Enter Date: **Enter NVLAP Lab Code:**

NIST HANDBOOK 150-17 CHECKLIST
CRYPTOGRAPHIC AND SECURITY TESTING PROGRAM

Instructions to the Assessor: This checklist addresses specific accreditation requirements prescribed in NIST Handbook 150-17, *Cryptographic and Security Testing*. The numbering of the checklist items correlates to the numbering scheme in NIST Handbook 150-17, clauses 4 and 5.

Place an “X” beside any of the following items that represent a nonconformity. Place a “C” beside each item on which you are commenting for other reasons. Record the item number and your nonconformity explanation and/or comments on the appropriate sheet(s) at the end of this checklist. Write "OK" beside all other items you observed or verified as compliant at the laboratory.

In addition to this checklist, fill out the supplemental checklist(s) associated with the laboratory’s scope of accreditation. Please note that there are no additional requirements for 17BCS Basic Cryptographic and Security Testing outside those listed in the main body of the NIST Handbook 150-17; therefore, there is no additional checklist for this area.

The following supplemental checklists are available for this program:

- Cryptographic Algorithm and Cryptographic Modules Testing
- Personal Identity Verification Testing
- General Services Administration Precursor Testing
- Security Content Automation Protocol Testing
- DHS Identity and Privilege Credential Management Testing.

4 Management requirements for accreditation

4.1 Organization

___ 4.1.1 The laboratory shall establish and maintain policies and procedures for maintaining laboratory impartiality and integrity in the conduct of cryptographic and security testing. To avoid any conflict of interest, the laboratory policies and procedures shall ensure that neither the applicant laboratory nor other divisions within its parent corporation can perform conformance testing if it is currently providing or has previously provided consulting services to the vendor for the IUT or SUT (e.g., develop testing evidence, design advice).

___ 4.1.2 For any other services of the laboratory’s parent corporation not listed in the 4.1.1, the laboratory shall have an explicit policy and a set of procedures for maintaining a strict separation, both physical and electronic, between the laboratory testers and company’s consultant teams, product developers, system integrators, and others who may have an interest in and/or may unduly influence the testing outcome.

___ 4.1.3 A CST laboratory shall have no financial interest for the work performed under the present scope of accreditation other than its conformance testing and/or validation fees.

4.1.4 The laboratory shall not perform conformance testing on a module for which the laboratory has:

___ a) designed any part of the IUT or SUT;

___ b) developed original documentation for any part of the IUT or SUT;

___ c) built, coded or implemented any part of the IUT or SUT; or

___ d) any ownership or vested interest in the IUT or SUT.

___ 4.1.5 A CST lab may take existing vendor documentation for an IUT or SUT (post-design and post-development) and consolidate or reformat the existing information (from multiple sources) into a set format. If this occurs, the validation programs shall be notified of this when the conformance test report is submitted.

4.2 Management system

___ 4.2.1 The management system shall include policies and procedures to ensure the protection of proprietary information. The policies and procedures shall specify how proprietary information will be protected from persons outside the laboratory, from visitors to the laboratory, from laboratory personnel without a need to know, and from other unauthorized persons.

___ 4.2.2 The laboratory shall comply with all policies and procedures to ensure technical integrity of the conformance testing analyses and results.

___ 4.2.3 The reference documents listed in 1.4, the annex associated with the specific test methods, and the program's website, as well as any other standards and publications related to the CST LAP, shall be available to all appropriate personnel at all times.

4.4 Review of requests, tenders and contracts

___ 4.4.1 If the laboratory conducts testing at any selected site other than the laboratory's site accredited for conformance testing, the site shall meet all requirements pertinent to the conformance testing of the IUT or SUT as the accredited testing laboratory.

___ 4.4.2 Policies for documents storage and maintenance of contracts under confidentiality, non-disclosure agreements, marked as secret, or copyright protected, shall be well defined according to the document's status.

These documents shall be protected commensurate with their classification and/or sensitivity, and access to them shall be given only to authorized personnel.

___ 4.4.3 The testing laboratory and vendor shall agree, in writing, what constitutes the IUT or SUT and what constitutes the environment within the IUT.

[For this program, the environment includes, but it is not limited to:

- *the specific test platform;*
- *the test configuration; and*
- *the external environment.]*

4.5 Subcontracting of tests and calibrations

___ If subcontracting is used as a mechanism by which the laboratory fulfills and/or enhances the conformance testing process, the subcontracting laboratory shall employ either services provided only by NVLAP-accredited laboratories whose scope includes the applicable test method(s) or by laboratories that satisfy all testing requirements as indicated in the NIST Handbook 150, NIST Handbook 150-17 and all documents pertaining to the validation program.

In the later instance, the subcontracting laboratory:

a) shall justify the selection explaining why this particular subcontractor was selected and how the subcontractor satisfies the testing requirements; and

b) shall assume full responsibility for the outcome of the conformance testing performed by the subcontractor.

4.13 Control of records

4.13.1 General

___ 4.13.1.1 The laboratory shall maintain a functional record-keeping system for each customer. Records shall be readily accessible and complete.

Digital media shall be logged and properly marked, and they shall be properly and securely backed-up.

Entries in paper-based laboratory notebooks shall be dated and signed or initialed.

___ 4.13.1.2 Software and data protected by non-disclosure agreements or classified as confidential shall be stored according to the vendor and/or government requirements and commensurate with the data sensitivity, and access shall be granted only to the authorized personnel. An access log file shall be maintained.

___ 4.13.1.3 If a vendor’s system on which testing is conducted is potentially open to access by third parties, the testing laboratory shall ensure that the testing environment is controlled so that the third parties do not gain access to that system during testing.

___ 4.13.1.4 Records of all management system activities including training, internal audits, and management reviews shall be securely saved for future reviews. The integrity of electronic documents shall be assured by means commensurate with the data sensitivity. Documents in hard copy form shall be marked and stored in a secure location and, if necessary, a file logging any access, change, or addition shall be maintained to preserve a document’s integrity and prevent unauthorized changes.

___ 4.13.1.5 Laboratories shall maintain records of the configuration of test equipment and all analyses to ensure the suitability of test equipment to perform the desired testing.

4.13.2 Technical records

___ 4.13.2.1 The final test results and/or the test reports generated using cryptographic or security testing tools for the IUT or SUT shall be kept by the laboratory following the completion of testing for the life of the IUT or SUT, or as specified by the validation body and/or the vendor in writing. Records may include hard or digital copies of the official test results and the test results error file(s). Records shall be stored in a manner that assures survivability, confidentiality, integrity, and accessibility.

___ 4.13.2.2 A copy of the final test results and/or the test reports generated using cryptographic or security testing tools for the IUT shall be submitted to the validation program.

4.14 Internal Audits

___ In the case where only one member of a laboratory staff is competent in some technical aspects of the program, or is the only expert in conducting a specific aspect of the conformance testing, an external audit by an appropriate expert shall be necessary in order to audit this technical aspect. An audit shall include, at a minimum, but not be limited to:

a) a review of documentation and instructions;

b) adherence to procedures and instructions; and

c) documentation of the audit findings.

5 Technical requirements for accreditation

5.1 General

___ The quality manual shall contain, or refer to documentation that describes and details the laboratory's implementation of procedures covering all the technical requirements in NIST Handbook 150 and this handbook.

5.2 Personnel

___ 5.2.1 The laboratory shall maintain responsible supervisory personnel and competent administrative and technical staff that are:

a) knowledgeable of all FIPS and NIST Special Publications (SP), and references in this handbook and on the CST LAP website;

b) familiar with cryptographic terminology and families of cryptographic algorithms and security functions with particular emphasis on the FIPS-approved and NIST-recommended security functions;

c) familiar with the cryptographic and security testing tools; and

d) knowledgeable of all programmatic test methods, test metrics, and implementation guidance.

___ 5.2.2 The laboratory shall maintain a list of the key personnel designated to satisfy NVLAP requirements, including their assigned roles and a brief summary of their latest training qualifications. The list shall include, but shall not be limited to:

a) Laboratory's Director;
b) Laboratory Manager;
c) Quality Manager;
d) Authorized Representative;
e) Approved Signatories; and
f) other key technical persons in the laboratory (e.g. testers).

___ 5.2.5 The quality manager shall receive management system training preferably in ISO/IEC 17025. If training is not available in ISO/IEC 17025, minimum training shall be acquired in the ISO 9000 series, especially ISO 9001, or equivalent with particular emphasis on internal auditor training.

___ 5.2.7 The personnel shall possess knowledge of, or be trained prior to accreditation on/in the areas listed below:

a) general requirements of the test methods, including generation of test reports;
b) system security concepts;
c) physical security;
d) identification and authentication technologies and techniques;
e) familiarity with cryptographic and security terminology;
f) standards compliance;
g) familiarity with all FIPS publications referenced in this document and NIST Handbook 150;
h) operation and maintenance of NVLAP/Validation Program-mandated testing tools; and
i) familiarity with the Internet and Internet-related software and the ability to locate and securely download references and information from a given website.

___ 5.2.8 The laboratory shall have a competency review program and procedures for the evaluation and maintenance of the competency of each staff member for each test method the staff member is authorized to conduct.

An evaluation and an observation of performance shall be conducted annually for each staff member by the immediate supervisor or a designee appointed by the laboratory director.

A record of the annual evaluation of each staff member shall be dated and signed by the supervisor and the employee.

5.3 Accommodation and environmental conditions

___ 5.3.1 The laboratory shall have its internal networks protected from unauthorized access by external entities, as well as protection against malicious software, worms, viruses, spybots, etc.

___ 5.3.2 If the laboratory is conducting multiple simultaneous testing activities, a system of separation between IUTs and SUTs of different vendors and conformance testing activities shall be maintained as necessary.

___ 5.3.3 The laboratory shall have Internet access for obtaining the most current documentation and test tools from NIST/ITL or NVLAP or other appropriate sites and secure e-mail capabilities for communication with NVLAP, NIST/ITL, CSEC, and the laboratory’s customers.

___ 5.3.4 The testing laboratory shall ensure that, when applicable, the correct version of the NIST/ITL-or NVLAP-provided testing tools are used and that the tools have not been altered in any way that might lead to incorrect results.

___ 5.3.5 For all conformance testing and validations, the laboratory shall ensure that any file containing old results or old test programs on the IUT or SUT is isolated from the current test programs and test or validation results.

___ 5.3.6 If a laboratory must conduct conformance testing at a location outside the laboratory facility, the environment shall conform, as appropriate, to the requirements for the laboratory site, and shall be checked by the NVLAP-accredited laboratory as a responsible party for the security of the environment and the integrity of all tests and recorded results.

[For additional information see subclause 4.4.3 of NIST Handbook 150-17.]

5.4 Test and calibration methods and method validation

___ 5.4.1 **General**

When testing is performed at a vendor site, all NVLAP requirements pertaining to equipment and environment as they apply to the tests scheduled outside the laboratory's accredited location, shall apply.

Moreover, only the personnel of the NVLAP-accredited laboratory shall perform all actions necessary to conduct the tests and record the results, including the loading, compiling, configuring, and execution of any of the mandated testing tools.

5.5 Equipment

___ 5.5.1 For its scope of accreditation, the laboratory shall have appropriate hardware, software, and computer facilities to conduct cryptographic and security testing. This includes but is not limited to:

a) required software test suites;
b) testing equipment for physical tests; and
c) all special equipment necessary to perform all tests derived from the most current version of the standard.

___ 5.5.3 The equipment used for conducting cryptographic and security testing shall be maintained in accordance with the manufacturer's recommendations and in accordance with internally documented laboratory procedures, as applicable.

___ 5.5.4 For conformance testing, the laboratory shall own, load and run a copy of the testing tool(s) provided by the validation program and produce test results using the tool(s) as appropriate. The testing tools provided by the validation program shall not be altered or changed and shall not be distributed outside the laboratory except to the validation program.

___ 5.5.5 Whenever major or minor changes are made to any testing tool, a testing laboratory shall have procedures to assure the accurate execution and correct performance of the test tool. The procedures shall include, at a minumum, the complete set of regression testing of the test tool.

___ 5.5.6 For a given test tool, there may be no suitable validation service available outside the testing laboratory to which accreditation is applicable, and no suitable reference implementation that could be used by the testing laboratory to validate the test tool.

In this situation, the testing laboratory shall define and document the procedures and methods that it uses to check on the correct operation of the test tool, and provide evidence that these procedures and methods are applied whenever the test tool is modified.

___ 5.5.7 The testing laboratory shall document and follow appropriate procedures whenever a test tool is suspected or found to contain errors which make the tool defective or unfit for use.

These procedures shall include establishing that there is a genuine error, reporting the error to the appropriate maintenance authority or validation body.

If the conformance testing results change for an IUT or SUT after correcting the test tool then the information shall be transmitted to the vendor and validation authority.

___ 5.5.8 The calibration of the hardware and software shall be accomplished through:

a) configuration management for all hardware and software; or
b) a version control system.

___ 5.5.9 Records shall be kept of the date, extent of all harware and software upgrades and updates and periods of use.

5.6 Measurement traceability

5.6.1 General

___ 5.6.1.1 Test results produced by the testing laboratory shall be traceable to standard test suites when appropriate, or otherwise to the applicable authoritative test suite.

5.6.2 Calibration

5.6.2.1 Test tools

___ 5.6.2.1.1 The laboratory shall ensure that any test tool used to conduct cryptographic and security testing is performing properly according to the validation body specifications.

The laboratory shall also examine to ensure that the tool does not interfere with the conduct of the test and does not modify or impact the IUT or SUT.

___ 5.6.2.1.2 Confirmation of the use of the most current version of testing tools shall be assured before conducting a test. Records of these confirmations shall be maintained.

5.6.2.2 Test equipment

___ 5.6.2.2.1 Laboratories shall maintain records of the configuration of test equipment and all analysis to ensure the suitability of test equipment to perform the desired testing.

___ 5.6.2.2.2 If applicable, the equipment used for conducting the conformance tests shall be maintained and calibrated in accordance with the manufacturer’s recommendation, as specified in the test method, or as specified in the annex associated with the specific test method(s).

___ 5.6.2.2.3 For calibrations performed in-house, the reference standards used and the environmental conditions at the time of calibration shall be documented for all calibrations.

Calibration records and evidence of the traceability of the reference standards used shall be made available for inspection during the on-site visit.

5.6.3 Testing

___ 5.6.3.1 Laboratories shall use the test methods described in the annex associated with that specific method.

When exceptions to the test methods are deemed necessary for technical reasons, the vendor and the validation program shall be informed and details shall be described in the test report.

Documentation shall be provided on the test method exceptions taken to ensure that the correct and required precision and interpretation of the program-specific test method is maintained.

___ 5.6.3.2 In those technical areas where there is a difference between program-specific test objectives and the testing tool's abstract test cases, the testing laboratory shall show how each realization of a test case is derived faithfully from the governing FIPS, with preservation of assignment of verdicts or measurements to the corresponding sets of observations.

5.8 Handling of test and calibration items

___ 5.8.1 Laboratories shall protect all IUTs, SUTs, and test tools from modifications of any kind or unauthorized access and use.

___ 5.8.2 When the IUT or SUT consists of software components, the laboratory shall ensure that a configuration management is in place to prevent inadvertent modifications.

This configuration management shall uniquely identify each IUT or SUT and control and document modifications to any of the software components.

5.10 Reporting the results

5.10.1 General

___ The laboratory shall issue test reports of its work which accurately, clearly, and unambiguously present the test conditions, the test setup when varies from the standard protocol, the test results, and all other information necessary to reproduce the test.

Any deviations or omissions from the standard shall be clearly indicated.

Test reports to customers shall meet contractual requirements in addition to meeting the requirements of NIST Handbooks 150 and 150-17, governing FIPS and other standards.

5.10.2 Test reports

___ 5.10.2.1 If a validation program-supplied test report tool or other reporting methodologies are provided, the laboratory shall follow those requirements and use those supplied test tools.

___ 5.10.2.2 If the testing laboratory includes comments, analysis or results in a test report that are not covered by the requirements of the governing FIPS, the laboratory shall state clearly which statements are outside the scope of its accreditation.

___ 5.10.2.3 Whenever test cases are such that an analysis of the observations by the testing staff is required in order to interpret the results before stating them in a test report, the testing laboratory shall have objective procedures to be followed by the test operators performing the analysis, sufficient to ensure that the repeatability, reproducibility, and objectivity of the test results can be maintained.

5.10.2.4 Test reports bearing the NVLAP symbol may be written for more than one purpose:

___ a) *Reports that are produced under contract and intended for use by the vendor*

Reports intended for use only by the vendor shall meet vendor/laboratory contract obligations and be complete, but need not necessarily meet all validation program requirements.

___ b) *Reports to be submitted to Validation Authority for IUT or SUT validation under a specific validation program*

Test reports intended for submission to any of the validation programs under the CST LAP shall meet the requirements of the associated DTRs and implementation guidance (IG) when applicable, as well as the requirements of NIST Handbook 150, NIST Handbook 150-17 and any other programmatic documentation guidance.

___ 5.10.2.5 The laboratory shall perform an independent technical quality review of the test report submission documents prior to submission to the validation program. This shall address accuracy, completeness, sufficient evidence of test results and consistency. A record of this review shall be maintained.

5.10.3 Electronic transmission of results to the Validation Programs

___ 5.10.3.1 The electronic version shall have the same content as the printed reports and shall be generated using a software application that is acceptable to the validation program.

___ 5.10.3.2 The laboratory shall ensure that an integrity and confidentiality mechanism commensurable with the data sensitivity and/or programmatic requirements and/or government requirements when electronic delivery of the test reports to the validation program is employed to ensure that the test report cannot be disclosed to anyone other than the intended recipient(s) and an integrity mechanism exists to ensure that the test report is not modified.

5.10.4 Amendments to test reports and calibration certificates

___ 5.10.4.1 For test reports created for validation purposes and submitted to any validation program under the CST LAP, the laboratory shall issue corrections or additions to a test report only by a supplementary document that is suitably marked and that meets the requirements of the respective validation program.

___ 5.10.4.2 For test reports created for purposes other than official IUT validation, the laboratory shall issue corrections or additions to a test report only by a supplementary document suitably marked; e.g., “Supplement to test report serial number […]”.

If the change involves a test assertion, this document shall specify which test assertion is in question, the content of the result, the explanation of the result, and the reason for acceptance of the result.

6 Additional requirements

NOTE *See the annexes of NIST Handbook-17 and the scope-specific checklists for requirements additional to those set forth in this checklist.*

NIST HANDBOOK 150-17 CHECKLIST
COMMENTS AND NONCONFORMITIES

Instructions to the Assessor: Use this sheet to document comments and nonconformities. For each, identify the appropriate item number from the checklist. Identify each comment with a "C" and each nonconformity with an "X." If additional space is needed, make copies of this page or use additional blank sheets.

Item No. *C or X* *Comments and/or Nonconformities*

DATE: **NVLAP LAB CODE:**

Item No. ***C or X*** ***Comments and/or Nonconformities***