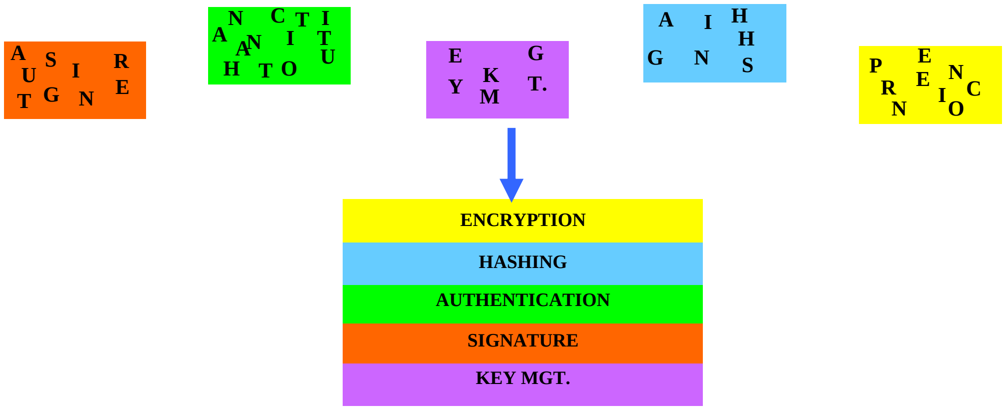
CAVP



ENCRYPTION

HASHING

AUTHENTICATION

SIGNATURE

KEY MGT.

Cryptographic Algorithm Validation Program Management Manual

DRAFT

(Version 1.0)

National Institute of Standards and Technology
and
Communications Security Establishment Canada

Initial release: June 24, 2009
Last update:

Revision History

Version	Date	Comment
1.0	June 24, 2009	Initial draft release

Table of Contents

Figures

1 Introduction

1.1 Background

The Communications Security Establishment Canada (CSEC) and the National Institute of Standards and Technology (NIST) announced the establishment of the Cryptographic Module Validation Program (CMVP) on July 17, 1995. At that time, the CMVP encompassed both the functions of the CMVP and the Cryptographic Algorithm Validation Program (CAVP). In 2003, with the increased number of approved Federal Information Processing Standards (FIPS-Approved) and NIST-recommended cryptographic algorithms, the CAVP was formed as a separate program. The CMVP validates commercial cryptographic modules to Federal Information Processing Standard Publication (FIPS PUB) 140-2, while the CAVP validates cryptographic algorithm implementations (See Section 4.1) to FIPS-Approved and NIST-recommended (referred to as Approved) cryptographic algorithm Special Publications and Federal Information Processing Standards (referred to as *references* (See Section 1.6.2). The CMVP and the CAVP are jointly managed by NIST and CSEC. Cryptographic 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 and algorithm implementations use independent, National Voluntary Laboratory Accreditation Program (NVLAP) or Standards Council of Canada (SCC) accredited Cryptographic and Security Testing (CST) laboratories to test their modules and implementations. The CST laboratories may perform all of the tests covered by the CMVP and CAVP. NIST and CSEC, as the joint CMVP and CAVP Validation Authorities, review laboratory reports and results, issue validation certificates, and typically conduct laboratory accreditations on behalf of NVLAP.

1.2 Purpose of the CAVP Management Manual

The *CAVP Management Manual* provides guidance for the CAVP and other parties in the validation process.

1.3 Applicability and Scope

The *CAVP Management Manual* applies to the CAVP Validation Authorities, the CST laboratories, and the vendors who participate in the program. Consumers who purchase validated cryptographic modules and validated cryptographic algorithm implementations may also be interested in the contents of this manual. This manual outlines the management activities and specific responsibilities of the various participating groups. This manual does not include any cryptographic standards.

1.4 Purpose of the CAVP

The CAVP provides assurance that cryptographic algorithm implementations adhere to the specifications detailed in the associated cryptographic algorithm references. A suite of validation tests is designed for each cryptographic algorithm (called the algorithm's validation system) to test the algorithm specifications, components, features, and/or functionality of that algorithm. The validation of cryptographic algorithm implementations in the cryptographic module are a prerequisite to the validation of that cryptographic module.

1.5 Use of Validated Cryptographic Modules and Algorithm Implementations

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). The U.S. Federal Government requires its departments and agencies to use cryptographic modules validated to either FIPS 140-1 or FIPS 140-2 for the protection of sensitive information where cryptography is required. Similarly, the Communications Security Establishment Canada recommends that GC departments and agencies use validated cryptographic modules for the protection of Protected information.

Several Common Criteria (CC) Protection Profiles (PP) require FIPS 140-1 or FIPS 140-2 validated cryptographic modules to provide verification of correct implementation of cryptographic security functions. 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 validated to FIPS 140-1 or FIPS 140-2 if the product implements cryptography.

Many private organizations use cryptographic modules validated to FIPS 140-2 for cryptographic protection because of the assurance in the level of security provided by the standard and a validation to it.

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

A separate list of validated cryptographic algorithm implementations for each FIPS-Approved and NIST-recommended cryptographic algorithm for which the CAVP has validation testing is located at the following NIST web site: http://csrc.nist.gov/groups/STM/cavp/validation.html

1.6 CAVP Related Documents

1.6.1 FAQ on CAVP

The CAVP maintains a list of frequently asked questions (FAQ) related to the CAVP. Information about the CAVP in general, the interpretation of specifications in an algorithm reference, etc. are included. This CAVP FAQ is located at http://csrc.nist.gov/groups/STM/cavp/documents/CAVPFAQ.pdf .

1.6.2 Federal Information Processing Standards and NIST Special Publications for Cryptographic Algorithms

Each approved and recommended cryptographic algorithm has an associated reference called a Federal Information Processing Standard (FIPS) or a Special Publication 800 series. These documents will be referred to as *references*. The detailed instructions on how to implement the specific algorithm are found in these references.

All cryptographic algorithm references for which the CAVP has developed cryptographic algorithm validation testing are available online on the official CAVP website at http://csrc.nist.gov/groups/STM/cavp/standards.html. A complete list of FIPS standards and NIST Special Publications is available at http://csrc.nist.gov/publications/index.

1.6.3 Validation Systems

Based on the specifications in the cryptographic algorithm reference, the CAVP designs and develops validation test suites that verify that the components of an algorithm are implemented correctly and completely. These tests exercise the mathematical formulas involved in the algorithm to ensure that they work properly for each possible scenario. If the implementation deviates from the reference or excludes any of the specified components, the validation tests will fail indicating an implementation flaw.

The validation systems are posted on the official Cryptographic Algorithm Validation Program website at http://csrc.nist.gov/groups/STM/cavp/index.html under the specific algorithm.

1.6.4 CST Laboratory Accreditation Standards

NIST standards for NVLAP accreditation of CST laboratories are published on the NVLAP website at http://ts.nist.gov/Standards/214.cfm. Links to these standards are also provided on the CMVP website http://csrc.ncsl.nist.gov/cryptval/labinfo.htm. The list of accredited testing laboratories is published on the CMVP website http://csrc.ncsl.nist.gov/cryptval/1401labs.htm.

These standards are:

1. NIST Handbook 150 (2006), *NVLAP Procedures and General Requirements,* http://ts.nist.gov/Standards/Accreditation/upload/nist-handbook-150.pdf; and
2. NIST Handbook 150-17 (2008), *NVLAP Cryptographic Module Testing,* http://ts.nist.gov/ts/htdocs/210/214/docs/hnbk-17.pdf.

Standards Council of Canada (SCC) standards for the accreditation of Canadian CST laboratories are published on the SCC website at http://www.scc.ca/en/publications/criteria/labs/index.shtml and include:

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

NVLAP accredits CST laboratories anywhere in the world.

The List of Accredited CST Laboratories (http://csrc.nist.gov/groups/STM/testing_labs/index.html and http://www.cse-cst.gc.ca/services/industrial-services/nvlap-e.html) contains the name of every CST laboratory accredited to perform cryptographic module and cryptographic algorithm testing. The list also includes a point of contact for each laboratory.

1.6.5 Other Documents on the CAVP Website

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

1. Announcements (http://csrc.nist.gov/groups/STM/cavp/announcements.html) contains information on changes made to documents or test tools pertinent to the Cryptographic Algorithm Validation Program.
2. Notices (http://csrc.nist.gov/groups/STM/cavp/notices.html) contains copies of statements published in the Federal Register and information indirectly related to the CAVP.
3. Standards (http://csrc.nist.gov/groups/STM/cavp/standards.html) contains a list of all FIPS and Special Publications for which CAVP has validation testing or is developing testing. The list is organized by type of algorithm (symmetric, asymmetric, hashing, etc.) and includes a link to each reference.
4. Cryptographic Algorithm Validation Systems (located at http://csrc.nist.gov/groups/STM/cavp/index.html under the heading of the specific algorithm) contains the suite of validation tests for each FIPS-Approved and NIST-recommended

cryptographic algorithm. These suites of validation tests must be successfully completed to claim conformance to the associated cryptographic algorithm reference.

5. Validation Lists (http://csrc.nist.gov/groups/STM/cavp/validation.html) contains the most current information about validated cryptographic algorithm implementations. A separate list exists for each Approved cryptographic algorithm, both current and archived (e.g. DES).
6. Contacts (http://csrc.nist.gov/groups/STM/cavp/contacts.html) contains information for each employee currently working in the CAVP.

2 CAVP Management

2.1 Roles and Responsibilities of Program Participants

The various roles and responsibilities of the participants in the CAVP are illustrated in Figure 2-1 below.

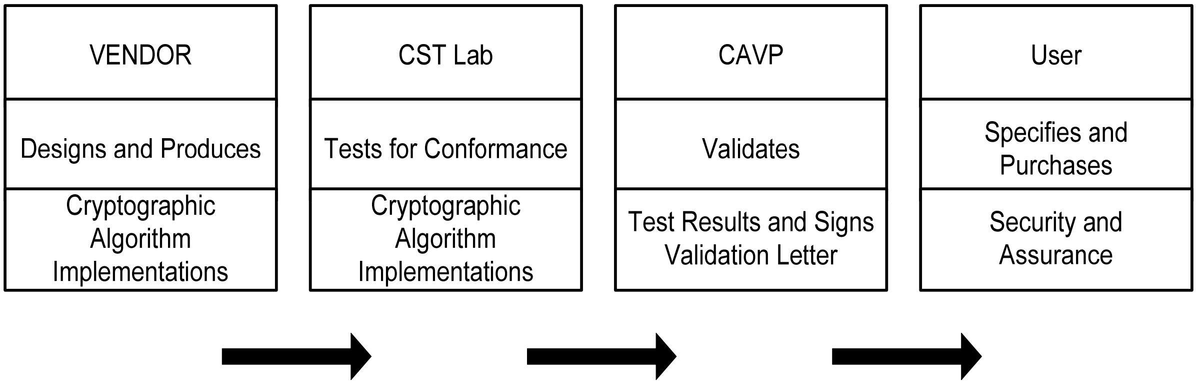

VENDOR
Designs and Produces
Cryptographic Algorithm Implementations
CST Lab
Tests for Conformance
Cryptographic Algorithm Implementations
CAVP
Validates
Test Results and Signs Validation Letter
User
Specifies and Purchases
Security and Assurance

Figure 2-1: Roles and Responsibilities in the CAVP

2.1.1 Vendor

The role of the vendor is to implement cryptographic algorithms that comply with the requirements specified in the applicable FIPS or NIST Special Publications. When a cryptographic algorithm implementation is ready for testing, the vendor selects a CST laboratory to validate their implementation. The CST laboratory assists the vendor in the validation process. Note that a vendor's implementation can be tested in-house by the vendor or it can be sent to the laboratory for testing by the laboratory.

If a modification is made to an existing validated cryptographic algorithm implementation, it is the vendor's responsibility to get the new implementation validated.

2.1.2 CST Laboratory

The role of the CST laboratory is to independently test cryptographic algorithm implementations. The laboratory uses the Cryptographic Algorithm Validation System (CAVS) testing tool and the individual algorithm validation systems (containing the implementation instructions for the required validation test suite), provided by NIST, to assist in the validation process. The CST laboratory requests pertinent information from the vendor concerning the implementation being tested. The laboratory then generates input vectors for each implemented algorithm. As mentioned in Section 2.1.1, the tester of the cryptographic algorithm implementation can be the vendor or the laboratory. If the vendor is the tester, the laboratory sends the input vectors to the vendor for testing. The vendor sends the resulting answers back to the laboratory. If the validation testing is being performed by the laboratory, the laboratory implements the appropriate algorithm validation systems. Using the vendor's implementation and the input test vectors, the laboratory runs the algorithm tests obtaining the test results from the cryptographic algorithm implementations.

The laboratory uses the CAVS tool to check the results for accuracy. If the results are not correct, the CAVS tool records which test failed and why. The laboratory informs the vendor that the implementation does not meet the requirements of the associated reference and provides the information generated by CAVS to assist the vendor in determining where their algorithm implementation deviates from the algorithmic specifications.

The laboratory contacts the CAVP when the implementation has successfully passed the validation testing.

CST laboratories must exercise due diligence when performing validation 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 or from the CSEC website at http://www.cse-cst.gc.ca/services/industrial-services/nvlap-e.html. The accreditation process for CST laboratories is briefly described in Section 3: CST Laboratory Processes of this manual.

2.1.3 CAVP Validation Authorities

The CAVP Validation Authorities are the National Institute of Standards and Technology for the Government of the United States of America and the Communications Security Establishment Canada for the Government of Canada.

The validation authorities are responsible for providing uniform validation testing for implementations of FIPS Approved and NIST recommended (referred to as Approved) cryptographic algorithms. This is accomplished by designing validation systems for every Approved cryptographic algorithm. The validation systems consist of a suite of validation tests necessary to thoroughly test the components of the cryptographic algorithm.

The validation authorities produce a validation system document describing the validation test suite. The validation system documents are posted on the CAVP website for use by end users.

The NIST CAVP validation authority designs, implements and maintains the Cryptographic Algorithm Validation System (CAVS) testing tool. CAVS is provided only to the accredited CST laboratories for cryptographic algorithm validation testing. All new validation systems produced by the validation authorities are implemented in the CAVS tool to provide the new testing. One feature of the CAVS tool assists the validation authority in the final validation of an implementation. This is the creation of a summary and log file which summarizes the tests performed and the success or failure of this test.

The NIST CAVP Validation Authorities receive the output of the CAVS tool from the CST laboratories. They use the summary and log files to assure the successful validation of the cryptographic algorithm implementation. If the cryptographic algorithm implementation is determined to be compliant with the associated cryptographic algorithm reference, then the implementation is validated and the online validation list is updated. If the results are not correct, the validation authorities work with the submitting CST laboratory to resolve any discrepancies.

2.1.4 User

The user verifies that a cryptographic algorithm implementation inside a cryptographic module or a product that he/she is considering purchasing has been validated. The listing of validated cryptographic algorithm implementations is located at http://csrc.nist.gov/groups/STM/cavp/validation.html. The listing of validated cryptographic module implementations is located at http://csrc.nist.gov/groups/STM/cmvp/validation.html. These validation lists contain the most current information about validated cryptographic algorithm implementations. A separate list exists for each Approved cryptographic algorithm.

3 CST Laboratory Processes

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

3.1 Accreditation of CST Laboratories

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

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

3.1.1 Recognized Standards and Standard Accreditation Bodies

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

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

3.1.2 Accreditation Process

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

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

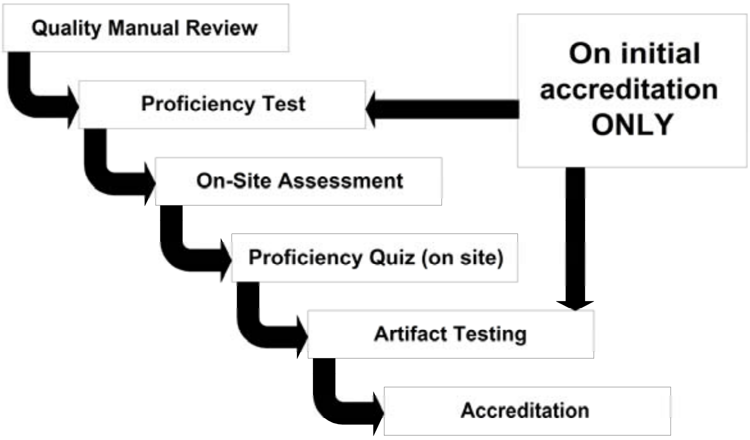


Figure 3-1: CST Laboratory Accreditation Process

3.1.2.1 Application for Accreditation and Selection of Assessment Team

The prospective CST laboratory must complete an application form, pay the respective fees, agree to conditions for accreditation, and provide a quality manual to NVLAP prior to the assessment process. Upon receipt of an application by NVLAP, an assessment team is selected mainly from the CMVP. This team is typically comprised of two representatives from NIST and one representative from CSEC. NVLAP technical assessors for CST laboratories are selected by the NVLAP Program Manager and are chosen based upon their knowledge of the relevant FIPS standards and related documentation, NVLAP requirements, assessment techniques, and quality systems. The assessors must not have a conflict of interest with the CST laboratory they will be assessing.

3.1.2.2 Quality Manual Review

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

3.1.2.3 CST Proficiency Examination

A CST Proficiency Examination will be administered to the applicant laboratory. The examination consists of approximately thirty questions relating to various aspects of CST laboratory activities, FIPS 140-2, and cryptographic algorithm implementation testing. The applicant laboratory is provided seven days to complete the exam. The assessing team will grade the exam and determine if the laboratory is competent.

3.1.2.4 On-Site Assessment

An on-site assessment of the laboratory is conducted to determine compliance with the accreditation criteria. The on-site assessment is scheduled by the assessment team following receipt of payment and a passing grade on the CST Proficiency Examination. An on-site assessment typically takes two 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 on-site assessment of an accredited CST laboratory, the laboratory must submit a satisfactory plan to NVLAP concerning resolution of deficiencies within thirty days of notification.

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

3.1.2.5 Proficiency Quiz

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

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. There is no set time limit to complete the testing. Once completed, the applicant laboratory must submit the test report to the assessment team for their review. The assessment team will then assess the competency of the laboratory from 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 not grant 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 a 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 CAVP Test Tools

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

3.2 Maintenance of CST Laboratory Accreditation

3.2.1 Proficiency of CST Laboratory

CST laboratories must submit at least one cryptographic module validation test report and one cryptographic algorithm validation submission during their accreditation cycle in order for the CMVP/CAVP staff to monitor the quality of the laboratory processes, and the technical skills and knowledge of the laboratory staff. Failing this, NVLAP will perform a new on-site assessment, monitoring visit, and/or proficiency test of the laboratory.

3.2.2 Renewal of Accreditation

The accreditation is valid for one year. Each accredited CST laboratory will receive a renewal application package before the expiration date of its accreditation to allow sufficient time to complete the renewal process. Fees for renewal are charged to the laboratory in accordance with the fee schedule published by NIST on the NVLAP website at http://ts.nist.gov/Standards/Accreditation/feesch.cfm. Both the application and fees must be received by the accreditation body prior to expiration of the laboratory's current accreditation to avoid a lapse in accreditation.

On-site assessments of accredited laboratories are performed in accordance with the procedures in section 3.2 of NIST Handbook 150. The re-accreditation process is the same as illustrated in Figure 3-1: CST Laboratory Accreditation Process and described in Section 3.1.2: Accreditation Process, except that the Proficiency Examination and the Artifact Testing steps are not performed. If deficiencies are found during the on-site assessment of an accredited laboratory, the laboratory must submit to NVLAP a satisfactory plan outlining the resolution of deficiencies within thirty days of notification.

3.2.3 Ownership of a CST Laboratory

In the event that a CST laboratory changes ownership, the accreditation body and the CMVP Validation Authorities must be informed within ten (10) working days of the identity of the new owner of the laboratory and the effective date of the change. The laboratory must also submit an update to the Quality Manual to NVLAP showing the new owner information.

3.2.4 Relocation of a CST Laboratory

In the event that a CST laboratory relocates to a new facility, the laboratory director must submit a relocation plan to the accreditation body and the CMVP at least one month before the relocation. The relocation plan must demonstrate that the new location meets the requirements as set out in the accreditation standards including information protection. The plan must also describe how sensitive information will be moved between locations.

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

3.2.5 Change of Approved Signatories

In the event of a change of the CST laboratory’s Approved Signatories, the accreditation body and the CMVP must be informed within ten (10) working days of the new signatories and the effective date of the change. The laboratory must also submit, if necessary, an update to the Quality Manual to NVLAP showing the new signatory information.

3.2.6 Change of Key Laboratory Testing Staff

In the event of changes to key laboratory testing staff, the accreditation body and the CMVP must be informed of the new staff and the effective date of the change within ten (10) working days. The laboratory must also submit, if necessary, an update to the Quality Manual to NVLAP showing the changes.

3.2.7 Monitoring Visits

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

3.2.8 Suspension, Denial and Revocation of Accreditation

If the accreditation body becomes aware that an accredited laboratory has violated the terms of its accreditation, it may suspend the laboratory’s accreditation or advise the laboratory of their intent to revoke the accreditation. The determination by the accreditation body whether to suspend the laboratory or to propose revocation of a laboratory’s accreditation will depend on the nature of the violation(s). Potential violations include but are not limited to, not performing tests in accordance with the standards, inadequate maintenance of CST laboratory equipment, or persistent process or technical shortfalls.

Discovery of serious violations such as breach of information confidentiality will result in an immediate recommendation by the NIST CMVP Director and CSEC Head 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 CAVP and CMVP provided material, test tools and documentation.

3.3 Confidentiality of Proprietary Information

Confidentiality of proprietary information is paramount to the operation of the CAVP and requires the establishment and enforcement of appropriate controls.

3.3.1 Confidentiality of Proprietary Information Exchanged between NIST, CSEC and the CST Laboratory

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

3.3.2 Non-Disclosure Agreement for Current and Former Employees

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

3.4 Code of Ethics for CST Laboratories

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

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

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

6. *to reject bribery in all its forms;*
7. *to treat others with dignity and professional courtesy;*
8. *to avoid injuring others, their property, reputation, or employment by false or malicious action; and*
9. *to assist co-workers in their professional development and to support them in abiding by this code of ethics.*

3.5 Management of CAVP Test Tools

Testers, or any other member of the laboratory, shall not distribute any of the test tools provided by NIST and CSEC to any entity outside the CST laboratory. This includes all versions of the Cryptographic Algorithm Validation System (CAVS) test tool and any other tools developed by NIST and CSEC for use by the CAVP. Violation of this policy may be considered cause for suspension of the CST laboratory's accreditation.

3.6 Design and Testing of Cryptographic Algorithm Implementations

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

1. a CST laboratory may not perform validation testing on an implementation for which the laboratory has:
   a. designed any part of the module;
   b. developed original documentation for any part of the implementation;
   c. built, coded or implemented any part of the implementation; or
   d. any ownership or vested interest in the implementation.
2. provided that a CST laboratory has met the above requirements, the laboratory may perform validation testing on implementations produced by a company when:
   a. the laboratory has no ownership in the company;
   b. the laboratory has a completely separate management from the company; and
   c. business between the CST laboratory and the company is performed under contractual agreements, as done with other clients.
3. a CST laboratory may perform consulting services to provide clarification to FIPS or Special Publications, and other associated documents at any time during the life cycle of the implementation.

4 Cryptographic Algorithm Validation Program Processes

This section provides a high-level overview of the cryptographic algorithm validation processes.

4.1 Definition of Cryptographic Algorithm Implementation

A cryptographic algorithm implementation is an entity that implements one or more cryptographic algorithms. The cryptographic algorithm boundary for this implementation is defined as the boundary encompassing the complete implementation. Each algorithm implementation has a unique associated name and version number (or part number).

A cryptographic algorithm validation involves the validation of a cryptographic algorithm implementation.

When an algorithm implementation is being validated for the first time, it is called a new implementation.

If a modification is made to anything within the cryptographic boundary of a validated cryptographic algorithm implementation, the implementation must be assigned a new version (or part) number and be validated as a new implementation. Examples of modifications made within the cryptographic boundary may include adding a new cryptographic algorithm implementation, adding a new attribute to an existing cryptographic algorithm implementation (example, for AES, adding CFB mode), making modification to code not related to any of the algorithm implementations, etc. Because a new version (or part) number is associated with this implementation and everything within the cryptographic boundary is being tested, this is called a new implementation.

Every cryptographic algorithm included in a cryptographic algorithm implementation does not have to be tested at the same time. Only those attributes validated will be recognized by the CAVP validation. If a vendor has a previously validated implementation that has not been modified since the official validation date, that vendor can validate additional attributes without getting the complete implementation validated. This is called an update to an existing implementation.

4.2 Cryptographic Algorithm Validation Process Overview

Approved cryptographic algorithm implementations are tested and validated separately from FIPS 140-2 cryptographic module testing. Cryptographic algorithm validation is a prerequisite to cryptographic module validation. Cryptographic algorithm testing may be performed concurrently with cryptographic module validation testing.

Figure 4-1 Cryptographic Algorithm Validation Testing Process shows the general flow of testing and validation of a cryptographic algorithm implementation to its associated FIPS or Special Publication.

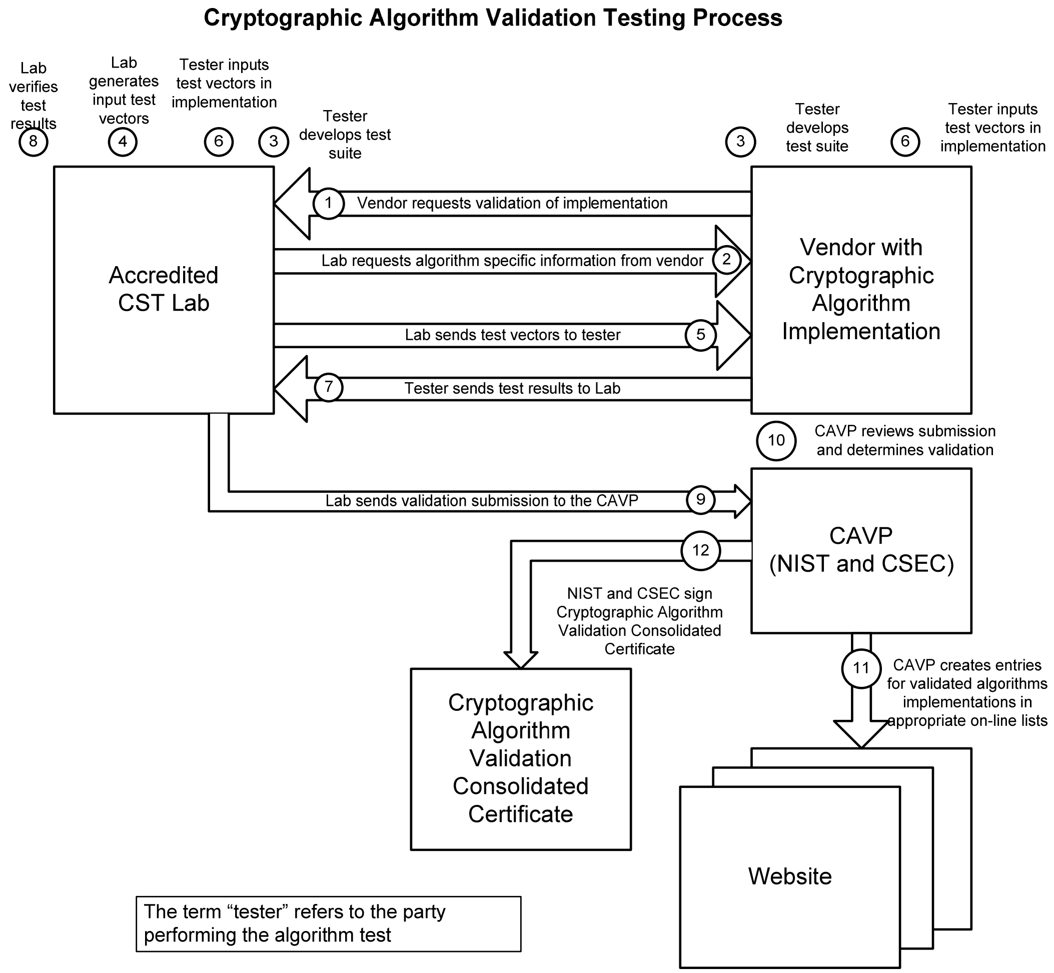

Cryptographic Algorithm Validation Testing Process
Lab verifies test results
8
Lab generates input test vectors
4
Tester inputs test vectors in implementation
6
3
Tester develops test suite
3
Tester develops test suite
6
Tester inputs test vectors in implementation
Accredited CST Lab
1
Vendor requests validation of implementation
Lab requests algorithm specific information from vendor
2
Vendor with Cryptographic Algorithm Implementation
Lab sends test vectors to tester
5
7
Tester sends test results to Lab
10
CAVP reviews submission and determines validation
Lab sends validation submission to the CAVP
9
CAVP (NIST and CSEC)
12
NIST and CSEC sign Cryptographic Algorithm Validation Consolidated Certificate
11
CAVP creates entries for validated algorithms implementations in appropriate on-line lists
Cryptographic Algorithm Validation Consolidated Certificate
Website
The term "tester" refers to the party performing the algorithm test

Figure 4-1: Cryptographic Algorithm Validation Process

The steps for the cryptographic algorithm validation process include (Refer to Figure 4-1):

Step 1. The vendor selects one of the accredited CST laboratories to oversee the algorithm validation testing of their cryptographic algorithm implementation. Note that the cryptographic algorithm implementation can be tested in-house by the vendor or it can be sent to the CST laboratory for testing (the term "tester" refers to the party performing the algorithm test).

Step 2. The CST laboratory requests information related to each cryptographic algorithm to be tested in the implementation.

Step 3. Using the validation system document, the tester implements the validation system test suite using the vendor's algorithm implementation.

Step 4. For each algorithm being tested, the CST laboratory uses this information and the Cryptographic Algorithm Validation System (CAVS) tool to generate input test vectors to be used in the validation tests.

Step 5. CST laboratory supplies the input test vectors to the tester.

Step 6. The tester uses the test vectors as inputs into the implementation.

Step 7. The results are forwarded to the CST laboratory.

The CST laboratory uses the CAVS tool to verify the results of the validation tests. If the results are not correct, the CAVS tool records which test failed and why. The laboratory informs the vendor that the implementation does not meet the requirements of the associated reference and provides the information generated by CAVS to assist the vendor in determining where their algorithm implementation deviates from the specifications in the reference.

Step 8. When the cryptographic algorithm implementation validation test successfully passes, the CST laboratory submits an algorithm validation submission request package to NIST. This package contains the official validation request from the laboratory and all the files generated from the CAVS tool including a file summarizing the validation test results for each algorithm tested.

Step 9. NIST reviews the package for completeness and verifies that all the tests have passed. If this is true, NIST and CSEC validate the implementation.

Step 10. NIST enters all pertinent information related to this validation into an internal database that generates the Cryptographic Algorithm Validation Consolidated Certificate (which contains multiple cryptographic algorithm implementations). NIST signs this certificate and sends it to CSEC for their signature.

Step 11. Once validated, the cryptographic algorithm implementation is posted to the CAVP website at http://csrc.nist.gov/groups/STM/cavp/validation.html. A separate cryptographic algorithm validation list exists for each Approved cryptographic algorithm for which NIST has testing available.

4.3 Testing of the Cryptographic Algorithm Implementation

A vendor contracts with an accredited CST laboratory to oversee the validation of the cryptographic algorithm implementation (Step 1). The laboratory requests information related to the cryptographic algorithm being tested (Step 2). This information includes:

Vendor information:

- Name
- Website
- Address
- Point of contact

Cryptographic algorithm implementation info:

- Implementation name
- Version number
- Implementation type (hardware, software or firmware)
- Implementation description

Operating environment:

- If the implementation type is software:
  - Processor and operating system
- If the implementation type is firmware:
  - Processor
- If the implementation type is hardware
  - Part Number

Cryptographic Algorithm:

- Modes of operation
- Cryptographic Algorithm specific details

The vendor provides the laboratory with the necessary documentation and either provides the cryptographic algorithm implementation to the laboratory or prepares for it to be tested at the vendor's facility. (The party testing the implementation will be referred to as the tester).

The tester implements the suite of validation tests required to claim conformance to the specific algorithm reference as outlined in a validation system document for each algorithm (Step 3). These validation system documents are located on the official CAVP website at http://csrc.nist.gov/groups/STM/cavp/index.html under the specific algorithm. The validation tests utilize the cryptographic algorithm implementation. The validation test suite is designed to test the algorithm specifications, components, features, and/or functionality as specified in the algorithmic reference.

The laboratory uses the Cryptographic Algorithm Validation System (CAVS) tool and the information supplied by the vendor to generate input vectors for all the validation tests in the associated test suite (Step 4). The CAVS tool generates three types of file. The request file contains the input vectors to be used in the testing. The sample file contains the format required by the response file (generated by the vendor's cryptographic algorithm implementation). The request and sample files are sent to the tester (Step 5). The third file type generated by the CAVS, the FAX file, contains information needed by the CAVS tool to calculate the answer. This information is used to generate the answers and then to compare them against the cryptographic algorithm implementation's response file.

The tester inputs the test vectors into each validation test (Step 6). This exercises the different features implemented in the cryptographic algorithm implementation resulting in output values. These output values are stored in response files and returned to the CST laboratory (Step 7).

The CST laboratory loads the response files into the CAVS tool. The CAVS tool verifies that the correct answers were generated by the cryptographic algorithm implementation (Step 8). If any errors occur, the log file contains information pertaining to the error. Using the log file, the CST laboratory provides information to the vendor related to the error that occurred. Wrong answers may be the result of implementation flaws such as pointer problems, insufficient allocation of space, improper error handling, incorrect behavior of the algorithm implementation and/or test harness errors. The vendor can correct and resubmit their implementation for testing until the implementation test passes.

Once the implementation successfully passes all the validation tests, the CST laboratory notifies NIST by submitting an official cryptographic algorithm validation request (Step 9).

4.4 Cryptographic Algorithm Validation Request Submission

Two types of requests are submitted to NIST by the laboratories - new implementation submission requests and update/change requests on existing implementations. Both cryptographic algorithm validation request submissions contain an official request letter and all the files generated by the CAVS tool for a validated cryptographic algorithm implementation and all response files containing the algorithm test results. The official request letter is called the algorithm validation request letter for new implementations and the update/change request letter for updates and/or changes to existing implementations. This official request letter is the only legally binding deliverable NIST receives from the CST laboratory.

The official cryptographic algorithm validation request letter for new requests indicates that the laboratory has correctly performed the validation testing of a particular cryptographic algorithm implementation and that it requests the validation of the implementation. The request letter only contains information pertaining to a single implementation. It contains information defining the vendor, implementation name and version, and algorithms and features tested. This information is collected by the CAVS tool for use by the laboratory. It is in a file named <foldername>TestedInfo.txt. The information in the TestedInfo file can be cut and paste into the request letter. The request letter must be signed by an official signatory at the laboratory. It should be generated on the laboratory's letterhead.

The official update/change request letter indicates that a vendor has contacted the laboratory requesting updates and/or changes to an existing validated implementation. If additional testing was requested, this letter indicates that the laboratory has correctly performed this additional validation testing. If changes to vendor or implementation information was requested by the vendor, the laboratory will officially request that these changes be made.

The files generated by the CAVS tool, along with the validation request letter should be zipped into one file.

To submit a request:

a. Copy the contents of the request letter into an email message. In addition to this information, also include the name of the zip file containing the CAVS files. Use the naming convention specified in Section 4.4.1 and 4.4.2 for the file name.

b. For new requests, the subject line should read:

   (ITAR – if applicable; Not To Be Posted On CAVP Web Site – if applicable) New Implementation Submission (name of implementation)…

   For update/change requests, the subject line should read: Update/Change On Existing Implementation…

c. Send the email to the CAVP at CAVPVal@nist.gov.

d. Upload the zip file to the CAVP FTP server at ftp://ftp.nist.gov/pub/CAVPFiles/.

4.4.1 Contents of the Official Cryptographic Algorithm Validation Request Letter For New Implementation

The official cryptographic algorithm validation request letter shall include:

1. Laboratory information:
   a. Date submitting validation request;
   b. Subject line – Validation Request – New Implementation: <name of implementation>;
   c. Laboratory name; and
   d. Signature of official signatory for the testing laboratory.
2. Statement that the cryptographic algorithm validation request is for either a new cryptographic algorithm implementation or an update to an existing validated cryptographic algorithm implementation.
3. Information on the implementation tested. This information is collected by the CAVS tool for use by the laboratory. It is in a file named <foldername>TestedInfo.txt. The information in this file include
   a. CAVS tool information:
      i. CAVS Tool version used to test the implementation.
   b. Vendor and implementation information as discussed in Section 4.3.
   c. If applicable, indication that the implementation is subject to the U.S. Department of State's International Traffic in Arms Regulations (ITAR).
   d. Other special processing requests
   e. List of algorithms that have been tested along with the individual components of each of the algorithms that have been tested.

   f. Supporting algorithms used by this implementation (prerequisites) and their associated certificate number (if it has been assigned). If the certificate number has not been assigned, indicate this and why – for example, “has not been assigned a certificate number because it is being validated in this implemented”.

4. Special notes pertaining to this validation. If the note is for the complete submission, indicate it here. If it is a special note for a specific algorithm, please indicate this information along with the algorithm information.
5. The name of the submission is the name of the zip file that the Lab uploads to CAVP ftp server.

4.4.2 Contents of the Official Cryptographic Algorithm Validation Request Letter for Update/Change Request For Existing Implementation

The official cryptographic algorithm validation update/change request letter shall include:

1. Laboratory information:
   a. Date submitting request;
   b. Subject line – Update/Change Request On Existing Implementation: <name of implementation>;
   c. Laboratory name; and
   d. Signature of official signatory for the testing laboratory.
2. Testing tool information:
   a. CAVS version used to test the implementation
3. Vendor information:
   a. Vendor name
4. Current implementation information:
   a. Algorithm certificate numbers; and
   b. Current postings of each field, which needs to be updated
5. Update information:
   a. Updated information for each field
   b. Statement on any changes within the algorithm boundary

For the update request, which adds new OSs or processors or part number(s) to the existing implementation also needs to provide the testing information and testing results, see Sections 4.3 and 4.4.1.

4.4.3 Instructions for Uploading the Zip file to the CAVP FTP server:

1. Type the address: *ftp://ftp.nist.gov/pub/CAVPFiles/* and press enter. Notice that the laboratories can only put files out on this directory; they can not see the files that are out there.

2. Drag and drop the zip file to the white space on this screen. The file will be visible only until the screen is refreshed, then it will disappear. This is the correct operation of this screen.

4.5 Role of NIST and CSEC in the Cryptographic Algorithm Validation Process

NIST receives the official cryptographic algorithm validation submission packages from all of the CST laboratories via email (CAVPVal@nist.gov) and FTP. The proper format for the contents of the submission package is in Section 4.4. Submission requests are processed on a first come, first serve basis. NIST reviews the validation submission package for completeness and validates that all the validation tests for each algorithm supported by the implementation under test have passed (Step 10). If the submission package has not been submitted properly (see Section 4.4), if the submission is incomplete or if all the validation tests have not run successfully, NIST stops processing this validation request and informs the CST laboratory to complete and resubmit the request. This submission request is deleted from the CAVP queue.

If the submission is complete and everything has tested successfully, the cryptographic algorithm implementation is added to the CAVP internal database (Step 11). The CAVP internal database contains all information pertaining to all cryptographic algorithm implementation validations. This information includes vendor information, implementation information, individual algorithm attribute information and the official Validation Date which reflects the date the NIST Validation Authority approves the validation. Periodically, all validated cryptographic algorithm implementations that have not been assigned a validation date are consolidated into a document (generated by the internal database) called the Cryptographic Algorithm Validation Consolidated Certificate. The consolidated certificate is sent to the NIST Validation Authority who reviews the algorithm implementation validation information and signs and dates the consolidated certificate. This date becomes the official validation date for all algorithm validations contained in this certificate. Once signed by the NIST Validation Authority, the validated cryptographic algorithm implementation is added to the applicable on-line validated cryptographic algorithm implementation list on the CAVP website and, the consolidated certificate is sent to CSEC for their review and signature. This document is scanned by CSEC and returned to NIST for their records (Step 12).

4.5.1 Cryptographic Algorithm Validation Consolidated Certificate

In January, 2008, the Cryptographic Algorithm Validation Consolidated Certificate became the official validation record for cryptographic algorithm implementations. The consolidated certificate contains the following information for each validated implementation:

a. the algorithm validation consolidated certificate letter tracking number;

b. the cryptographic algorithm;

c. the algorithm certificate number;

d. implementation name;

e. version/part number;

f. vendor name;

g. NIST official signature and date; and

h. CSE official signature and date.

NIST and CSEC no longer issue certificates for individual cryptographic algorithms.

4.6 The Cryptographic Algorithm Validation System (CAVS) Tool

The Cryptographic Algorithm Validation System (CAVS) tool is provided only to the accredited CST Laboratories for cryptographic algorithm validation testing. This tool is designed to provide *uniform* validation testing for implementations of Approved cryptographic algorithms.

For each FIPS-Approved and NIST-recommended cryptographic algorithm, a validation test suite is designed by the CAVP to test the algorithm specifications, components, features, and/or functionality as specified in the algorithmic reference. These test suites are incorporated into the CAVS tool. An interface for each algorithm requests all the information needed to perform the validation tests for that algorithm. Test vectors are generated and placed in request files which are given to the tester along with sample files which contain file formatting information. The cryptographic algorithm implementation computes the resulting answers to these test vectors and stores them in the specified format in response files which are returned to the laboratory. The CAVS tool verifies that the cryptographic algorithm implementation computed the correct values by comparing the implementation's values to the expected answers.

During this process, the CAVS tool generates a summary and a log file. The summary file indicates which tests were run and whether or not they passed successfully. The number of successful answers out of the total answers expected is recorded. If a failure occurs, the log file will indicate which value failed and possibly why it failed. The CST laboratories use these files to provide to the vendor information related to error that occurred which will help the vendor fix its cryptographic algorithm implementation. If an error occurs, the cryptographic algorithm implementation must regenerate all values after the implementation error is fixed. The CST laboratories use the CAVS tool to verify the values again.

4.7 CAVP Internal Database

The CAVP Internal Database contains all the information pertaining to every cryptographic algorithm implementation that has been validated. It automates many of the NIST processes involved in the validation of a cryptographic algorithm implementation. A separate table is contained in the database for each algorithm containing pertinent information for that algorithm. Data is automatically imported into the database via a file generated by the CAVS tool. The database automatically generates the following reports: the Cryptographic Algorithm Validation Consolidated Certificate, monthly CAVP validation process status chart, tables with actual numbers for each validated algorithm for each fiscal year, and the on-line validated cryptographic algorithm implementation list for each cryptographic algorithm.

4.8 Requests for CAVP Guidance to NIST and CSEC

CAVP guidance can be separated into several categories:

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

Test-specific Questions: These are questions concerning specific test issues of the CAVP. These issues may be technology related or related to areas of the FIPS or Special Publication reference that may appear to be open to interpretation.

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

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

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

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

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

Informal Request: Informal requests are considered as ad hoc questions aimed at clarifying issues about the cryptographic algorithm references and testing as well as other aspects of the CAVP. Replies to informal requests by the CAVP are non-binding and subject to change. It is recommended that informal requests be submitted to all points of contact. Every attempt is made to reply to informal requests with accurate, consistent, clear replies in a timely manner.

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

Request for Guidance (RFG) Format: Questions submitted in this format will result in an official response from the CAVP that will state current policy or interpretations. This format provides the CAVP a clear understanding of the question. A RFG shall have the following items:

1. Clear indication of whether the RFG is PROPRIETARY or NON-PROPRIETARY;
2. A descriptive title;
3. Applicable statement(s) from FAQ CAVP;
4. Applicable statements from cryptographic algorithmic references;
5. Background information if applicable, including any previous CMVP or CAVP official rulings or guidance;
6. A concise statement of the problem, followed by a clear and unambiguous question regarding the problem; and
7. A suggested statement of the resolution that is being sought.

All questions should be presented in a detailed and implementation-specific format, rather than an academic or hypothetical format. This information should also include a brief non-proprietary description of the implementation. This will enable a more efficient and timely resolution of cryptographic algorithm related questions by the CAVP. The statement of resolution shall be stated in a manner which the CAVP can either answer *YES* or *NO*. The CAVP may optionally provide its rationale if the answer is not in line with the suggested statement of resolution.

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

RFGs from CST laboratories are placed in a queue and answered in order. Responses to the RFGs are coordinated and agreed upon by both NIST and CSEC. RFGs should be addressed to, at a minimum, the following contacts. Other contacts in the CAVP can also be notified.

NIST
Sharon Keller
Director, Cryptographic Algorithm Validation Program
Computer Security Division
National Institute of Standards and Technology

CSEC
Jean Campbell
Head, Cryptographic Module Validation Program
Industry Program Group
Communications Security Establishment Canada
(613) 991-8121

(301) 975-2910 jean.campbell@cse-cst.gc.ca
sharon.keller@nist.gov

4.9 CAVP Website

This section describes the information available on the CAVP website.

4.9.1 CAVP Home Page

The official CAVP website, located at http://csrc.nist.gov/groups/STM/cavp/index.html, contains current publicly-available information concerning the Cryptographic Algorithm Validation Program. This section contains a brief overview of the CAVP, followed by the cryptographic algorithm validation specifications for each algorithm for which the CAVP currently has validation testing. Each algorithm section consists of links to:

- the cryptographic algorithm FIPS or Special Publication (discussed in Section 4.9.4 – Standards),
- the algorithm validation test suite specification (the Validation System document). This document defines the suite of validation tests designed to exercise all aspects of the algorithm to give assurance that it has been implemented correctly,
- the algorithm validation list (discussed in Section 4.9.5 – Algorithm Validation Lists), and
- the test vectors. The test vectors contain the inputs and expected outcomes of each validation test. These test vectors can be used to informally verify the correctness of the algorithm implementation and the harness to perform the validation tests before having the implementation tested by a laboratory. Use of these vectors does not take the place of validation obtained through the CAVP.

The CAVP home page also contains the most recent announcement and notice, making this information readily accessible.

4.9.2 Announcements

This webpage contains announcements concerning the CAVP. An example would be the announcement of a new release of the CAVS tool.

4.9.3 Notices

This webpage contains notices concerning the CAVP.

4.9.4 Standards

This webpage provides links to the FIPS and Special Publications for all cryptographic algorithms for which the CAVP currently has validation testing. The direct link to this page is http://csrc.nist.gov/groups/STM/cavp/standards.html.

4.9.5 Algorithm Validation Lists

This webpage provides links to algorithm validation lists for each algorithm for which the CAVP currently has validation testing. These validation lists contain information pertaining to each cryptographic algorithm implementation that has successfully completed the validation process. The direct link to this page is http://csrc.nist.gov/groups/STM/cavp/validation.html. Algorithm validation lists are updated on at least a weekly basis. They are updated when new cryptographic algorithm implementations are validated or when a change request is approved.

In addition to the validated cryptographic algorithm implementations, this website also contains several validation lists for algorithms that are no longer recognized or for algorithms where testing is no longer performed. These lists are provided for historical purposes only. The DES algorithm is no longer recognized as an Approved security function. And testing is no longer specifically performed for FIPS 113, *Computer Data Authentication* nor FIPS 171, *Key Management Using ANSI X9.17*. Therefore the *MAC Validation List* and the *FIPS 171 (ANSI X9.17 Key Management) Validation List* are no longer updated. These lists include:

- MAC validation list, http://csrc.nist.gov/groups/STM/cavp/validation.html
- DES validation list, http://csrc.nist.gov/groups/STM/cavp/validation.html
- FIPS 171 (ANSI X9.17 Key Management) validation list, http://csrc.nist.gov/groups/STM/cavp/validation.html.

4.9.6 Contacts

This site contains the names and contact information for each person in the CAVP. The direct link to this page is http://csrc.nist.gov/groups/STM/cavp/contacts.html.

4.9.7 FAQ

This webpage contains a compilation of frequently asked questions received from the CST laboratories relating to the validation of cryptographic algorithm implementations.

This is intended for use by the CST laboratories and vendors when going through the validation testing process. Questions range from general CAVP operations questions to algorithm specific questions. A direct link to this document is http://csrc.nist.gov/groups/STM/cavp/documents/CAVPFAQ.pdf

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 CAVP metrics.

5.1 Overview

The CMVP and CAVP Programmatic Metrics Collection process is indented to document the quality performance of the testing processes of the CAVP 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 CAVP. 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 CAVP/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 CAVP metrics will be collected by each CST laboratory for cryptographic algorithm implementations undergoing validation:

- Vendor and implementation name;
- Algorithm;
- Type of the implementation;
- Certificate number;
- Validation date;
- Determination whether the vendor already has a validated implementation; and
- Determination whether the algorithm implementation failed on the first testing.

5.4 Reported Metrics

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

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

- The number of certificates issued for cryptographic algorithm implementation; and
- The number of cryptographic algorithm implementations which failed the initial testing.

5.5 Metrics Reporting

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

The CAVP/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 CAVP/CMVP. For each query performed, the laboratory has to send to CAVP/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 CAVP/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 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 implementation can not be preserved.

5.7 Metrics Submission

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

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

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

6 Documentation and Test Tool Maintenance Processes

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

6.1 FAQ

The CAVP FAQ is updated whenever new guidance is created. Questions asked by CST laboratories are resolved and transformed into general guidance and added to the CAVP FAQ.

6.2 Cryptographic Algorithm FIPS and NIST Special Publications

The CAVP provides validation testing for Approved cryptographic algorithms. Approved cryptographic algorithms are defined as those specified in Federal Information Processing Standards (FIPS) and in NIST Special Publications (SPs). NIST formally reevaluates cryptographic algorithm FIPS and SPs every five years. Both standards and possible threats reducing the security provided through the use of a standard will undergo review by NIST as appropriate, taking into account newly available analysis and technology. In addition, the awareness of any breakthrough in technology or any mathematical weakness of the algorithm will cause NIST to reevaluate the standard and provide necessary revisions as necessary.

Please refer to the Security Technology Group at csrc.nist.gov for a list of the documents including the cryptographic algorithm standards and Special Publications: http://csrc.nist.gov/publications/index.html and http://csrc.nist.gov/CryptoToolkit/. A link to the cryptographic algorithm documents for which the CAVP has validation testing is also included on the CAVP official website (http://csrc.nist.gov/groups/STM/cavp/index.html) in the appropriate section.

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 CAVP official website, and implemented.

Responsible Positions: NIST’s Cryptographic Technology Group.

6.3 Cryptographic Algorithm Testing Instructions

Cryptographic algorithm testing instruction documents are created as automated tests are developed for FIPS-Approved and NIST-recommended cryptographic algorithms. They may be modified if an error is discovered in the provided instructions, especially if the error results in confusion for individuals developing the implementation or executing tests on the cryptographic algorithm.

In some cases, companion instruction documents may be created for additional tests for one or more cryptographic algorithms.

Cryptographic algorithm testing instruction documents may become irrelevant if the cryptographic algorithm is no longer Approved for use or the testing or test files have been significantly modified.

Cryptographic algorithm test instructions are posted on the same page as the reference for the cryptographic algorithm to which the instructions apply.

Responsible Position: Director NIST CAVP.

6.4 Test Tools

6.4.1 Cryptographic Algorithm Validation System

A major version (primary number changed) of the CAVS test tool is created and released to CST laboratories whenever new cryptographic algorithm testing is added to the test tool or a major change is made in its functioning.

A minor (decimal number changed) version of the CAVS test tool may be created and released for minor changes in operation and/or bug fixes. A summary of the changes for the released version of the CAVS tool accompany the tool.

When a new version of the CAVS tool is released to CST laboratories, the laboratories must immediately begin using the new version to generate input vectors for all NEW cryptographic algorithm validation requests. For current cryptographic algorithm implementations that are in the process of being validated, using a previous version of the CAVS tool (i.e. input vectors have been generated by a previous version of the CAVS tool AND have already been sent to the vendor), the vendor is allowed a transition period of approximately three months to return the cryptographic algorithm validation test results to the laboratory for validation. The CST laboratory should contact those vendors or the vendor’s representative to inform them that the cryptographic algorithm validation files supplied to them will expire at the end of the transition period. If the vendor or the vendor’s representative fails to return the results within this transition period, the input vectors will expire. The laboratory would then generate new input vectors using the current CAVS tool and resend them to the vendor for the cryptographic algorithm validation testing.

Responsible Position: Director NIST CAVP.

6.4.2 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 CAVP Validation Authorities prior to the development of the release. A summary of the changes made for the released version of the METRIX tool accompany the tool.

Responsible position: Head CSEC CMVP

6.4.3 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.

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

Responsible position: Head CSEC CMVP

6.5 CAVP Management Manual

The *CAVP Management Manual* is revised as necessary and posted on the official CAVP website. It will also be reviewed annually.

Responsible Position: Director NIST CAVP and Head CSEC CMVP.

6.6 CST Laboratory Accreditation Standards

6.6.1 Handbook 150 – Procedures and General Requirements

It is essential for the mutual recognition of NVLAP-accredited laboratories by other laboratory accreditation bodies that NVLAP procedures maintain their consistency with international standards and guidelines. NVLAP signs Mutual Recognition Arrangement (MRA) or Multilateral Recognition Arrangement (MLA) agreements for organizations of laboratory accreditation bodies such as the International Laboratory Accreditation Cooperation (ILAC) group, the Asia Pacific Laboratory Accreditation Cooperation (APLAC) group, the Inter American Laboratory Accreditation Cooperation (IAAC) group, the European co-operation for Accreditation (EA) association, and the National Cooperation for Laboratory Accreditation (NACLA) group. Specifically, NVLAP procedures must be consistent with in the current version of ISO/IEC 17025: *General Requirements for the Competence of Testing and Calibration Laboratories* and ISO/IEC Guide 58: *Calibration and Testing Laboratory Accreditation Systems - General Requirements for Operation and Recognition*. Since these procedures are contained in Handbook 150, this Handbook must be updated as necessary. Handbook 150 may also need to be restructured from time to time so that it conforms to internationally accepted rules for the structure and drafting of standards and similar technical documents and ensure it is easy to understand and use.

Revisions to NIST Handbook 150 must be published in the US Federal Register and officially approved by the office of the U.S. Secretary of Commerce. The Forward of NIST Handbook 150 summarizes the changes made in the current edition of the handbook since the last published edition of the handbook. Handbook 150 is posted on the NVLAP website at http://ts.nist.gov/Standards/Accreditation/upload/nist-handbook-150.pdf and distributed to the NVLAP-accredited laboratories after publication.

Responsible Position: Chief of NVLAP.

6.6.2 Handbook 150-17 – Cryptographic and Security Testing

Handbook 150-17, as the program specific handbook for Cryptographic and Security Testing, is revised when there is a perceived need for its update identified by the Director of the NIST CMVP or the Program Manager for Information Technology Security Testing. Changes in this handbook are made in recognition of advancements in technology and tools or when a change is made in the general accreditation requirements for a Cryptographic and Security Testing laboratory or requirements for meeting a defined accreditation level.

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

Revisions to Handbook 150-17 are made by the Program Manager for Information Technology Security Testing. Handbook 150-17 is not available on-line.

Responsible Position: Program Manager, Information Technology Security Testing.

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

CAN-P-4E, *General Requirements for the Competence of Testing and Calibration Laboratories* is a verbatim Canadian adoption of ISO/IEC 17025: *General Requirements for the Competence of Testing and*

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

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

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

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

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

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

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

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

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

The purpose of CAN-P-1621 is to establish requirements, in addition to those specified in CAN-P-4E and in CAN-P-1591B, for technical and organizational matters for the SCC accreditation of testing facilities to perform the conformance testing of cryptographic modules to FIPS PUB 140-2, *Security Requirements for Cryptographic Modules* and the conformance testing of the associated cryptographic algorithms.

CAN-P-1621 is published on the Standards Council of Canada website at http://www.scc.ca/Asset/iu_files/criteria/1621_e.pdf.

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

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

Annex A: Abbreviations

ACT Canada	Advanced Card Technology Association of Canada
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
APLAC	Asia Pacific Laboratory Accreditation Cooperation
CAN-P	Canadian Publication
CAVP	Cryptographic Algorithm Validation Program
CAVS	Cryptographic Algorithm Validation System
CC	Common Criteria
CMVP	Cryptographic Module Validation Program
CMT	Cryptographic Module Testing
CSEC	Communications Security Establishment Canada
CST	Cryptographic and Security Testing
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
EA	European co-operation of Accreditation
ECDSA	Elliptical Curve Digital Signature Algorithm
FAQ	Frequently Asked Questions
FIPS	Federal Information Processing Standard
GC	Government of Canada
HMAC	Keyed-Hash Message Authentication Code
IAAC	InterAmerican Accreditation Cooperation
IEEE	Institute of Electrical and Electronics Engineers
ILAC	International Laboratory Accreditation Cooperation
ISO	International Organization for Standardization
ITSET	IT Security Evaluation and Test
IUT	Implementation Under Test
MAC	Message Authentication Code
MLA	Multilateral Recognition Arrangement
MRA	Mutual Recognition Arrangement
NACLA	National Cooperation for Laboratory Accreditation
NIST	National Institute of Standards and Technology
NSTISSP	National Security Telecommunications and Information Systems Security Policy

NVLAP	National Voluntary Laboratory Accreditation Program
PP	Protection Profile
RFG	Requests for Guidance
RNG	Random Number Generator
RSA	Rivest Shamir Adleman cryptographic algorithm
SBU	Sensitive but Unclassified
SCC	Standards Council of Canada
SHS	Secure Hash Standard
SP	Special Publication
STM	Security Testing and Metrics
Triple-DES	Triple Data Encryption Standard
FTP	File Transfer Protocol
Approved	NIST-Recommended and FIPS-Approved
Reference or Associated Reference	NIST Special Publication or FIPS