriate personnel for processing, track the number and type of requests submitted per CST laboratory, and maintain the transmitted data in a more organized manner for data reference and archival.

4. ZIP File Naming Format

Submission documents are contained within a zip file. The name of the zip file abides to the aforementioned naming convention. The files within the zip file abide to the following naming convention.

For scenarios 2, 3 and 5

- TID-00-0000-0000-140crtxxx.doc.....the draft certificate in Word format
- TID-00-0000-0000-140spxxxx.pdf.....the security policy in PDF
- TID-00-0000-0000-report.pdf.....the test report contains the documents described in paragraphs 2, 3 and 4 of [Section 4.3 Test Report Submission](#)
- TID-00-0000-0000_vendor.txt.....module information in ASCII format

For scenarios 1, 2 and 4

For Re-Validation Letters

- TID-00-0000-0000-re-validation-change-letter.doc
- TID-00-0000-0000-re-validation-change-letter.pdf

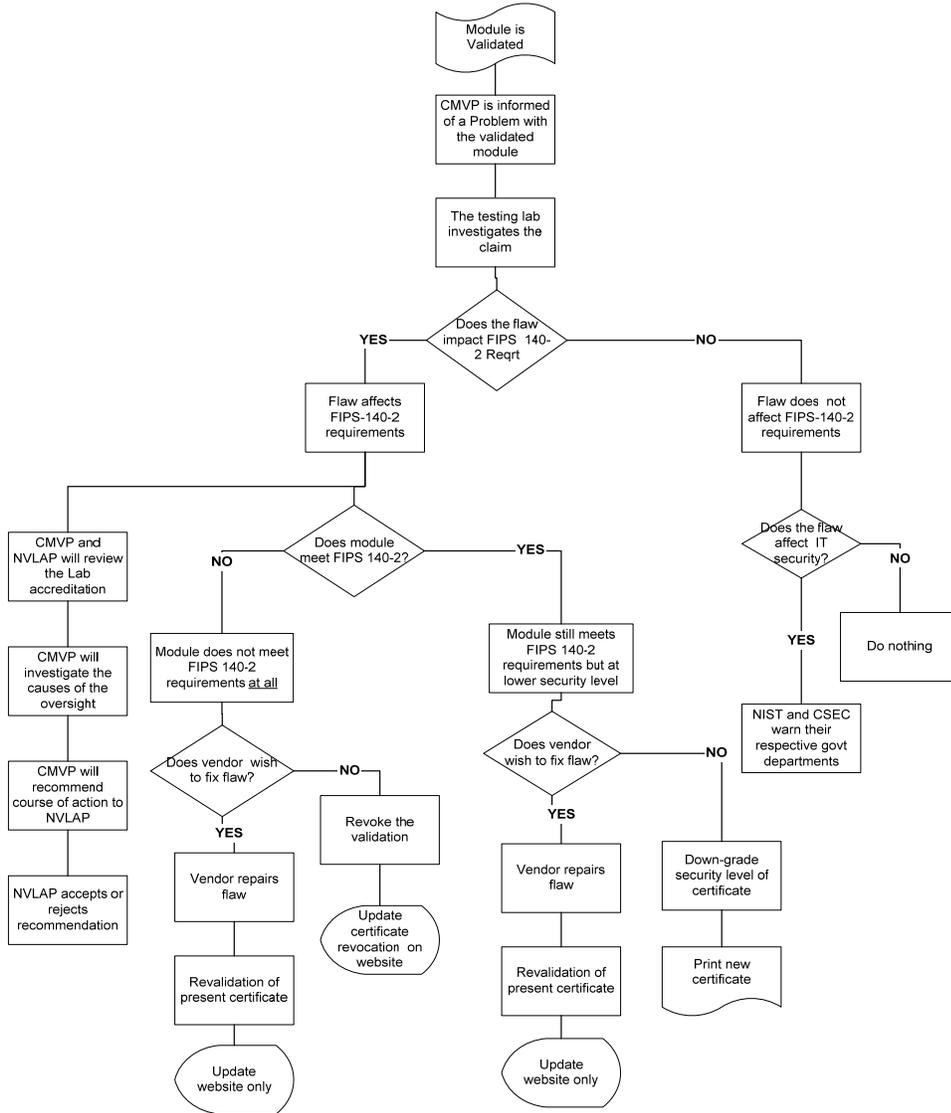
Annex B: Regression Tests for FIPS 140-2 Validated Cryptographic Modules

AS	TE	Security Level			
		1	2	3	4
Section 1 - Cryptographic Module Specification					
AS01.03	TE.01.03.02	x	x	x	x
Section 2 - Cryptographic Module Ports and Interfaces					
AS02.06	TE02.06.02	x	x	x	x
	TE02.06.04	x	x	x	x
AS02.13	TE02.13.03	x	x	x	x
AS02.14	TE02.14.02	x	x	x	x
AS02.16	TE02.16.02			x	x
AS02.17	TE02.17.02			x	x
Section 3 - Roles, Services and Authentication					
AS03.02	TE03.02.02	x	x	x	x
	TE03.02.03	x	x	x	x
AS03.12	TE03.12.03	x	x	x	x
AS03.13	TE03.13.02	x	x	x	x
AS03.14	TE03.14.02	x	x	x	x
AS03.15	TE03.15.02	x	x	x	x
AS03.17	TE03.17.02		x		
AS03.18	TE03.18.02		x		
AS03.19	TE03.19.02			x	x
	TE03.19.03			x	x
AS03.21	TE03.21.02	x	x	x	x
AS03.22	TE03.22.02		x	x	x
AS03.23	TE03.23.02	x	x	x	x
Section 4 - Finite State Model					
AS04.03	TE.04.03.01	x	x	x	x
AS04.05	TE04.05.08	x	x	x	x
Section 5 - Physical Security					
	NONE				
Section 6 - Operational Environment					
AS06.05	TE06.05.01	x			
AS06.06	TE06.06.01	x			
AS06.07	TE06.07.01	x	x	x	x
AS06.08	TE06.08.02	x	x	x	x

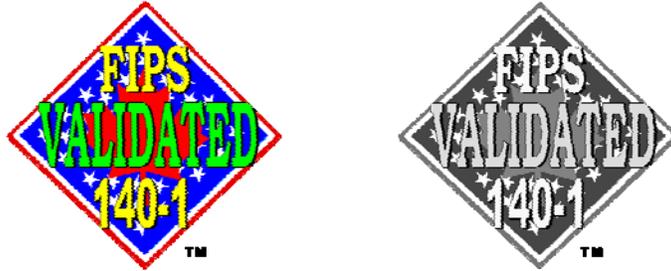
AS	TE	Security Level			
		1	2	3	4
AS06.11	TE06.11.02		x	x	x
	TE06.11.03		x	x	x
AS06.12	TE06.12.02		x	x	x
	TE06.12.03		x	x	x
AS06.13	TE06.13.02		x	x	x
	TE06.13.03		x	x	x
AS06.14	TE06.14.02		x	x	x
	TE06.14.03		x	x	x
AS06.15	TE06.15.02		x	x	x
AS06.16	TE06.16.02		x	x	x
AS06.17	TE06.17.02		x	x	x
AS06.22	TE06.22.02			x	x
	TE06.22.03			x	x
AS06.24	TE06.24.02			x	x
	TE06.24.03			x	x
AS06.25	TE06.25.02			x	x
Section 7 - Cryptographic Key Management					
AS07.01	TE07.01.02	x	x	x	x
AS07.02	TE07.02.02	x	x	x	x
AS07.15	TE07.15.02	x	x	x	x
	TE07.15.03	x	x	x	x
	TE07.15.04	x	x	x	x
AS07.25	TE07.25.02	x	x	x	x
AS07.27	TE07.27.02	x	x	x	x
AS07.28	TE07.28.02	x	x	x	x
AS07.29	TE07.29.02	x	x	x	x
AS07.31	TE07.31.04			x	x
AS07.39	TE07.39.02	x	x	x	x
AS07.41	TE07.41.02	x	x	x	x
Section 8 - EMI / EMC					
	As Required				
Section 9 - Self Tests					
AS09.04	TE09.04.03	x	x	x	x
AS09.05	TE09.05.03	x	x	x	x
AS09.09	TE09.09.02	x	x	x	x

AS	TE	Security Level			
		1	2	3	4
AS09.10	TE09.10.02	x	x	x	x
AS09.12	TE09.12.02	x	x	x	x
AS09.22	TE09.22.07	x	x	x	x
AS09.35	TE09.35.05	x	x	x	x
AS09.40	TE09.40.03	x	x	x	x
	TE09.40.04	x	x	x	x
AS09.45	TE09.45.03	x	x	x	x
AS09.46	TE09.46.03	x	x	x	x
Section 10 - Design Assurance					
AS10.03	TE10.03.02	x	x	x	x
Section 11 - Mitigation of Other Attacks					
	NONE				
Appendix C - Cryptographic Module Security Policy					
	As Required				

Annex C: Flaw Discovery Handling Process Diagram



Annex D: Guidelines for the Use of the FIPS 140-1 Logo



The phrase *FIPS 140-1 Validated* and the FIPS 140-1 Logo are intended for use in association with cryptographic modules validated by the National Institute of Standards and Technology (NIST) and the Communications Security Establishment Canada (CSEC) as complying with FIPS 140-1, *Security Requirements for Cryptographic Modules*. Vendors with cryptographic modules that have been validated by NIST and CSEC may use the phrase and logo provided that they agree in writing to the following:

1. The phrase *FIPS 140-1 Validated* and the FIPS 140-1 Logo are Certification Marks of NIST, which retains exclusive rights to their use.
2. NIST reserves the right to control the quality of the use of the phrase *FIPS 140-1 Validated* and the logo itself.
3. Permission for advertising FIPS 140-1 validation and use of the logo is conditional on and limited to those cryptographic modules validated by NIST and CSEC as complying with FIPS 140-1.
4. A cryptographic module may either be a component of a product, or a standalone product. Use of the FIPS 140-1 Logo on product reports, letterhead, brochures, marketing material, and product packaging must be accompanied by the following: ‘TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S. or Canadian Governments’. If the cryptographic module is a component of a product, the phrase “FIPS 140-1 Inside” must accompany the logo.
5. Permission for the use of the phrase *FIPS 140-1 Validated* and the logo may be revoked at the discretion of NIST.
6. Permission to use the phrase *FIPS 140-1 Validated* and the FIPS 140-1 Logo in no way constitutes or implies product endorsement by NIST or CSEC.
7. Photographic and electronic copies of the logo are available from NIST upon request.

Signature below acknowledges full agreement with the above conditions for the use of the phrase *FIPS 140-1 Validated* and the FIPS 140-1 Logo. Use of the phrase and logo as specified above may begin upon receipt of the original signed validation certificate. A signed form is required for each validated cryptographic module.

Signature: _____ Date: _____
Printed Name: _____
E-mail ID: _____
Title: _____
Company: _____
FIPS 140-1 Certificate
Number(s): _____

Return signed form to: Beverly Trapnell, NIST, 100 Bureau Drive, Suite 8930, Gaithersburg, MD 20899

TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S. or Canadian Governments.

Annex E: Guidelines for the Use of the FIPS 140-2 Logo



The phrase *FIPS 140-2 Validated* and the FIPS 140-2 Logo are intended for use in association with cryptographic modules validated by the National Institute of Standards and Technology (NIST) and the Communications Security Establishment Canada (CSEC) as complying with FIPS 140-2, *Security Requirements for Cryptographic Modules*. Vendors with cryptographic modules that have been validated by NIST and CSEC may use the phrase and logo provided that they agree in writing to the following:

1. The phrase *FIPS 140-2 Validated* and the FIPS 140-2 Logo are Certification Marks of NIST, which retains exclusive rights to their use.
2. NIST reserves the right to control the quality of the use of the phrase *FIPS 140-2 Validated* and the logo itself.
3. Permission for advertising FIPS 140-2 validation and use of the logo is conditional on and limited to those cryptographic modules validated by NIST and CSEC as complying with FIPS 140-2.
4. A cryptographic module may either be a component of a product, or a standalone product. Use of the FIPS 140-2 Logo on product reports, letterhead, brochures, marketing material, and product packaging must be accompanied by the following: ‘TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S. or Canadian Governments’. If the cryptographic module is a component of a product, the phrase “FIPS 140-2 Inside” must accompany the logo.
5. Permission for the use of the phrase *FIPS 140-2 Validated* and the logo may be revoked at the discretion of NIST.
6. Permission to use the phrase *FIPS 140-2 Validated* and the FIPS 140-2 Logo in no way constitutes or implies product endorsement by NIST or CSEC.
7. Photographic and electronic copies of the logo are available from NIST upon request.

Signature below acknowledges full agreement with the above conditions for the use of the phrase *FIPS 140-2 Validated* and the FIPS 140-2 Logo. Use of the phrase and logo as specified above may begin upon receipt of the original signed validation certificate. A signed form is required for each validated cryptographic module.

Signature: _____ Date: _____
Printed Name: _____
E-mail ID: _____
Title: _____
Company: _____
FIPS 140-2 Certificate Number(s): _____

Return signed form to: Beverly Trapnell, NIST, 100 Bureau Drive, Suite 8930, Gaithersburg, MD 20899

TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S. or Canadian Governments.

Annex F: Glossary

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
CCMVS	Counter with Cipher Block Chaining-Message Authentication Code Validation System
Cert	Certificate
CESG	Communications-Electronics Security Group
CST	Cryptographic and Security Testing
CMVP	Cryptographic Module Validation Program
CSEC	Communications Security Establishment Canada
CTCPEC	Canadian Trusted Computer Product Evaluation Criteria
DES	Data Encryption Standard
DOC	Word Document
DSA	Digital Signature Algorithm
DSAVS	Digital Signature Algorithm Validation System
DTR	Derived Test Requirements
EA	European co-operation of Accreditation
EAL2	Evaluation Assurance Level 2
ECB	Electronic Codebook
ECDSA	Elliptical Curve Digital Signature Algorithm
ECDSAVS	Elliptical 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 Message 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 Regulations
ITSEC	Information Technology Security Evaluation Criteria
ITSET	IT 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	Requests for Guidance
RNG	Random Number Generator
RNGVS	Random Number Generator Validation System
RSA	Rivest Shamir Adleman cryptographic algorithm
RTF	Rich Text Format
SBU	Sensitive but Unclassified
SCC	Standards Council of Canada
SHA	Secure Hash Algorithm
SHAVS	Secure Hash Algorithm Validation System
SHS	Secure Hash Standard
SoC	Secretary of Commerce
SP	Special Publication
TCSEC	Trusted Computer Systems Evaluation Criteria
TDES	Triple Data Encryption Standard
TID	Tracking Identification
TM	Trademark
URL	Uniform Resource Locator