Cryptographic Module Validation Program Management Manual

(Version 1.3)

National Institute of Standards and Technology and Communications Security Establishment

Initial release:	15 April 2009
Last update:	7 March 2017

Revision History

Version	Date	Comment
1.0	15 April 2009	Initial publication of the CMVP Management Manual
1.1	05 Jun 2014	Updated NIST CMVP Fee information
1.2	28 Oct 2016	Updated document
1.3	7 Mar 2017	Updated NIST CMVP Fee information, coordination deadline, added validation deadline

Table of Contents

List of Figures

List of Tables

1 Introduction

1.1 Background

The Communications Security Establishment (CSE) 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 CSE. 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 CSE, as the joint CMVP Validation Authorities, review laboratory reports, issue validation certificates, and participate in laboratory accreditations.

1.2 Purpose of the CMVP Management Manual

The purpose of the *CMVP Management Manual* is to provide effective guidance for the management of the CMVP, and the conduct of activities necessary to ensure that the standards are fully met.

1.3 Applicability and Scope

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

1.4 Purpose of the Cryptographic Module Validation Program

The purpose of the Cryptographic Module Validation Program is to 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 FIPS 140-2 for the protection of sensitive information where cryptography is required. Similarly, the Communications Security Establishment 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 140-2 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 140-2 if the product implements cryptography.
- Many private sector organizations enforce the use of cryptographic modules validated to FIPS 140-2 in order to conform to a minimum baseline of security functionality and assurance.

A list of FIPS 140-2 validated cryptographic modules is located at the following NIST web site: http://csrc.nist.gov/groups/STM/cmvp/validation.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 140-2

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.

1.7.2 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 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 140-2 divided into a set of assertions (AS) (i.e., statements that must be true for the cryptographic module to satisfy the requirement of a given area at a given level). All assertions are direct quotations from FIPS 140-2. Following each assertion is a set of information requirements that must be fulfilled by the vendor (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

1.7.3 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 CSE to questions posed by the CST laboratories, vendors, and other interested parties.

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

1.7.4 CST Laboratory Accreditation Standards

NIST laboratory accreditation standards applicable to the NVLAP accreditation of CST laboratories are published on the NVLAP website at http://ts.nist.gov/Standards/214.cfm.

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

1. NIST Handbook 150 (2016), *NVLAP Procedures and General Requirements,* http://www.nist.gov/nvlap/upload/nist-handbook-150.pdf; and
2. NIST Handbook 150-17 (2013), *NVLAP Cryptographic and Security Testing,* Document available on-line at http://www.nist.gov/nvlap/upload/NIST-HB-150-17-2013.pdf.

1.7.5 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 where the test report has been submitted to the CMVP for validation. (The listing is voluntary where vendors may choose to have their module listed on this list). For more information regarding a specific module, please contact the vendor.

6. Implementation Under Test (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 but have not yet been submitted to the CMVP. (The listing is voluntary where vendors may choose to have their module listed on this list.) the CMVP does not have information regarding the status of these modules or whether a test report will be submitted to the CMVP. For more information regarding a specific module, please contact the vendor.

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 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 CSE. If a vendor is under contract with a CST laboratory for testing to FIPS 140-2, the vendor must contact the contracted laboratory for all questions concerning the test requirements.

The name, telephone number and email address for the NIST and CSE Program Managers are:

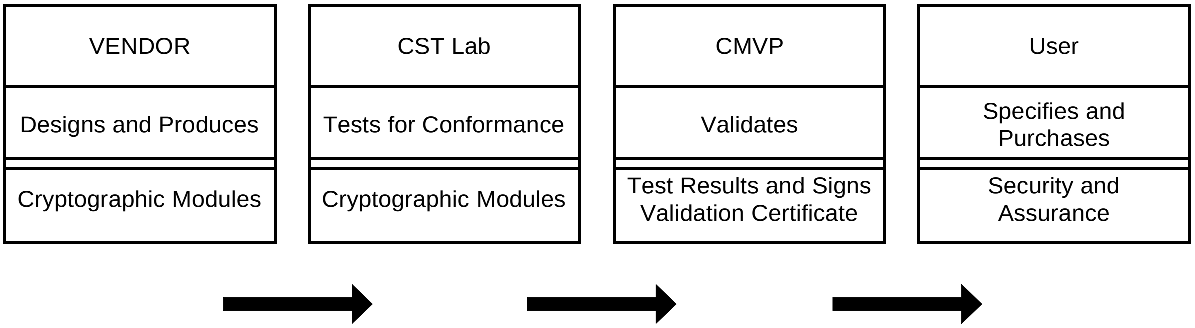
NIST	CSE
Jennifer Cawthra	Carolyn French
NIST CMV Program Manager	CSE CMV Program Manager
Security Testing, Validation, and Measurement Group	Architecture and Technology Assurance
301-975-8514	613-949-7703
jennifer.cawthra@nist.gov	carolyn.french@cse-cst.gc.ca

Table 1: CMVP Program Manager Contact Information

A complete list of all CMVP points of contact can be found on the CMVP website at: 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.



VENDOR	CST Lab	CMVP	User
Designs and Produces	Tests for Conformance	Validates	Specifies and Purchases
Cryptographic Modules	Cryptographic Modules	Test Results and Signs Validation Certificate	Security and Assurance

Figure 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 cannot 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 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 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. 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 for the Government of Canada.

The role of the Validation Authorities is to validate the test results for every cryptographic module. The test results are documented in the submission package prepared by a CST laboratory and reviewed by the CMVP. If the cryptographic module is determined to be compliant with FIPS 140-2, then the module is validated, a validation certificate is issued and the on-line validation list is updated. During the review process, the Validation Authorities submit any questions they may have to the CST laboratory. The questions are typically technical in nature and are intended to ensure that the cryptographic module meets the requirements of the standard and that the information provided is accurate and complete. The CST laboratory may need to re-submit the validation submission along with supporting documentation such as a draft validation certificate, validation report, or security policy.

The CMVP participates, on behalf of NVLAP, in the CST laboratory accreditation process which includes the review of the management system manual, the conducting 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 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.

The CMVP validates specific versions of a cryptographic module and the user must verify that the version procured is in fact the validated version. The validated version number of a cryptographic module is also specified on the *Validated FIPS 140-1 and 140-2 Cryptographic Modules* list on the CMVP web site.

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 CSE. Decisions are made jointly by both organizations with the NIST and the CSE Program Managers communicating regularly.

2.5.1 CMVP Meetings

CSE 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 CSE organize annual CST laboratory manager meetings to discuss issues relating to the CMVP, CAVP, and CST laboratories. An agenda is created and distributed to the CST laboratories before the meetings and presentation materials are distributed to the CST laboratories for reference following the meetings. CST laboratory managers are welcomed to add any new agenda items at any time. Typically, the CST laboratory manager meetings are to include only CST laboratory managers and the CMVP and CAVP Validation Authorities, however CST laboratory staff may be invited to attend, space permitting.

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, CSE, 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, CSE, 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, CSE, 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 CSE.

NIST, CSE, 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 CSE. NIST and CSE 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 CSE and by the Computer Security Division at NIST.

2.8 Programmatic Directives and Policies, and Internal Guidance and Documentation

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

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

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

3 CST Laboratory Processes

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

3.1 Accreditation of CST Laboratories

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

Note: This section describes the process used by NVLAP.

3.1.1 Recognized Standards and Standard Accreditation Body

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

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

3.1.1 NIST Handbook 150 (2016) and Handbook 150-17 (2013) under the NVLAP of the Government of the United States of America; and

3.1.2 Accreditation Process

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

The accreditation process is illustrated in Figure 2: CST Laboratory Accreditation Process. All steps in the accreditation process are sequential and must be completed in the order shown.

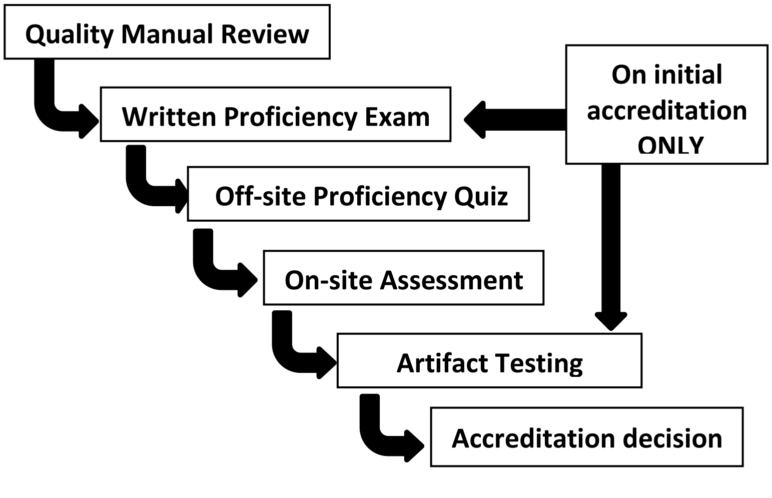


Figure 2: CST Laboratory Accreditation Process

3.1.2.1 Application for Accreditation and Selection of Assessment Team

The prospective CST laboratory must complete an application form, pay the respective fees, agree to 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. This team is typically comprised of one technical assessor from CMVP and one lead assessor from NVLAP. NVLAP technical assessors for CST laboratories are selected by the NVLAP Program Manager and are chosen based upon their knowledge of the relevant FIPS standards and related documentation, NVLAP requirements, assessment techniques, and quality systems. The assessors must not have a conflict of interest with the CST laboratory they will be assessing.

3.1.2.2 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 written 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) calendar days to complete the exam. The assessing team will grade the exam and determine if the laboratory is competent.

3.1.2.4 Off-site Proficiency Quiz

Prior to the on-site assessment, the assessment team will conduct a proficiency interview 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. The assessment team will grade the exam and if the lab passes, the on-site assessment will be scheduled.

3.1.2.5 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) to three (3) business days to perform. The activities performed during an assessment are described in Section 3.2 Assessment of NIST Handbook 150.

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

3.1.2.6 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 3 months. 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 three validation test reports 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 may suspend or revoke the laboratory's accreditation.

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://www.nist.gov/nvlap/nvlap-fee-policy.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 2: CST Laboratory Accreditation Process and described in Section 3.1.2 except there is no initial Written Proficiency Exam. 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. The accreditation is valid for 2 years.

3.2.3 Ownership of a CST Laboratory

In the event that a CST laboratory changes ownership, the accreditation body and the CMVP Validation Authorities must be informed within 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 thirty (30) 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 thirty (30) 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 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, CSE and the CST Laboratory

The confidentiality of the proprietary information exchanged between NIST, CSE 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.*

The IEEE code of ethics is available from http://www.ieee.org/about/corporate/governance/p7-8.html.

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 CSE 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 CSE for use by the CMVP and CAVP. Violation of this policy may be considered cause for suspension of the CST laboratory's accreditation.

4 Cryptographic Module Validation Program Processes

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

4.1 Cryptographic Module Validation Process Overview

This section provides a high-level overview of the validation program.

4.1.1 General Overview

Figure 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.

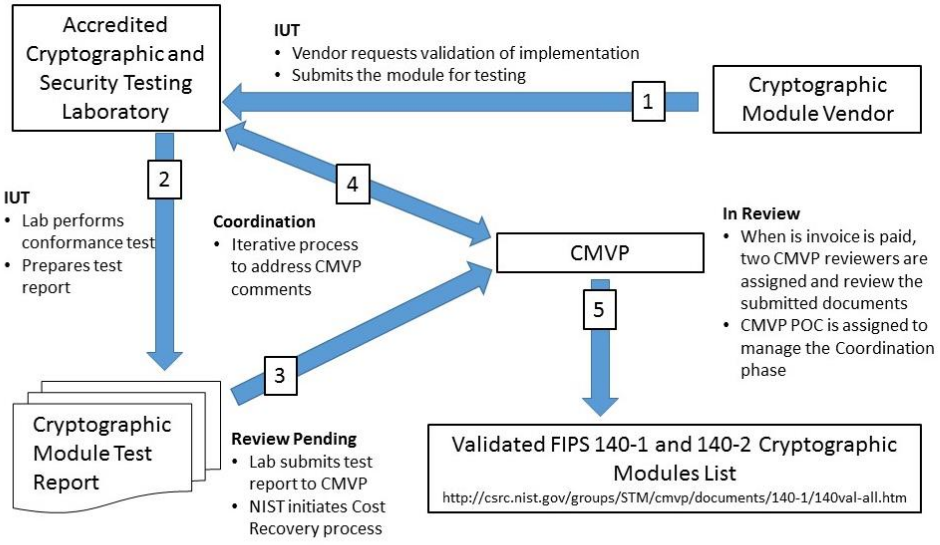

Accredited Cryptographic and Security Testing Laboratory
IUT
• Vendor requests validation of implementation
• Submits the module for testing
1
Cryptographic Module Vendor
2
4
IUT
• Lab performs conformance test
• Prepares test report
Coordination
• Iterative process to address CMVP comments
CMVP
In Review
• When is invoice is paid, two CMVP reviewers are assigned and review the submitted documents
• CMVP POC is assigned to manage the Coordination phase
5
3
Cryptographic Module Test Report
Review Pending
• Lab submits test report to CMVP
• NIST initiates Cost Recovery process
Validated FIPS 140-1 and 140-2 Cryptographic Modules List
http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

Figure 3: Cryptographic Module Testing and Validation Process

The steps for the cryptographic module validation life cycle include:

Step 1. The vendor submits the cryptographic module for testing to an accredited CST laboratory under a contractual agreement. Cryptographic module validation testing is performed using the Derived Test Requirements (DTR) for FIPS 140-2, *Security Requirements for Cryptographic Modules*. If the CST laboratory has any questions or requires clarification of any requirement in regards to the particular cryptographic module, the laboratory can submit Requests for Guidance (RFG) to NIST and CSE as described in the *Implementation Guidance for FIPS 140-2 and the Cryptographic Module Validation Program G.1*.

Step 2. Once all the testing requirements have been completed, a validation submission is prepared.

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

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

Step 5. Once the cryptographic module has been validated, the validation information is posted to the *Validated FIPS 140-1 and FIPS 140-2 Cryptographic Module List* at the CMVP website: http://csrc.nist.gov/groups/STM/cmvp/validation.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 CSE that the cryptographic module is an Implementation Under Test (IUT). The laboratory provides the name of the cryptographic module and the cryptographic module vendor's name and indicates whether this information is to appear in the *IUT list*.

The CST laboratory assigns a Tracking Identification Number (TID) using the convention described in the *CMVP E-mail Correspondence document*. The first two digits of the TID are assigned by the CMVP upon laboratory accreditation, the second set of four digits is assigned by the laboratory, and the last four digits are assigned by CSE when the validation submission is accepted. In all, a ten-digit TID number is created and used to track the submission.

The CST laboratory performs the cryptographic module testing as prescribed by the Derived Test Requirements (DTR) for FIPS 140-2, *Security Requirements for Cryptographic Modules* and enters all assessments for the testing in the CRYPTIK tool. Although testing requirements are in the DTR, FIPS 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 CSE and NIST in determining how to apply the FIPS 140-2 standard to the particular cryptographic algorithm module.

The FIPS 140-2 validation process is an iterative process. If the CST laboratory discovers any non-conformances in the cryptographic module documentation or the cryptographic module itself, it must bring details of the non-conformance(s) to the attention of the cryptographic module vendor. The cryptographic module vendor must correct the non-conformance(s) and resubmit the document or the cryptographic module for validation testing.

When the CST laboratory has completed all required validation testing and has determined that the cryptographic module is conformant to FIPS 140-2, the laboratory prepares the validation test report and the rest of the validation test submission and sends it to NIST and CSE 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 CSE TID as described in Annex A: CMVP Convention for e-mail Correspondence. When the submission is accepted by the CMVP, the module is moved to the PENDING REVIEW stage of the Modules in Process list. The module will remain in the PENDING REVIEW stage until the NIST Cost Recovery fee is paid and the first reviewer begins the review. When the reviewer begins the review, the cryptographic module is moved to the IN REVIEW stage of the Modules In Process. When the CMVP reviewers have completed their review of the validation submission and provided comments, the comment file is encrypted and sent to the CST laboratory via email. The cryptographic module is then moved to the COORDINATION stage.

The CST laboratory addresses the comments and resubmits a complete submission containing any modified documents as per Section 4.3: Preparation and Submission of the Validation Submission. Test Report Submission. The CSE 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 daily.

4.1.4 Validation Certificate

At the end of the validation process NIST and CSE, 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 and the Cryptographic Module Validation Program G.13.*

When NIST and CSE are satisfied with the test report, CSE sends the finalized comment file 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, CSE will issue a certificate number to the laboratory and the certificate is posted to the NIST web site. At the end of each month, the Validation Authorities sign a consolidated validation certificate which lists all modules that were validated during the month.

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 the *Implementation Guidance for FIPS 140-2 and the Cryptographic Module Validation Program G.8,* the module's validation will be updated on the website 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 website.

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 Implementation Under Test (IUT) and Modules In Process (MIP) Lists* are provided for information purposes only. Participation on the list is *voluntary* and is a joint decision by the vendor and the CST laboratory. Modules are listed alphabetically by name. If a vendor and CST laboratory chose not to list the module on either list, the module will be reflected at the end of the list in the "Not Displayed" row. Posting on the list does not imply or guarantee FIPS 140-2 validation. The IUT and MIP lists are available on the NIST web site http://csrc.nist.gov/groups/STM/cmvp/inprocess.html.

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

The following sections describe the requirements or activities that take place during each stage of the FIPS 140-2 Modules In Process. The status of each cryptographic Module In Process is identified.

1. Implementation Under Test (IUT)

- There exists a viable contract between the vendor and the CST laboratory for the testing of the cryptographic module.
- The cryptographic module is resident at the CST laboratory.

- All of the required documentation is resident at the CST laboratory. NOTE: if the vendor requires the CST laboratory personnel to test the cryptographic module on-site, all documents must also be on-site with the module.

2. Review Pending

- Complete set of testing documents submitted to NIST and CSE for review. The set includes: draft certificate, detailed test report, non-proprietary security policy, and website information. In addition, some modules may require a separate physical security testing report.
- Signed letter from laboratory stating recommendation for validation by NIST and CSE.

3. In Review

- NIST and CSE reviewers assigned.
- NIST and CSE perform a review of the test documents.
- Comments coordinated by NIST and CSE reviewers and a consolidated set of comments sent to the CST laboratory.

4. Coordination

This phase of the process may be iterative.

- Comments received by the CST laboratory from NIST and CSE for resolution.
- Additional testing (if required).
- Additional documentation (if required).
- Comments resolution developed for resubmission to NIST and CSE.
- Testing documents updated for resubmission to NIST and CSE.
- Responses to comments and revised test documents submitted to NIST and CSE.
- Several iterations may be required to address all comments.

5. Finalization

- Final resolution of validation review comments submitted to NIST and CSE.
- Testing documents updated based on resolutions and submitted to NIST and CSE.
- After the NIST and CSE final review of the draft certificate, a copy is sent to the CST laboratory for a final review.
- Once the CST laboratory approves the final draft certificate, CSE assigns a certificate number and NIST posts the certificate to the Validated FIPS 140-1 and 140-2 Cryptographic Modules list.

6. Consolidated Certificate

- At the end of each month, a consolidated certificate is generated which includes all of the certificates that were published during the month.
- CSE and NIST sign the consolidated certificate and it is posted to the web site: http://csrc.nist.gov/groups/STM/cmvp/validation.html

4.3 Preparation and Submission of the Validation Submission

NIST and CSE 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 and the Cryptographic Module Validation Program* G.2.

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

1. **Non-proprietary Security Policy in PDF**. The security policy **shall** not be marked as proprietary or copyright, 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 v9.0c (or higher) reports in PDF**. The validation report submission must be output from the NIST-provided CRYPTIK tool:
    a. **Signature page** – insert PDF of signed signature page;
    b. **General Vendor / Module Information** page – PDF;
    c. **Full Report with Assessments** – PDF; and
    d. **Certificate –** MS Word
    e. **Vendor Text File** - TXT
3. **Physical Security Test Report** (mandatory at 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. **Entropy Report –** PDF, if applicable

The CST laboratory has the option to additionally provide *Notes and Proprietary Information* output with the Detailed Report with Assessments, but this is not required by NIST and CSE. 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 CSE reviewers, and sent to the following NIST and CSE points of contact:

- **NIST**: CMVP@nist.gov
- **CSE**: 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-serve basis.

The internal review disposition of a module report is left to the sole discretion of the NIST and CSE CMVP program managers. Reports will not be marked as FULL or RE-VALIDATION on the MIP list, or ordered differently as currently posted.

4.4.2 Non-security Relevant Re-validation

Non-security relevant change letters as described in the *Implementation Guidance for FIPS 140-2 and the Cryptographic Module Validation Program G.8* will be handled upon receipt.

4.4.3 HOLD Status for Cryptographic Modules on the Modules In Process

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

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

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

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

If CMVP comments are sent to the lab and the lab has not responded with 120 days, the module will be placed on HOLD and removed from the MIP list until the CST laboratory provides a response. Effective July 1, 2017, the amount of time will be reduced from 120 days to 90 days.

4.4.4 Validation Deadline

Effective January 1, 2018, CMVP will drop modules that have not completed the validation process within 2 years of report submission or request for an invoice. When the module is dropped, the vendor and lab must restart the validation process including paying a new cost recovery fee at the current rate. This applies to all submissions currently in the process as well as to new submissions.

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

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

4.5.1 International Traffic in Arms Regulations Policy

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

4.5.1.1 CMVP ITAR Guidance

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 CSE TID. A CSE 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.

Report review

- **a.** Each ITAR report will be reviewed by two NIST reviewers.

Certificate generation and posting

- **a.** Certificates will be prepared by NIST only.
- **b.** Certificates will be signed only by NIST. The CSE signature field will be marked as: Not Applicable – ITAR.
- **c.** The NIST CMVP web page will only post the following information: Certificate number, Vendor (null), Cryptographic Module (validated to FIPS 140-2), Module Type, Validation Date, and Level/Description.
- **d.** The official certificate will be scanned and emailed to the CST laboratory for presentation to the vendor.

Re-validation

- **a.** All re-validation changes under the *Implementation Guidance for FIPS 140-2 and the Cryptographic Module Validation Program G.8* will result in a new certificate sent to the CST laboratory for presentation to the vendor since the web site will not have any identifiable information.
- **b.** Report submission, report review, certificate generation and posting as outlined above and following the requirements stated in *the Implementation Guidance for FIPS 140-2 and the Cryptographic Module Validation Program G.8*.

[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.

4.6 NIST Cost Recovery[2]

The NIST CMVP fee schedule is published under **CMVP Notices** at http://csrc.nist.gov/groups/STM/cmvp/notices.html.

The fee amount is based on the overall security level of the validation and the submission scenario under IG G.8. The schedule includes cost recovery (CR) fees as well as extended cost recovery (ECR) fees.

	Base fee:	**Extended fee:**
IG G.8 Scenarios 1, 2 and 4 All Security Levels:	N/A	$1,000
IG G.8 Scenarios 1A and 1B All Security Levels:	$1,500	$1,000
IG G.8 Scenario 3 All Security Levels:	$3,000	$1,500
IG G.8 Scenario 5 Security Level 1:	$6,000	$3,000
Security Level 2:	$8,000	$4,000
Security Level 3:	$11,000	$5,000
Security Level 4:	$15,000	$6,000

Table 2: Cost Recovery Fee Schedule Effective October 1, 2016

	Base fee:	**Extended fee:**
IG G.8 Scenarios 1, 2 and 4 All Security Levels:	N/A	$1,000
IG G.8 Scenarios 1A and 1B All Security Levels:	$1,500	$1,000
IG G.8 Scenario 3 All Security Levels:	$3,000	$1,500
IG G.8 Scenario 5 Security Level 1:	$6,000	$3,000
Security Level 2:	$8,000	$4,000
Security Level 3:	$8,000	$4,000
Security Level 4:	$8,000	$4,000

Table 3: Cost Recovery Fee Schedule Effective October 1, 2017

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

4.6.1 Cost Recovery Fee

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

4.6.2 Extended Cost Recovery Fee

An extended cost recovery (ECR) fee is applicable when a report submission requires significant additional review effort by the validators. The extended fee is applicable to all report submissions under FIPS 140-2 IG G.8. The CMVP will review the rationale for the application of the extended cost recovery fee with the CST laboratory before determination of its applicability. The extended cost recovery fee is billed separately from the CR fee, if applicable, and must be remitted prior to validation. The fee varies by submission type and security level. See Table 4-1 for the specific fees.

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

Complexity

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

If the single report submission represents many modules, the review time will increase based on the quantity and module differences; the review time will exceed the average and ECR will be applied or the report may be rejected and the number of modules per report reduced.

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

Quality

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

During CMVP review and coordination, the CMVP generates many comments and comment rounds due to issues in the report such as: incomplete information, inconsistent information, insufficient information, or not following CMVP Implementation Guidance or adherence to the FIPS 140-2 conformance requirements. This leads to significant and sometimes specialized effort by CMVP to resolve; ECR will be applied.

During CMVP review and coordination it may be discovered that the module is not conformant to FIPS 140-2 or CMVP Implementation Guidance and this was not discovered by the CST laboratory during the testing process. The determination leads to significant and sometimes specialized effort by CMVP to assess what is necessary to complete the testing; ECR will be applied.

4.6.3 NIST Payment Policy

NIST CMVP maintains the billing information for each CST laboratory. If the CST laboratory’s information needs to be updated, contact NIST CMVP. Upon receipt of the CST laboratory's submission or a request for an invoice (see IG G.16), NIST billing prepares an invoice and submits it to the identified payee. Only CST laboratories will be invoiced by NIST billing. Review of submissions will not begin until NIST CMVP receives confirmation from NIST Receivables that the invoice has been paid.

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

4.7 Request for Transition Period Extension

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

4.8 Flaw Discovery Handling Process

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

1. NIST, CSE and the CST laboratory will investigate the allegation about the flaw, and determine its impact on the validation;
2. NIST and CSE 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 CSE may advise their respective federal departments of the flaw and its impact; and
4. NIST and CSE 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.

4.9 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.

If the validation certificate is revoked, it will be annotated with “revoked” and appear on the *CMVP Historical Validation List*.

4.10 CMVP Webpage Update

This section provides information about the CMVP website.

4.10.1 Official CMVP Website

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

4.10.2 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 140-2:

- *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
- *CMVP Historical Validation List* – a single list of
  - revoked certificates;
  - modules with non-approved algorithms on the FIPS approved algorithms list (e.g. due to algorithm transitions); and
  - certificates older than 5 years.
- *Consolidated Validation Certificates*
- *FIPS 140-2 Modules In Process*
- *FIPS 140-2 Implementation Under Test*
- *FIPS 140-1 and FIPS 140-2 Vendor List*

4.11 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. Press releases are not accepted.

4.11.1 Update Frequency of Validation Lists

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

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

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

This list is updated and posted daily.

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

This list is updated when new validation certificates are posted to the web site 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.

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

The FIPS 140-1 and FIPS 140-2 logo request form is available from the CMVP web site: http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402LogoForm.pdf. The form includes the terms of use. Completed forms are sent to cmvp@nist.gov. If approved, NIST CMVP will send the artwork to the requestor.

5 CMVP and CAVP Programmatic Metrics Collection

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

5.1 Overview

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

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

5.2 Confidentially of the Collected Metrics Data

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

5.3 Collected Metrics

The following CMVP metrics will be collected by each CST laboratory for modules that have been validated or re-validated, refer to the *Implementation Guidance for FIPS 140-2 and the Cryptographic*

Module Validation Program G.8.

- 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 August and January, 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 cannot be preserved.

5.7 Metrics Submission

The CMVP metrics **shall** be included into a single zip file, encrypted for all NIST and CSE 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)

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

Responsible Positions: CMVP Validation Authorities.

6.2 Cryptographic Algorithm FIPS and NIST Special Publications

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

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

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

For NIST Recommendations, the NIST Special Publications are posted on the NIST web site 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 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 Cryptographic Technology Group.

6.3 Derived Test Requirements

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

Responsible Positions: NIST CMVP and CSE CMVP Program Managers.

6.4 Implementation Guidance

The IG is updated on a quarterly basis

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

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

Responsible Position: NIST CMVP and CSE CMVP Program Managers.

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 CSE 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: NIST CMVP and CSE CMVP Program Managers.

6.6 Test Tools

6.6.1 CRYPTIK

Cryptik is a required tool for the completion of module testing, and generation of documents that **shall** be included in a formal submission from the CST.

Responsible Individual: NIST CMVP Program Manager.

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: CSE CMVP Program Manager

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: CSE CMVP Program Manager

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*. Handbook 150 may need to be restructured from time to time so that it conforms to internationally accepted rules for the structure and drafting of standards and similar technical documents and ensure it is easy to understand and use.

Revisions to NIST Handbook 150 must be published in the US Federal Register and officially approved by the office of the U.S. Secretary of Commerce. The Forward of NIST Handbook 150 summarizes the changes made in the current edition of the handbook since the last published edition of the handbook. Handbook 150 is posted on the NVLAP website at http://nvlpubs.nist.gov/nistpubs/hb/2016/NIST.HB.150-2016.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 on a periodic basis. Changes in this handbook are made in recognition of advancements in technology and tools or when a change is made in the general accreditation requirements for a Cryptographic and Security Testing laboratory or requirements for meeting a defined accreditation level.

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

Revisions to Handbook 150-17 are made by the Program Manager for Information Technology Security Testing. Handbook 150-17 is available on-line: https://www.nist.gov/sites/default/files/documents/nvlap/NIST-HB-150-17-2013.pdf .

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

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: NIST CMVP and CSE CMVP Program Managers.

Annex A: CMVP Convention for E-mail Correspondence

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

Acronyms

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

e-mail Subject Line format:

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

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

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

Field1 – LC-nnnn **CSTL TID**

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

The 2-digit LC designations are as follows:

LC	CST Laboratory	LC	CST Laboratory
01	InfoGard	17	ECSEC
02	CEAL	18	Epoche and Espri
03	DOMUS	19	ITSC
04	COACT	20	CSC
05	SAIC - VA	21	UL
06	EWA	22	BAE Systems AI
07	LogicaCMG	23	CGI
08	BT	24	BAH
09	TÜViT	25	ADS
10	Aspect	26	UL Transaction Security
11	atsec	27	Penumbra
12	ICSA	28	Gossamer
13	Leidos	29	Acumen Security
14	ACTL	30	Asia Pacific IT Lab, TÜV NORD
15	Ægisolve	31	Serma
16	TTC		

Field2 – nnnn **CSE TID**

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

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

[4-digit character email tag as defined below]

Pre-validation Activities:

IUTA[3]	– Add report to IUT list
IUTB	– Request an invoice from NIST for Cost Recovery before report submission
IUTC	– Cancel a request for an invoice from NIST for Cost Recovery - only available if the invoice has not been paid
IUTR	– Remove report from the IUT list
IUTM[3]	– Modify an existing IUT entry

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

sSUB[3]	– Report Submission (FIPS 140-2 IG G.2)
sHLD	– Place report on HOLD
sNSn[3]	– NIST comments
sCSn[3]	– CSE comments
sCMn[3]	– CMVP comments or returned CSTL addressed comments
CRVn[3]	– CMVP (int) review w/ OK comments & draft certificate
NCRn[5]	– NIST (cert) review response to draft certificate
CCRn[5]	– CSE (cert) review response to draft certificate

n=0	[if comments not sent to CSTL] **OR**
n=1+	[nth time CMVP comments sent to the CSTL]

Finalization Activities:

FAOK[3]	– All OK comments w/draft certificate for CSTL review and moves MIP reporting to Finalization
FCLC[5]	– CSTL review response to draft certificate
FRCN	– Request certificate number assignment
FVCN	– Assignment of validation certificate number
FWPH	– Posting of validation entry on NIST web site
FCVC[1]	– Consolidated Validation Certificate
FMOD[2]	– Modification of posted validation entry

Miscellaneous:

ASSG	– CSE assigned TID
DRPT	– CSTL request to DROP report
RQFG	– CSTL request for guidance
ALOR	– Internal Assignment of NIST or CSE report reviewer
STAT	– Query report status

[3] **Shall** include file attachment

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

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

OTHR	– Other

Billing:

NECN[6]	– NIST Extended Cost Recovery Notification to CSTL
NECR[6]	– NIST Extended Cost Recovery CSTL Response

Field4 – **Vendor Name**
[1 to10-digit *alphanumeric* characters maximum]

Field5 – **Date of Transaction**
[6-digit *numeric* date of transaction (format: yymmdd)]

Field6 – **V**n **Version Number**

n [nth transaction]

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

Field7 – **Certificate Number**
[Newly Assigned Certificate Number (FVCN)], or

Field8 – **Report Review or Draft Certificate Review Completed**
[**OK** – NIST, CSE or CSTL review completed with no further comments]
[If the OK is not included on the subject line, there will be another round of comments]

---

[6] **Shall** include file attachment

TO: and CC: minimum requirements:

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

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

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

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

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

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

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

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

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

   TO: cmvp@cse-cst.gc.ca

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

   TO: cmvpitar@nist.gov

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

   TO: <CST Lab>

File attachment naming convention:

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

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

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

1. *Security Policy*:
   - **s(scenario) = 1A, 1B, 3 or 5** <ZIP FILE NAME>**_140sp.pdf**
   - **s = 1[7] or 4[7]** <ZIP FILE NAME>**_140sp**<CertNo>**.pdf**
     (one security policy for *each* certificate number referenced)

2. *CRYPTIK Assessment Reports (IG G.2 and IG G.8 minimum requirements)*:
   - **s = 3** <ZIP FILE NAME>**_report.pdf**
     Signed Signature Page || General Vendor/Module Information || Revalidation Report with Assessments (including list of changes) || Full Report || Physical Test Report (Section 4.5 Levels 2, 3 and 4)
   - **s = 4** <ZIP FILE NAME>**_report.pdf**

     Physical Test Report (Section 4.5 Levels 2, 3 and 4)
   - **s = 5** <ZIP FILE NAME>**_report.pdf**

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

3. *CRYPTIK Vendor Text File*:
   - **s = 1, 3, 4, or 5** <ZIP FILE NAME>**_vendor.txt**[8]

4. *CRYPTIK Draft Certificate*:
   - **s = 1A, 1B, 3, or 5** <ZIP FILE NAME>**_140crt.doc**

5. *CMVP Comments*:
   - **s = 1, 3, 4, or 5** <ZIP FILE NAME>**.doc**

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

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

6. *Change Request Letter*[9] :

   - **s = 1 or 4**

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

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

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

Submission Scenarios	**CSTL to CMVP**	**File Content**	**CMVP to CSTL**
5SUB	_vendor.txt _140sp.pdf _report.pdf _140crt.doc, .docx, .rtf .doc, .docx, .rtf[10]	General Vendor/Module and Billing Information Security Policy Test Report Draft Certificate CMVP Comments with CSTL Resolutions	.doc, .docx, .rtf[11] .doc, .docx, .rtf
4SUB	_vendor.txt _letter_unsigned.pdf _letter_signed.pdf _140sp<CertNo>.pdf _report.pdf .doc, docx, .rtf[1]	General Vendor/Module and Billing Information Change Request Letter Change Request Letter – signed Security Policy[12] Test Report[13] CMVP Comments with CSTL Resolutions	.doc, docx, .rtf
3SUB	_vendor.txt _140sp.pdf _report.pdf _140crt.doc, docx, .rtf .doc, .docx, .rtf[1]	General Vendor/Module and Billing Information Security Policy Test Report Draft Certificate CMVP Comments with CSTL Resolutions	.doc, .docx,. rtf[2] .doc, .docx, .rtf
1SUB	_vendor.txt _letter_unsigned.pdf _letter_signed.pdf _140sp.pdf _140sp<CertNo>.pdf _140cert.doc, .docx, .rtf .doc, .docx, .rtf[1]	General Vendor/Module and Billing Information Change Request Letter Change Request Letter – signed Security Policy for 1A or 1B Security Policy[3] for 1SUB Draft Certificate for 1A or 1B CMVP comments with CSTL resolutions	.doc, .docx, .rtf

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

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

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

[13] Physical Security Test Report.

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

Report Submission Examples

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

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

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

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

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

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

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

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

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

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

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

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

Typical COORDINATION set of comment rounds for a revalidation s=3

First set of CMVP comments sent to the CSTL:

Example 7a: TID-05-0004-0024-3CM1-Cisco_Syst-100115-V1-1024

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

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

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

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

Second set of CMVP comments sent to the CSTL:

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

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

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

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

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

---

Example 8: TID-04-0005-**ITAR**-5NS1-Attachmate-080520-V1

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

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

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

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

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

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

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

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

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

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

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

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

Sending Consolidated Validation Certificate to CSE for signature

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

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

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

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

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

The validation entry for Cert. #nnnn has … *or*
The validation entries for Certs. #nnnn, #nnnn and #nnnn have …
been modified and the NIST CMVP web site will be posted

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

The subject report has been assigned to you.

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

Please provide status for this report

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

NIST CMVP sent to CST Lab:

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

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

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

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

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

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

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

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

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

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

Lab assigned TID number 04-0006, CSE TID number not yet assigned, submitted by COACT – IUT Modify Request, Vendor Cisco Systems, Inc. - Sent on February 4, 2015, Version 1
The attached zip file would include the _vendor.txt file

File attachment examples; the attached file names would be named as follows:

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

TID-06-0001-0000-**1SUB**-Motorola-100802-V1.zip

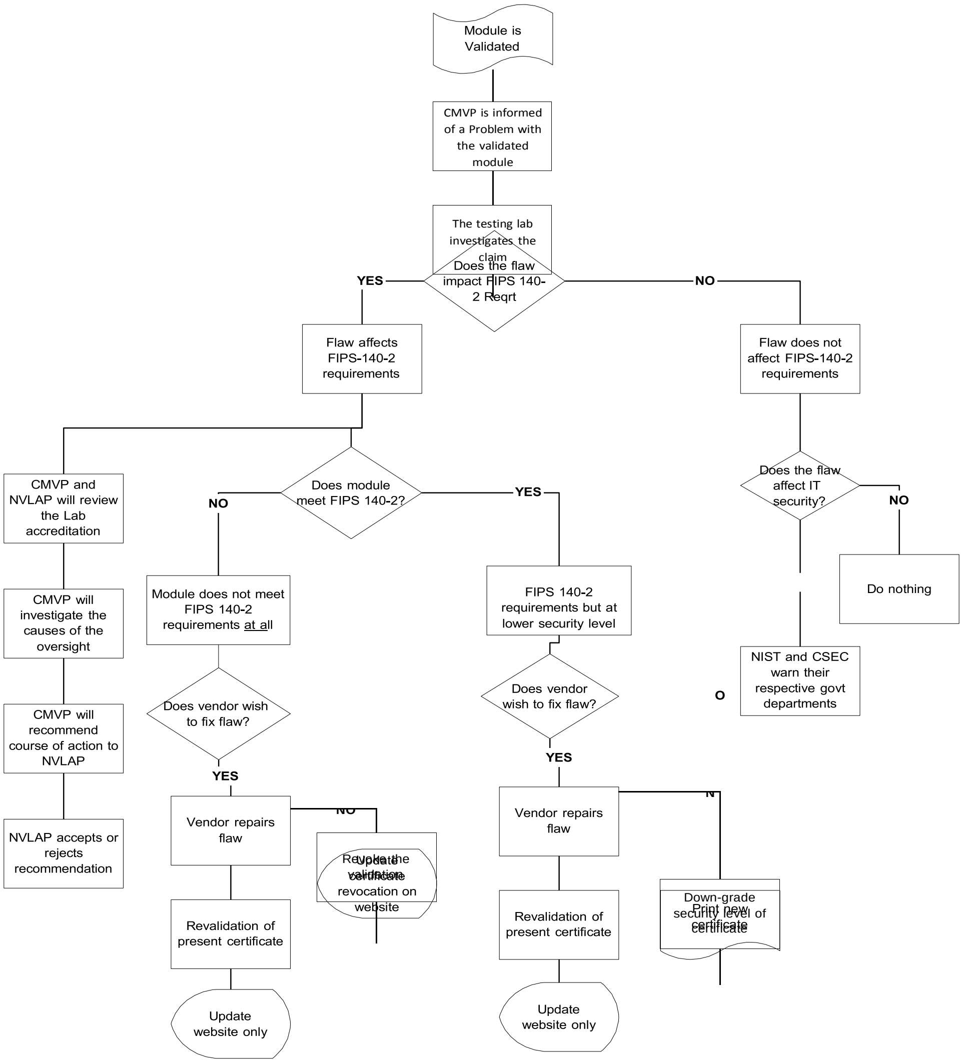
TID-16-0001-0000-**1SUB**-Motorola-100802-V1**.**zip

TID-05-0004-0024-**3CM2**-Cisco-100123-V2-1024.zip

TID-04-0005-**ITAR**-**5NS1**-Attachmate-080520-V1.zip

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

Annex B: Flaw Discovery Handling Process Diagram


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

Annex C: 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
CSE	Communications Security Establishment
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
SHA	Secure Hash Algorithm
SHAVS	Secure Hash Algorithm Validation System
SHS	Secure Hash Standard
SoC	Secretary of Commerce
SP	Special Publication
TCSE	Trusted Computer Systems Evaluation Criteria
TDES	Triple Data Encryption Standard
TID	Tracking Identification
TM	Trademark
URL	Uniform Resource Locator