NIST HANDBOOK 150-17

National Voluntary Laboratory Accreditation Program

Cryptographic Module Testing

Jeffrey Horlick
Annabelle Lee
Lisa Carnahan

June 2000

U.S. Department of Commerce
William M. Daley, Secretary

Technology Administration
Dr. Cheryl L. Shavers, Under Secretary for Technology

National Institute of Standards and Technology
Raymond G. Kammer, Director

National Institute of Standards and Technology
NIST Handbook 150-17
67 pages (June 2000)
CODEN: NIHAE2

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 2000

For sale by the Superintendent of Documents
U.S. Government Printing Office
Washington, DC 20402-9325

NVLAP AND THE NVLAP LOGO

PREFACE

NIST Handbook 150-17 presents the technical requirements of the National Voluntary Laboratory Accreditation Program (NVLAP) for laboratories seeking accreditation for conformance testing of cryptographic modules conducted in accordance with FIPS PUB 140-1, *Security Requirements for Cryptographic Modules*. It is intended for information and use by staff of accredited laboratories, those laboratories seeking accreditation, other laboratory accreditation systems, users of laboratory services, and organizations needing information on the requirements for accreditation under the Cryptographic Module Testing (CMT) Laboratory Accreditation Program (LAP).

This handbook supplements NIST Handbook 150, *NVLAP Procedures and General Requirements,* which contains Part 285 of Title 15 of the U.S. Code of Federal Regulations (CFR) plus all general NVLAP procedures, criteria, and policies. The criteria in NIST Handbook 150 encompass the requirements of ISO/IEC Guide 25 and the relevant requirements of ISO 9002 (ANSI/ASQC Q92-1987). Handbook 150-17 contains information that is specific to the CMT LAP and interprets the Procedures and General Requirements where appropriate.

The numbering of the sections of this handbook is patterned after Handbook 150; for example, Section 285.3 of Handbook 150 presents the description and goal of NVLAP, whereas Section 285.3 of Handbook 150-17 presents only the description of the CMT LAP. Where there is no CMT LAP-specific information, the section number is omitted.

Questions or comments concerning this handbook should be submitted to: NVLAP, National Institute of Standards and Technology, 100 Bureau Drive, Stop 2140, Gaithersburg, MD 20899-2140; phone: (301) 975-4016; fax: (301) 926-2884; e-mail: nvlap@nist.gov.

SUMMARY

This handbook presents the technical requirements of the Laboratory Accreditation Program for conformance testing of Federal Information Processing Standard Publication (FIPS PUB) 140-1, *Security Requirements for Cryptographic Modules*. This handbook augments NIST Handbook 150, *NVLAP Procedures and General Requirements*. Technical requirements are explained to indicate how the NVLAP criteria are applied.

Any laboratory (including commercial, manufacturer, university, or federal, state, or local government laboratory) that performs any of the test methods that comprise the Cryptographic Module Testing (CMT) Laboratory Accreditation Program (LAP) may apply for NVLAP accreditation. Accreditation will be granted to a laboratory that complies with the conditions for accreditation as defined in this document. Accreditation does not imply a guarantee of laboratory performance or of product test data; it is a finding of laboratory competence.

Testing services covered: Conformance testing of cryptographic modules using the test procedures specified in *Derived Test Requirements for FIPS PUB 140-1, Security Requirements for Cryptographic Modules*. Conformance testing of cryptographic algorithms using test procedures and tests listed at the web site <http://csrc.nist.gov/cryptval>.

Types of cryptographic modules covered: The types of cryptographic modules covered by the CMT LAP are specified in FIPS PUB 140-1; i.e., modules used in a security system protecting sensitive information within computer and telecommunication systems (including voice systems). These modules include, but are not limited to, hardware components or modules, software programs or modules, computer firmware, or any combination thereof.

Period of accreditation: One year, renewable annually.

On-site assessment: Visit by a team of one or more assessors to determine compliance with the NVLAP criteria before initial accreditation and every two years thereafter. Additional monitoring visits as required. Initial assessment requires a demonstration of testing and procedure. Test demonstration can be at the laboratory site or at a site designated by NIST.

Assessors: Experts with experience in the appropriate field(s) of testing and quality system assessment.

Proficiency testing: Each laboratory is required to demonstrate its capability to successfully perform conformance testing. Proficiency testing is required for initial accreditation and is conducted periodically thereafter. Advance notice and instructions are given before testing is scheduled.

Granting accreditation: Based upon compliance with criteria, satisfactory on-site assessment, resolution of deficiencies, and proficiency testing.

Fees: Payments are required as listed on the NVLAP fee schedule, including the administrative/technical support fee, on-site assessment fee, and proficiency testing fee.

ACKNOWLEDGMENTS

The technical requirements and checklist for the CMT LAP were developed by Lisa D. Mitchell, of the MITRE Corporation, under the guidance of Jeffrey Horlick, NVLAP, and Lisa Carnahan of the National Institute of Standards and Technology (NIST), Information Technology Laboratory (ITL).

The NVLAP Program Handbook series, begun in 1982, comprises the combined efforts of the entire NVLAP staff, both past and present.

TABLE OF CONTENTS

PREFACE iii

ACKNOWLEDGMENTS iv

SUMMARY vi

Sec. 285.1 Purpose 1

Sec. 285.2 Organization of procedures 1

Sec. 285.3 Description of NVLAP CMT LAP 1

Sec. 285.4 References 1

Sec. 285.5 Definitions 2

Sec. 285.6 NVLAP documentation 3
- (a) Handbooks 3
- (b) Checklists 3
- (c) Test Method Selection List 3

Sec. 285.22 Assessing and evaluating a laboratory 3
- (a) On-Site Assessment 3
- (b) Proficiency Testing 5

Sec. 285.23 Granting and renewing accreditation 6

Sec. 285.24 Denying, suspending, and revoking accreditation 6

Sec. 285.33 Criteria for accreditation 6
- (a) Scope 6
- (b) Organization and management 6
- (c) Quality system, audit and review 6
- (d) Personnel 7
- (e) Accommodation and environment 8
- (f) Equipment and reference materials 9
- (g) Measurement traceability and calibration 10
- (h) Calibration and test methods 10
- (i) Handling of calibration and test items 11
- (j) Records 11
- (k) Certificates and reports 12
- (l) Subcontracting of calibration or testing 13

APPENDICES
- SAMPLE ACCREDITATION DOCUMENTS A-1
- GENERAL OPERATIONS CHECKLIST B-1
- SPECIFIC OPERATIONS CHECKLIST C-1
- TEST METHOD SELECTION LIST D-1

Sec. 285.1 Purpose

NIST Handbook 150-17 presents the procedures and technical requirements of the National Voluntary Laboratory Accreditation Program (NVLAP) for laboratories seeking accreditation for conformance testing of cryptographic modules conducted in accordance with FIPS PUB 140-1, *Security Requirements for Cryptographic Modules* and conformance testing of associated cryptographic algorithms. This handbook complements and supplements the NVLAP programmatic procedures and general requirements found in NIST Handbook 150.

The interpretive comments and additional requirements contained in this handbook make the general NVLAP criteria specifically applicable to the Cryptographic Module Testing (CMT) Laboratory Accreditation Program (LAP). Specific circumstances under which departures from the NVLAP general procedures are allowable within the scope of the CMT LAP are also addressed in this handbook.

Sec. 285.2 Organization of procedures

(a) The numbering of the sections of this handbook is patterned after Handbook 150, *NVLAP Procedures and General Requirements,* to allow easy cross-reference.

(b) The procedures and general requirements of Handbook 150 and the interpretations and specific requirements in this handbook must be combined to produce the criteria for accreditation in the CMT LAP.

(c) In addition, the handbook contains four appendices which supplement the text:

(1) Appendix A provides examples of a Certificate of Accreditation and a Scope of Accreditation for the CMT LAP;

(2) Appendix B provides the General Operations Checklist, which NVLAP assessors use during an on-site technical assessment to evaluate a laboratory's quality system and ability to conduct testing in general;

(3) Appendix C provides the CMT LAP Specific Operations Checklist, which NVLAP assessors use during an on-site technical assessment of a laboratory; and

(4) Appendix D lists the standard test methods and their accompanying NVLAP Codes for the CMT LAP as given on the Test Method Selection List.

Sec. 285.3 Description of NVLAP CMT LAP

The purpose of the CMT LAP is to accredit laboratories that perform conformance testing for acceptance by the Cryptographic Module Validation Program (CMVP), a product certification program administered jointly by the National Institute of Standards and Technology (NIST) Information Technology Laboratory (ITL) and the Communications Security Establishment (CSE) of the Government of Canada. Requirements for laboratories submitting test reports to NIST/ITL and CSE are also included in this handbook.

The CMT LAP was developed at the request of the NIST/ITL. Cryptographic modules validated by the CMVP will be accepted for use in Canada and by the U.S. government for the protection of sensitive, unclassified information. The testing requirements derived from FIPS PUB 140-1 and the Cryptographic Support Test Tool (*Cryptik*) were developed by NIST/ITL.

Sec. 285.4 References

Reference documents, standards and publications for the CMVP and CMT LAP are given below.

(a) NVLAP publications:

(1) NIST Handbook 150, *NVLAP Procedures and General Requirements*; and

(2) NIST Special Publication 810, *NVLAP Directory* (most current edition).

NVLAP publications may be ordered from:

NVLAP
National Institute of Standards and Technology
100 Bureau Drive, Stop 2140
Gaithersburg, MD 20899-2140

Phone: (301) 975-4016
Fax: (301) 926-2884
E-mail: *nvlap@nist.gov*

NIST Handbook 150 and the On-Line Directory of Accredited Laboratories are also available on the NVLAP web site: <http://ts.nist.gov/nvlap>.

(b) NIST/ITL publications and software:

(1) *Derived Test Requirements for FIPS PUB 140-1, Security Requirements for Cryptographic Modules,* March 1995 (hereinafter called *140-1:Derived Test Requirements*);

(2) *Implementation Guidance for FIPS PUB 140-1 and the Cryptographic Module Validation Program,* updated periodically (hereinafter called *140-1:Implementation Guidance*);

(3) *Cryptographic Support Test Tool- Cryptik*; and

(4) Software packages of cryptographic algorithm tests and test procedures.

NIST/ITL publications and software may be ordered from:

Information Technology Laboratory (ITL)
Cryptographic Module Validation Program
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899-8930

Phone: (301) 975-2934
Fax: (301) 948-1233.

140-1:Derived Test Requirements may also be obtained from the web site:
<http://csrc.nist.gov/cryptval/140-1/140test1.htm>.

140-1:Implementation Guidance may also be obtained from the web site:
<http://csrc.nist.gov/cryptval/140-1/1401ig.htm>.

Cryptographic algorithm tests and test procedures may also be obtained from the web site:
<http://csrc.nist.gov/cryptval>.

(c) FIPS PUB 140-1, *Security Requirements for Cryptographic Modules*, available from:

National Technical Information Service
5285 Port Royal Road
Springfield, VA 22161

Phone: (800) 553-6847
Fax: (703) 605-6900
E-mail: *orders@ntis.fedworld.gov.*

FIPS PUB 140-1 is also available on the web site:
<http://csrc.nist.gov/cryptval>.

(d) ISO/IEC 15408 - Parts 1 through 3:1999, *Information technology—Security techniques—Evaluation criteria for IT security* (Common Criteria) are available from:

<http://csrc.nist.gov/cc/ccv20/ccv2list.htm#ISO>.

Sec. 285.5 Definitions

CMT LAP: The NVLAP Cryptographic Module Testing Laboratory Accreditation Program.

CMV: Cryptographic Module Validation is the act of determining if a cryptographic module conforms to the requirements of FIPS PUB 140-1.

CMVP: The cryptographic module validation program administered jointly by NIST/ITL and CSE.

Conformance: The state of an implementation satisfying the requirements and specifications of a specific standard as tested by a test suite or some approved test method.

Conformance testing: The testing of an implementation against the requirements specified in one or more standards.

Cryptik: The Cryptographic Support Test Tool (CSTT), defined below.

Cryptographic algorithm testing: Input/output testing to determine whether the implementation conforms with the specification.

Cryptographic boundary: An explicitly defined contiguous perimeter that establishes the physical bounds of a cryptographic module.

Cryptographic module (CM): The set of hardware, software, firmware, or a combination thereof that implements cryptographic logic or processes, including cryptographic algorithms and key generation, and is contained within the cryptographic boundary of the module.

CSTT: Cryptographic Support Test Tool, used for documenting cryptographic module test results. This is the *Cryptik* database of abstract test cases (referred to as the *Cryptik* database).

DTR: *Derived Test Requirements* for FIPS PUB 140-1.

FIPS: Federal Information Processing Standard.

IG: *Implementation Guidance* for FIPS PUB 140-1.

Security: The assurance that a cryptographic module will maintain an acceptable level of confidentiality, integrity and availability of data or of a system.

Security requirements: Functionality and design controls which, when implemented in a cryptographic module, help ensure security.

Validation: The administrative acts by NIST/ITL and CSE of determining the level of conformance of an implementation to specified requirements.

Sec. 285.6 NVLAP documentation

(a) Handbooks

(1) The NVLAP quality system requirements, procedures, and general requirements are contained in NIST Handbook 150, *NVLAP Procedures and General Requirements*. Handbook 150 is used for all NVLAP testing laboratory and calibration laboratory programs.

The general terms used in Handbook 150 are interpreted in the program-specific handbook.

(2) The program-specific requirements and technical procedures are contained in this handbook.

Portions of Handbook 150 are interpreted, expanded, and detailed for the CMT LAP.

(b) Checklists

Checklists contain definitive questions about all aspects of the NVLAP criteria for accreditation. NVLAP programs incorporate two types of checklists: a General Operations Checklist (Appendix B) and a Specific Operations Checklist (Appendix C).

Checklists are filled out during the on-site assessment, discussed during the exit briefing, and signed by the laboratory representative and the assessor; a copy is given to the laboratory. The checklists become part of the laboratory history kept by NVLAP.

(1) The NVLAP General Operations Checklist, based on section 285.33 of Handbook 150, is applicable to evaluating a laboratory's ability to conduct testing in general. It addresses factors such as the laboratory's organization, management, and quality system in addition to its testing competency. This checklist will be revised only when Handbook 150 is revised.

(2) The Specific Operations Checklist applies only to CMV conformance testing, focusing on the testing requirements and any special personnel and equipment requirements, and including the assessor's observations of test demonstrations. This checklist may be revised when appropriate to reflect changes in the technical requirements, scope, and/or technology of the program.

Each of these checklists ends with a Comments and Deficiencies form. The assessor uses these forms to explicitly identify and describe deficiencies noted in the body of the checklist. Additionally, the assessor may use the form to document comments on any aspect of the laboratory or its performance.

(c) Test Method Selection List

Most NVLAP programs have scopes that cover more than one test method. Depending on the breadth of its testing capabilities, a laboratory may seek accreditation to all, or to selected, methods within the scope of the program. Selected methods are identified on the Test Method Selection List, which is provided to a laboratory seeking accreditation as part of the NVLAP application package for the program.

Appendix D shows the Test Method Selection List for the CMT LAP, which indicates the test methods associated with each test method grouping. Test method 17/C01 is specified for FIPS PUB 140-1, and test method 17/C02 is specified for the associated cryptographic algorithms. Test method 17/C01 comprises the procedures for all the requirements identified in *140-1:Derived Test Requirements*.

Sec. 285.22 Assessing and evaluating a laboratory

(a) On-Site Assessment

(1) The on-site assessment for NVLAP testing laboratories will most likely be performed by one or two NVLAP assessors in one day plus the following morning. All observations made by the assessors during the assessment are held in strictest confidence.

The on-site assessment may involve the laboratory site and a separate test site for the proficiency testing. If the site for the proficiency demonstration is geographically remote from the laboratory site, the demonstration will have to occur before the laboratory visit.

The laboratory should be prepared to conduct test demonstrations, have equipment in good working order, and be ready for examination according to the requirements identified in this handbook, NIST Handbook 150, and the laboratory's quality manual. Efforts will be made to keep disruption of the normal working routines at a minimum. The assessor will need time and work space to complete assessment documentation during the visit to the laboratory.

The assessor will use the General Operations Checklist and the CMT LAP Specific Operations Checklist. The checklists, based on Handbook 150 and the technical specifics contained in this handbook, serve to ensure that the assessment is complete and that each assessor covers the same items at any laboratory. The checklists are written to cover all possibilities; therefore, not all questions apply in all circumstances. On the other hand, the assessor may go beyond the checklist in order to delve more deeply into a technical issue.

(2) The agenda for a typical on-site assessment is given below.

(i) The assessor will have reviewed the quality manual submitted to NVLAP before the on-site. The assessor conducts an entry briefing with laboratory management and supervisory personnel to explain the purpose of the on-site and to discuss the schedule for the assessment activities. Information provided by the laboratory on its application form may be discussed during this meeting. At the discretion of the laboratory manager, other staff may attend this meeting.

The assessor will ask the laboratory manager to assist in arranging times for interviews with laboratory staff members. While it is not necessary for the assessor to talk to all staff members, he/she may select staff members representing all aspects of the laboratory.

Laboratory personnel should only answer questions that they feel qualified to answer. Knowing whom to ask or where to find the answer is usually considered an acceptable response by the assessor.

(ii) The assessor reviews laboratory documentation, including compliance to the quality system, quality manual, equipment and maintenance records, software versions, record keeping procedures, testing procedures, laboratory test reports, personnel competency records, personnel training plans and records, procedures for updating pertinent information (e.g., Implementation Guidance and the validated products list), and safeguards for the protection of vendor-sensitive and proprietary information.

The assessor will discuss the quality manual with appropriate laboratory staff.

One (or more) laboratory staff member(s) must be available to answer questions; however, the assessor may wish to review the documents alone. Under some circumstances, the assessor may remove some documents from the laboratory during the assessment. Specifically, the assessor may remove for review documents related to the quality system; for example, a revised quality manual, proficiency test data, and new procedures. The material will be returned or destroyed at the laboratory's direction.

The assessor will check personnel information for job descriptions, resumes, and technical performance reviews. The assessor need not be given information which violates individual privacy such as salary, medical information, or performance reviews outside the scope of the laboratory's accreditation. At the discretion of the laboratory, a member of its Human Resources Department (or equivalent) may be present during the review of personnel information.

(iii) The assessor examines hardware, software, equipment, and facilities for appropriateness, capability, adherence to specification, etc.

(iv) The assessor conducts proficiency testing using one or more of the methods indicated in Sec. 285.22(b)(1). This will take place at the laboratory or another mutually agreeable site.

Before the NVLAP assessor arrives at the test demonstration site, the laboratory should load the NIST-provided *Cryptik* and be prepared to run it. The assessor may bring the results of *Cryptik* runs generated by NIST/CSE and ask that results be interpreted by the laboratory. A complete test report produced by the laboratory should be available for discussion.

(v) At the end of the on-site, an exit briefing is held with the laboratory manager and staff to discuss the assessor's findings. Deficiencies are discussed and resolutions may be mutually agreed upon. Deficiencies that must be addressed before accreditation can be granted are emphasized. All deficiencies require subsequent response to NVLAP within 30 days. Items that have been corrected during the on-site assessment and any recommendations are specifically noted.

Comments not identified as deficiencies by the assessors should be given serious consideration, but are taken at the laboratory's discretion. Any disagreements between the laboratory and the assessor should be referred to NVLAP for evaluation.

(vi) The assessor completes an On-Site Assessment Report which summarizes the findings. The assessor attaches copies of the completed checklists to this report during the exit briefing. The report is signed by the assessor and the laboratory's Authorized Representative. A copy of the report and of the two checklists is given to the laboratory representative for retention.

The decision to grant or renew accreditation is not made by the assessor team but by NVLAP in accordance with the procedures described in Handbook 150.

(3) The laboratory will be responsible for demonstrating its competence to prepare and use the *Cryptik* database. This demonstration will include: loading *Cryptik*; configuration; running the tool; preparation of test reports based on *Cryptik*; and updates to *Cryptik*.

(b) Proficiency Testing

(1) Laboratories are required to participate in proficiency testing for identified test methods. NIST Handbook 150 describes how proficiency testing is included in the accreditation process. Successful completion of proficiency testing is required prior to initial accreditation and periodically thereafter. Laboratories renewing accreditation must have satisfactorily participated in all required proficiency testing during their previous accreditation period. Proficiency testing is required for the CMT LAP as designated in the Test Method Selection List, Application Supplement (Appendix D).

To properly evaluate a laboratory, proficiency testing may consist of several parts. The proficiency test concept is designed to allow the evaluation of the laboratory's ability to produce repeatable and reproducible test data. Portions of the testing process may be "highlighted" in proficiency testing; e.g., software, hardware, data analysis, etc. Proficiency testing may consist of one or more of the following methods:

(i) A quiz to be responded to by all appropriate test personnel. The quiz shall pose questions for each test method that is included in each accreditation unit for which the laboratory is seeking accreditation. These questions will test for familiarity with the test methods, ability to determine how a particular cryptographic module should be tested for a particular test requirement, and how a specific algorithm should be tested to a specification.

(ii) Testing of a specially designed artifact with one or more features that are not in conformance with FIPS PUB 140-1. The laboratory must discover the non-conformities, document them, and indicate

which FIPS PUB 140-1 requirements have failed due to the presence of the nonconformities.

(iii) Examination of a specially designed finite state machine (FSM) with one or more features that are not in conformance with FIPS PUB 140-1. For example, the FSM may indicate that there is a direct transition from an error state to a user state. The laboratory must discover the nonconformities, document them, and indicate which FIPS PUB 140-1 requirements have failed because of the presence of the nonconformities.

(iv) Demonstration of correct use of The Cryptographic Support Test Tool *(Cryptik)*. The laboratory must demonstrate that all appropriate personnel understand its use and operation. This may be demonstrated by the assessor observing the use of *Cryptik* by lab personnel.

(v) Ability to produce a report in the approved format and with the identical content of that produced with *Cryptik*.

(vi) Ability to handle *Cryptik* databases that have been preloaded by a vendor. Preloaded databases may be produced by a vendor who wishes to load document references and to prevalidate the module prior to actual conformance testing. The laboratory shall demonstrate that all appropriate personnel are familiar with the procedures for resetting the pass/fail indicators for each prevalidated test.

(vii) Ability to interpret test results reported in *Cryptik*.

The on-site assessor may hand carry proficiency test samples to the laboratory. Alternatively, the on-site assessor may deliver proficiency test samples to the laboratory prior to the on-site assessment.

(2) The results of proficiency testing will be reported to the participants in appropriate documents and reports. Problems indicated by proficiency testing will be discussed with appropriate laboratory personnel responsible for developing and implementing plans for resolving the problems.

Deficiencies identified by proficiency testing during an on-site assessment, scheduled proficiency testing, or submission of a validation report must be resolved.

Sec. 285.23 Granting and renewing accreditation

Laboratories granted NVLAP accreditation are provided with two documents: a Certificate of Accreditation and a Scope of Accreditation. Samples of these accreditation documents for the CMT LAP are shown in Appendix A.

Sec. 285.24 Denying, suspending, and revoking accreditation

Failure to comply with all NVLAP requirements, as specified in this Handbook and in NIST Handbook 150, *NVLAP Procedures and General Requirements*, may result in the denial, suspension, or revocation of a laboratory's accreditation. This includes failure to resolve noted deficiencies and failure to successfully participate in proficiency testing activities.

Sec. 285.33 Criteria for accreditation

(a) Scope

This section presents the specific requirements for a laboratory to be recognized as competent to carry out CMV and cryptographic algorithm conformance testing.

(b) Organization and management

(See NIST Handbook 150, 285.33(b).)

(c) Quality system, audit and review

(1) The quality system requirements are designed to promote laboratory practices which ensure technical integrity of the analyses and adherence to quality assurance practices appropriate to CMV and cryptographic algorithm conformance testing. The laboratory must maintain a quality manual which fully documents the laboratory's policies and practices and the specific steps taken to ensure the quality of CMV conformance testing.

The quality manual and related documentation must contain, or refer to, documentation that

describes and details the laboratory's implementation of procedures covering all of the technical requirements in this handbook. This information will be reviewed by NVLAP assessors during on-site assessments.

(2) The quality manual and related documentation must include procedures for handling software and maintaining its integrity.

The quality system must provide for routine checks of the competence of the staff involved in the conduct and evaluation of tests.

Records must be kept of all quality system activities; for example, training, quality audit, quality system review.

The reference documents, standards, and publications for the CMVP and the CMT LAP listed in Sec. 285.4 of this handbook shall be available as references in developing and maintaining the quality system.

The laboratory shall establish and maintain documented procedures for the review of contracts between itself and its clients. The contract review shall be conducted to ensure that the laboratory is capable of providing the service, and that the requirements, rights, and responsibilities of the parties are understood.

If the laboratory conducts testing at client sites, procedures must exist to address the above requirements.

(3) Audits must be conducted on a periodic basis and management reviews must be conducted at least annually.

(i) In the case where only one member of a laboratory staff is competent to conduct a specific aspect of the conformance testing, audits must at a minimum include a review of documentation and instructions, adherence to procedures and instructions, and documentation of the audit findings.

(ii) In order to audit technical aspects of the program, external audits by NVLAP or another appropriate organization, submission of validation test reports to NIST/ITL and CSE, and/or telephone audits by assessors may be necessary.

(4) A testing laboratory shall have procedures defining the evaluation to be performed whenever major or minor changes are made to *Cryptik* or other test tools. This is necessary to ensure that harmonization is maintained as appropriate with other testing laboratories and that correctness is maintained with respect to the relevant standard(s) or specification(s). (Note: cryptographic algorithm tests that are not supplied by NIST must be purchased through the appropriate standards bodies.)

The procedures for carrying out the test tool validation and for using the *Cryptik* database shall be documented by the laboratory.

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.

(d) Personnel

(1) The laboratory shall maintain a competent administrative and technical staff appropriate for FIPS PUB 140-1 and cryptographic algorithm conformance testing. The laboratory shall maintain position descriptions and resumes for the staff members assigned to FIPS PUB 140-1 and cryptographic algorithm testing related positions and responsible supervisory personnel.

The laboratory shall maintain a list of personnel designated to satisfy NVLAP requirements including: laboratory director, authorized representative, approved signatories, and key technical persons in the laboratory. The laboratory must also identify a staff member as quality manager with overall responsibility for quality assurance and for maintenance of the quality manual. An individual may be assigned or appointed to serve in more than one position; however, to the extent possible, the laboratory director and the quality manager positions should be independently staffed.

(2) Laboratories shall document the required qualifications for each staff position involved in the CMV and cryptographic algorithm conformance testing processes. The staff information may be kept in the official personnel folders or in separate, official folders that contain only the information that the NVLAP assessor(s) needs to review.

(3) The laboratory shall have staff members with appropriate college degrees or equivalent experience, such as a minimum of two years in security product development, testing, or evaluation experience. Training for the laboratory staff shall concentrate on the following areas:

(i) general requirements of the test methods, including generation of test reports;

(ii) familiarity with classes of hardware platforms (for software-based cryptographic algorithms);

(iii) voltage and temperature measurement (Environmental Failure Protection/Environmental Failure Testing (EFP/EFT) for Level 4 only);

(iv) computer security concepts;

(v) finite state machine model analysis;

(vi) production grade, tamper evident, and tamper detection techniques;

(vii) software design specifications, including high-level languages and formal models;

(viii) key management techniques and concepts;

(ix) Electromagnetic Interference/ ElectromagneticCompatibility(EMI/EMC) techniques;

(x) cryptographic self-test techniques;

(xi) FIPS-approved cryptographic algorithms;

(xii) operating system concepts;

(xiii) familiarity with all FIPS PUBs relating to cryptography;

(xiv) familiarity with cryptographic terminology and families of cryptographic algorithms;

(xv) familiarity with the Common Criteria (ISO/IEC 15408:1999);

(xvi) operation and maintenance of *Cryptik*; and

(xvii) familiarity with the Internet and Internet-related software and the ability to locate and download references and information from the CMVP web site <http://csrc.nist.gov/cryptval>.

(4) The laboratory shall have a detailed documented description of its training program for new and current staff members. Each new staff member must be trained for assigned duties. Current staff members must receive additional training when hardware and/or software are changed, when new cryptographic algorithms are approved, when new responsibilities are assigned, or when relevant cryptographic FIPS are modified or developed. This training shall include applying new test methods and *140-1:Implementation Guidance* and performing tests. Each staff member may receive training for assigned duties either through on-the-job training, formal classroom study, or another appropriate mechanism.

(5) The laboratory shall have a competency review program and procedures for the evaluation of each staff member for each test method the staff member is authorized to conduct. An evaluation and an observation of performance must 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 must be dated and signed by the supervisor and the employee.

(e) Accommodation and environment

(1) The laboratory shall have adequate facilities to meet the requirements for NVLAP accreditation. This includes facilities for conformance testing, staff training, record keeping, document storage, and software

storage. In addition, the laboratory shall meet the equipment and environment requirements specific to cryptographic module validation testing and cryptographic algorithm testing specified in the DTR.

(2) Under the CMVP, provisions are made for conformance testing at the client site. When this is done, all NVLAP requirements pertaining to equipment and environment shall apply. In addition, the client site shall meet all CMVP-specific requirements pertaining to equipment and environment.

(3) Electronic mail capability and Internet access are required by the CMVP. FIPS PUB 140-1 and related documents are available or are referenced at the CMVP web site. Test reports and other communications may be sent to NIST/ITL and CSE by e-mail.

(4) The testing laboratory and client shall agree in writing what constitutes the implementation under test (IUT) and what constitutes the environment within the system under test (SUT). For this program, the environment includes the specific test platform, the test configuration, and the external environment.

(5) The testing laboratory shall ensure that the correct version of the test tool is used and that it has not been modified in any way that might lead to incorrect test results.

(6) For all software testing and validation, it shall be ensured that any files containing old results or old test programs on the SUT cannot be confused with the current test programs and test or validation results.

(f) Equipment and reference materials

(1) For its scope of accreditation, the laboratory shall have appropriate hardware, software, and computer facilities to conduct cryptographic module testing. This includes test and measurement equipment for physical tests, as well as special equipment for Level 4 tests.

The following types of equipment and information are required for conducting the conformance tests:

(i) standard laboratory bench equipment;

(ii) digital storage oscilloscope or logic analyzer (to view outputs from ports);

(iii) tools to perform physical security conformance tests;

(iv) power supply (variable power supply for Level 4);

(v) temperature chamber (Level 4 only);

(vi) access to all relevant validated/evaluated products lists;

(vii) formal model texts (Level 4 only); and

(viii) ANSI C Compiler.

(2) The testing laboratory shall document and follow appropriate procedures whenever a test tool is suspected or found to contain errors which make it defective or unfit for use. These procedures shall include establishing that there is a genuine error, reporting the error to the appropriate maintenance authority, withdrawing the test tool or test case(s) from service, as appropriate, correcting the errors, and then revalidating the test tool, as appropriate.

(3) The laboratory shall own, load and run a NIST/ITL-originated copy of *Cryptik* and produce printed output of the test results using the *Cryptik* database.

The laboratory shall also meet the following minimum hardware, software, and operating system requirements for the platform on which *Cryptik* will run: IBM 486 or compatible; MS DOS 6.0 or later; Microsoft Windows 3.1 or Windows 95/98 or compatible; minimum of 5 Mb of available hard disk space; minimum 4 Mb memory; and 3.5" high-density floppy disk drive.

(4) The laboratory shall document procedures for the following actions that involve *Cryptik*: updates; copying original software onto the appropriate media; and transporting database information from one site to another.

(g) Measurement traceability and calibration

(1) The equipment used for conducting the conformance tests must be maintained/recalibrated:

(i) in accordance with the manufacturer's recommendation,

(ii) as specified in the test method, or

(iii) as specified below,

whichever results in shorter time periods between calibrations.

Apparatus/Instrumentation	*Frequency*
ohmmeters	annually
voltmeters	annually
wattmeters	annually
oscilloscopes	annually
logic analyzer	annually
temperature chamber	annually

(2) The laboratory's calibrations may be performed by properly trained staff using calibrated standards, or through contract(s) with a competent external calibration service. (See NVLAP PG-1-1998, *Use of Accredited Calibration Laboratories by NVLAP-Accredited Testing and Calibration Laboratories to Achieve Traceability of Measurements.)* All calibrations and characterizations must be done against reference standards that are traceable to national standards maintained by NIST or by an equivalent foreign national standards authority.

(3) The reference standards used and the environmental conditions at the time of calibration must be documented for all calibrations. Calibration records and evidence of the traceability of the reference standards used must be made available for inspection during the on-site visit.

(4) In addition, validation of the use of the latest version of *Cryptik* must be assured before conducting a test. This may be accomplished through configuration management for all hardware and software, or through software version control. Records shall be kept of the date and extent of all hardware and software upgrades and updates.

The validation of a test tool is the process of verifying as far as possible that the test tool will behave properly and produce results that are consistent with the specifications of the relevant test suites, with any relevant standards and, if applicable, with a previously validated version of the test tool.

The traceability of the abstract test cases is assured through the use of *Cryptik*. Traceability to the requirements in the FIPS PUB 140-1 documentary standard is achieved via the assertions and associated DTRs documented in the database in the *Cryptik* tool. The assertions are either direct quotes from FIPS PUB 140-1, or are directly derivable from these requirements. The DTRs are divided into two sets of requirements: one levied on the vendor and one levied on the tester of the cryptographic module.

(5) Test results produced by the testing laboratory shall be traceable to international standard test suites, when available, or otherwise to the applicable authoritative test suite.

(6) In those technical areas where there is a difference between FIPS PUB 140-1 requirements and the *Cryptik* database of abstract test cases, the testing laboratory shall show how each realization of a test case is derived faithfully from FIPS PUB 140-1, with preservation of assignment of verdicts or measurements to the corresponding sets of observations.

(h) Calibration and test methods

(1) Tests may be conducted at the client or laboratory site or other mutually agreed upon site. When testing is performed at a client site, only the laboratory personnel shall perform all actions necessary to conduct the tests and record the results, including the loading, compiling, configuring, and running of *Cryptik*.

(2) Laboratories shall use the test methods described in the *140-1:Derived Test Requirements*, with clarifications provided in *140-1:Implementation Guidance*. When exceptions are deemed necessary for technical reasons, the client shall be informed and details shall be described in the test report. Substantive documentation shall be provided on exceptions

taken to *Cryptik* to ensure that the correct and required precision and interpretation of the test assertion is maintained. These reports may be used to update *Cryptik* and its accompanying documentation.

(3) Laboratories shall use the test methods and tests for the cryptographic algorithms listed at the web site <http://csrc.nist.gov/cryptval>.

(4) Cryptographic modules that are digital devices are subject to "FCC verification." The FCC Rules and Regulations are contained in 47 CFR Parts 2 and 15 as identified below. Verification testing must be conducted by an accredited testing laboratory.

(i) Title 47-Telecommunication, Chapter I-Federal Communications Commission, Part 2-Frequency Allocations and Radio Treaty Matters; General Rules and Regulations, Subpart J—Equipment Authorization Procedures, Sec. 2.902 Verification.

(ii) Title 47-Telecommunication, Chapter I-Federal Communications Commission, Part 15-Radio Frequency Devices, Subpart B—Unintentional Radiators, Sec. 15.101 Equipment Authorization of Unintentional Radiators.

No submission to the FCC is required from either the vendor or the test laboratory. There is no FCC ID number. Products must be tested and the evidence of conformance to the FCC regulations must be retained. The requirements are given in Part 15 Subpart B. The FCC Equipment Authorization regulations are given in Part 2.

Products used in a residence must meet FCC Class B limits; products for use in other than residences must meet Class A limits. Products must be labeled according to the FCC regulations.

Questions regarding the FCC regulations and FCC requirements may be directed to the FCC, Office of Engineering and Technology Laboratory at <labinfo@fcc.gov> or 301-362-3000.

The U.S. Code of Federal Regulations may be found at <http//www.access.gpo.gov/nara/index.html#cfr>.

(i) Handling of calibration and test items

When the cryptographic module consists of software components, the laboratory shall provide configuration management mechanisms to control and document modifications to the software components.

(j) Records

(1) The laboratory shall maintain a functional record keeping system for each client testing process. Records must be readily accessible and complete. Computer-based media must be logged and properly marked, and there must be proper back-up. Entries in laboratory notebooks must be dated and signed or initialed. Computer-based records must contain entries of pertinent staff/date information for data as required in the quality manual and means to preserve integrity for maintenance of records, without later modifications, as an established safeguard.

The testing laboratory shall take steps to ensure that no third party can gain access to the on-line records either during or after testing.

If a client's system on which testing is conducted is potentially open to access by third parties, the testing laboratory shall ensure that the client controls the testing environment so that third parties do not gain access to that system during testing.

(2) Records covering the following are required and will be reviewed during the on-site assessment:

(i) quality system;

(ii) staff training dates and competency reviews;

(iii) software versions and updates;

(iv) *Cryptik* versions and updates;

(v) *Cryptik* documentation;

(vi) statement of policy and conditions for testing;

(vii) test equipment and instrumentation calibration (software documentation updates, if applicable);

(viii) acceptance/rejection of modules submitted for test;

(ix) comprehensive logs for tracking samples and test activities;

(x) problems with test equipment or system(s), records that such equipment and systems were removed from service, and repair or resolution of problems;

(xi) test data (including any diagrams, algorithm test suites, photos, and graphic images) and official reports; and

(xii) correspondence file including questions submitted, as defined in *140-1:Implementation Guidance*, and responses.

(3) Testing equipment or verification records should include the following:

(i) equipment name or description;

(ii) model, style, serial number or other unique ID;

(iii) manufacturer;

(iv) date received and date placed in service;

(v) current location, where appropriate;

(vi) condition when received (e.g., new, used, reconditioned);

(vii) copy of the manufacturer's instructions, where available;

(viii) notation of all equipment variables requiring verification;

(ix) the range of verification;

(x) the resolution of the instrument and its allowable error;

(xi) date of next calibration and/or verification;

(xii) date and result of last calibration and/or verification;

(xiii) details of maintenance carried out to date and planned for the future;

(xiv) history of any damage, malfunction, modification or repair;

(xv) identity of the laboratory individual or external service responsible for calibration; and

(xvi) source of reference standard and traceability.

(4) Final test reports generated using *Cryptik* and final test values for the algorithm IUT shall be kept by the laboratory following the completion of testing for the life of the cryptographic module or as specified by the client. Records may include hard copies or tapes/disks of the official results and the test results error file stored in a manner that assures survival and retrievability of records

(k) Certificates and reports

(1) The laboratory shall issue test reports of its work which accurately, clearly, and unambiguously present the test conditions, test setup, test results, and all required information. Test reports to clients shall meet contractual requirements in addition to meeting the requirements of FIPS PUB 140-1 and NIST Handbook 150. Test reports shall provide all necessary information to permit the same or another laboratory to repeat the test and obtain comparable results.

If the testing laboratory includes comments, analysis or results in a test report that are not covered by the requirements of FIPS PUB 140-1, it shall state clearly that these are outside the scope of its accreditation.

Whenever test cases are such that 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 define objective procedures to be followed by the test operators performing the analysis, sufficient to ensure the repeatability, reproducibility, and objectivity of the test results can be maintained.

(2) Test reports endorsed with the NVLAP logo may be written for more than one purpose:

(i) *Reports that are produced under contract and intended for use by the client*

Reports intended for use only by the client shall meet client/laboratory contract obligations and be complete, but need not necessarily meet all CMVP validation requirements. Each test report must contain sufficient information for the exact test conditions so that they may be reproduced at a later time. Any deviations or omissions from the standard must be clearly indicated. The test report must meet the requirements of NIST Handbook 150.

(ii) *Reports to be submitted to NIST/ITL and CSE for the CMVP*

Test reports intended for submission to the CMVP must meet the requirements of *140-1:Derived Test Requirements* and *140-1:Implementation Guidance* as well as the requirements of NIST Handbook 150. Test results created for cryptographic algorithm testing must include the values generated by the IUT.

In addition to printed reports, laboratories may submit reports to NIST/ITL and CSE in electronic form using media such as floppy disks. The electronic version shall have the same content as the printed reports and shall use a software application that is acceptable to NIST/ITL and CSE. A printed copy should be placed in the laboratory records.

(3) Reports that are produced by *Cryptik* are acceptable as CMVP test reports.

(4) Test reports that will be delivered to NIST/ITL and CSE in electronic form via electronic transfer technology shall be digitally signed or have a message authentication code applied to ensure integrity of the report and the identity of the laboratory that produced the report. The laboratory shall provide a secure means of conveying the necessary information to NIST/ITL and CSE for the verification of the signature or the message authentication code. Confidentiality mechanisms shall be employed to ensure that the test report cannot be disclosed to anyone other than the intended recipient(s).

(5) For test reports created for validation purposes and submitted to the CMVP, the laboratory shall issue corrections or additions to a test report only by a further document that is suitably marked and that meets the requirements of the CMVP.

For test reports created for purposes other than CMVP validation, the laboratory shall issue corrections or additions to a test report only by a further document suitably marked; e.g., "Supplement to test report serial number ...." If the change involves a test assertion, this document must 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.

(l) Subcontracting of calibration or testing

Laboratories that subcontract EMI/EMC tests referenced in section (h)(4) must comply with the requirements of Handbook 150. If subcontracted, EMI/EMC testing shall be conducted in a test laboratory recognized by the Federal Communications Commission (FCC).

The FCC list of accredited laboratories, *Contract Test Firms on File,* may be found at <http://www.fcc.gov/oet/info/database/testsite>. Accredited laboratories are indicated as described at the web site.

APPENDIX A

SAMPLE ACCREDITATION DOCUMENTS

United States Department of Commerce
National Institute of Standards and Technology

NVLAP®

ISO/IEC GUIDE 25:1990
ISO 9002:1987

Certificate of Accreditation

DEPARTMENT OF COMMERCE ★ UNITED STATES OF AMERICA ★

LABORATORY NAME

ANYTOWN, USA

is recognized under the National Voluntary Laboratory Accreditation Program for satisfactory compliance with criteria established in Title 15, Part 285 Code of Federal Regulations. These criteria encompass the requirements of ISO/IEC Guide 25 and the relevant requirements of ISO 9002 (ANSI/ASQC Q92-1987) as suppliers of calibration or test results. Accreditation is awarded for specific services, listed on the Scope of Accreditation for:

INFORMATION TECHNOLOGY SECURITY TESTING
CRYPTOGRAPHIC MODULE TESTING

March 31, xxxx
Effective through

David F. Alderman
For the National Institute of Standards and Technology

NVLAP-01C (11-95)

NVLAP Lab Code: 000000-0

National Institute of Standards and Technology

NVLAP®

National Voluntary Laboratory Accreditation Program

ISO/IEC GUIDE 25:1990
ISO 9002:1987

Scope of Accreditation

CRYPTOGRAPHIC MODULE TESTING **NVLAP LAB CODE 000000-0**

LABORATORY NAME
Street Address
Anytown, USA 00000-0000
Mr. John Doe
Phone: 000-000-0000 Fax: *###-###-####*

NVLAP Code	*Designation & Short Title*
17/C01	NIST-CSTT:140-1; National Institute of Standards and Technology - Cryptographic Support Test Tool (CSTT) for the Federal Information Processing Standard 140-1 (FIPS 140-1), "Security Requirements for Cryptographic Modules."
17/C01a	Test Method Group 1: All test methods derived from FIPS 140-1 and specified in the CSTT, except those listed in Group 2 and Group 3.
17/C01b	Test Method Group 2: Test methods for Physical Security, Level 4 derived from FIPS 140-1 and specified in the CSTT.
17/C01c	Test Method Group 3: Test methods for Software Security, Level 4 derived from FIPS 140-1 and specified in the CSTT.
17/C02	FIPS-Approved Cryptographic Algorithms (see <http://csrc.nist.gov/cryptval>) as required in FIPS PUB 140-1.

March 31, xxxx
Effective through

David F. Alderman
For the National Institute of Standards and Technology

NVLAP/1S(11-95)

APPENDIX B

GENERAL OPERATIONS CHECKLIST

NVLAP LAB CODE: _____

GENERAL OPERATIONS CHECKLIST

Instructions to the Assessor: This checklist addresses general accreditation criteria prescribed in applicable sections of NIST Handbook 150, *NVLAP Procedures and General Requirements*.

This checklist follows and is numbered to correspond to the *NVLAP Procedures and General Requirements*, Subsection 285.33. The numbers in square brackets identify related checklist items. A small black triangle appears in the left-hand margin of selected lines of text throughout this checklist; the marked text applies only to the Calibration Laboratory Accreditation Program (LAP).

Place an "X" beside each checklist item which represents a deficiency. Place a "C" beside each item on which you are commenting for other reasons. Record the item number and your written deficiency explanations and/or comments in this list or on the attached comment sheets. Place a check beside all other items you observed or verified at the laboratory.

SEC. 285.33 CRITERIA FOR ACCREDITATION

(b) *Organization and management*

(1) The laboratory shall be:

_____ (i) legally identifiable;

Legal name of laboratory ownership: _____

(ii) organized and shall operate in such a way that its permanent, temporary and mobile facilities meet the NVLAP requirements [see also (b)(2)(i), (c)(2)(ii)];

_____ (iii) properly identified on the NVLAP Application.

(2) The laboratory shall:

_____ (i) have managerial staff with the authority and resources needed to discharge their duties [see also (b)(1)(ii), (c)(2)(ii)];

_____ (ii) have policies to ensure that its personnel are free from any commercial, financial and other pressures which might adversely affect the quality of their work;

_____ (iii) be organized in such a way that confidence in its independence of judgment and integrity is maintained at all times;

_____ (iv) specify and document the responsibility, authority and interrelation of all personnel who manage, perform or verify work affecting the quality of calibrations and tests;

_____ (v) provide supervision by persons familiar with the calibration or test methods and procedures, the objective of the calibration or test, and the assessment of the results. The ratio of supervisory to non-supervisory personnel shall be such as to ensure adequate supervision;

_____ (vi) have a technical manager (however named) who has overall responsibility for the technical operations;

Name of person: _____

_____ (vii) have a quality manager (however named) who has responsibility for the quality system and its implementation. The quality manager shall have direct access to the highest level of management at which decisions are taken on laboratory policy or resources, and to the technical manager. In some laboratories, the quality manager may also be the technical manager or deputy technical manager;

Name of person: _____

_____ (viii) nominate deputy(ies) in case of absence of the technical or quality manager;

Name(s): _____

_____ (ix) have documented policy and procedures to ensure the protection of clients' confidential information and proprietary rights [see also (c)(2)(xviii)];

_____ (x) where appropriate, participate in interlaboratory comparisons and proficiency testing programs [see also (c)(2)(xiv), (c)(6)(ii), (g)(3)];

_____ (xi) have documented policy and procedures to ensure that its clients are served with impartiality and integrity.

(c) ***Quality system, audit and review***

(1) The laboratory shall:

_____ (i) have an established and maintained quality system appropriate to the type, range and volume of calibration and testing activities it undertakes;

_____ (ii) have the elements of the quality system documented;

_____ (iii) ensure that the quality documentation is available for use by the laboratory personnel;

_____ (iv) define and document its policies and objectives for, and its commitment to, good laboratory practice and quality of calibration or testing services;

_____ (v) have the laboratory management which ensures that these policies and objectives are documented in a quality manual and communicated to, understood, and implemented by all laboratory personnel concerned;

_____ (vi) ensure that the quality manual is maintained current under the responsibility of the quality manager [see also (c)(2)(iv)].

Date of quality manual: _____

Date of latest update: _____

(2) The quality manual, and related quality documentation, shall state the laboratory's policies and operational procedures established in order to meet the NVLAP requirements. The quality manual and related quality documentation shall contain:

_____ (i) a quality policy statement, including objectives and commitments, by top management;

_____ (ii) the organization and management structure of the laboratory, its place in any parent organization and relevant organizational charts;

_____ (iii) the relations between management, technical operations, support services and the quality system;

_____ (iv) procedures for control and maintenance of documentation [see also (c)(1)(vi), (j)(1)];

_____ (v) job descriptions of key staff and reference to the job descriptions of other staff;

_____ (vi) identification of the laboratory's approved signatories (list here or in the comments section): _____

_____

_____ (vii) the laboratory's procedures for achieving traceability of measurements;

_____ (viii) the laboratory's scope of calibrations and/or tests;

_____ (ix) written procedures for ensuring that the laboratory reviews all new work to ensure that it has the appropriate facilities and resources before commencing such work;

_____ (x) reference to the calibration, verification and/or test procedures used;

_____ (xi) procedures for handling calibration and test items;

_____ (xii) reference to the major equipment and reference measurement standards used;

_____ (xiii) reference to procedures for calibration, verification and maintenance of equipment;

_____ (xiv) reference to verification practices including interlaboratory comparisons, proficiency testing programs, use of reference materials and internal quality control schemes [see also (b)(2)(x), (c)(6)(ii), (g)(3)];

(xv) procedures to be followed for feedback and corrective action whenever:

_____ a) testing discrepancies are detected, or

_____ b) departures from documented policies and procedures occur;

_____ (xvi) the laboratory management policies for departures from documented policies and procedures or from standard specifications;

_____ (xvii) procedures for dealing with complaints [see also (n)];

_____ (xviii) procedures for protecting confidentiality and proprietary rights [see also (b)(2)(ix)];

_____ (xix) procedures for audit and review;

_____ (xx) a description of the laboratory's policy regarding the use of the NVLAP logo;

▸ _____ (xxi) a statement of the laboratory's policy for establishing and changing
▸ calibration intervals for equipment it controls; and

► _____ (xxii) a statement of the laboratory's policy concerning the technique(s) to be used
► for determining measurement uncertainty and calibration/verification
► adequacy.

_____ (3) The laboratory shall arrange for audits of its activities at appropriate intervals to verify that its operations continue to comply with the requirements of the quality system. Such audits shall be carried out by trained and qualified staff who are, wherever possible, independent of the activity to be audited. Where the audit findings cast doubt on the correctness or validity of the laboratory's calibration or test results, the laboratory shall take immediate corrective action and shall immediately notify, in writing, any client whose work may have been affected.

The audits shall be objective and be conducted internally or on contract. The audits shall include both general criteria (documents, records and policies) and technical compliance (test methods and practices and calibration procedures).

_____ (4) The quality system adopted to satisfy the NVLAP requirements shall be reviewed at least once a year by the management to ensure its continuing suitability and effectiveness and to introduce any necessary changes or improvements.

_____ (5) All audit and review findings and any corrective actions that arise from them shall be documented. The person responsible for quality shall ensure that these actions are discharged within the agreed timescale.

(6) In addition to periodic audits the laboratory shall ensure the quality of results provided to clients by implementing checks. These checks shall be reviewed and shall include, as appropriate, but not be limited to:

_____ (i) internal quality control plans, such as control charts and other available statistical techniques;

NOTE: Measurement assurance techniques are acceptable means to control the measurement process and consistently produce the highest quality measurements.

_____ (ii) participation in proficiency testing or other interlaboratory comparisons [see also (b)(2)(x), (c)(2)(xiv), (g)(3)];

_____ (iii) regular use of certified reference materials and/or in-house quality control using secondary reference materials;

_____ (iv) replicate testings using the same or different methods;

_____ (v) retesting of retained items;

_____ (vi) correlation of results for different characteristics of an item.

(d) ***Personnel*** [see also (c)(2)(v)]

_____ (1) The testing laboratory shall have sufficient personnel, having the necessary education, training, technical knowledge and experience for their assigned functions.

_____ (2) The testing laboratory shall ensure that the training of its personnel is kept up-to-date.

_____ (3) Records on the relevant qualifications, training, skills and experience of the technical personnel shall be maintained by the laboratory.

(e) ***Accommodation (facilities) and environment*** [see also (i)(3)]

_____ (1) Laboratory accommodation, calibration and test areas, energy sources, lighting, heating and ventilation shall be such as to facilitate proper performance of calibrations or tests.

NOTE: Laboratory design will be, to the maximum extent practical, in accordance with the guidelines found in the NCSL Recommended Practice #7, *Laboratory Design*, July 25, 1993.

_____ (2) The environment in which these activities are undertaken shall not invalidate the results or adversely affect the required accuracy of measurement. Particular care shall be taken when such activities are undertaken at sites other than the permanent laboratory premises.

NOTE: It is expected that environments which do not meet generally accepted norms, such as those found in NCSL Recommended Practice #7, yet which exhibit the stability required to apply necessary correction factors, will be specified by the laboratory for the purpose of assessment of compliance with its own procedures to achieve its stated uncertainties.

_____ (3) The laboratory shall provide facilities for the effective monitoring, control and recording of environmental conditions as appropriate. Due attention shall be paid, for example, to biological sterility, dust, electromagnetic interference, humidity, voltage, temperature, and sound and vibration levels, as appropriate to the calibrations or tests concerned.

_____ (4) There shall be effective separation between neighboring areas when the activities therein are incompatible.

_____ (5) Access to and use of all areas affecting the quality of these activities shall be defined and controlled.

_____ (6) Adequate measures shall be taken to ensure good housekeeping in the laboratory.

NOTE: While it is the laboratory's responsibility to comply with relevant health and safety requirements, this is outside the scope of this assessment.

(f) ***Equipment and reference materials***

(1) The laboratory shall:

_____ (i) be furnished with all items of equipment (including hardware, software, and reference materials) required for the correct performance of calibrations and tests;

_____ (ii) in those cases where the laboratory needs to use equipment outside its permanent control, including rented, leased and client-owned equipment, ensure that the relevant NVLAP requirements are met.

_____ (2) All equipment shall be properly maintained. Maintenance procedures shall be documented. Any item of the equipment which has been subjected to overloading or mishandling, or which gives suspect results, or has been shown by verification or otherwise to be defective, shall be taken out of service, clearly identified and wherever possible stored at a specified place until it has been repaired and shown by calibration, verification or test to perform satisfactorily. The laboratory shall examine the effect of this defect on previous calibrations or tests.

_____ (3) Each item of equipment including reference materials shall, when appropriate, be labelled, marked or otherwise identified to indicate its calibration status.

_____ (4) Records shall be maintained of each item of equipment and all reference materials significant to the calibrations or tests performed. The records shall include:

_____ (i) the name of the item of equipment, software or reference material;

_____ (ii) the manufacturer's name, type identification, and serial number or other unique identification;

_____ (iii) date received and date placed in service;

NOTE: For initial accreditation, the date received and the date placed in service are not considered mandatory requirements for inclusion in laboratory records, although this is encouraged as good laboratory practice.

_____ (iv) current location, where appropriate;

_____ (v) condition when received (e.g., new, used, reconditioned);

_____ (vi) copy of the manufacturer's instructions, where available;

_____ (vii) dates and results of calibrations and/or verifications and date of next calibration and/or verification;

_____ (viii) details of maintenance carried out to date and planned for the future;

_____ (ix) history of any damage, malfunction, modification or repair;

► _____ (x) measured value observed for each parameter found to be out of tolerance
► during calibration/verification.

(g) ***Measurement traceability and calibration***

_____ (1) All measuring and testing equipment having an effect on the accuracy or validity of calibrations or tests shall be calibrated and/or verified before being put into service. The laboratory shall have an established program for the calibration and verification of its measuring and test equipment. The program will ensure the recall or removal from service of any standard or equipment which has exceeded its calibration interval or is otherwise judged to be unreliable.

_____ (2) The overall program of calibration and/or verification and validation of equipment shall be designed and operated so as to ensure that, wherever applicable, measurements made by the laboratory are traceable to national standards of measurement where available. Calibration certificates shall, wherever applicable, indicate the traceability to national standards of measurement and shall provide the measurement results and associated uncertainty of measurement and/or a statement of compliance with an identified metrological specification.

NOTE: Traceability to national standards includes traceability to standards maintained or defined at national laboratories in foreign countries where applicable. In these cases, traceability is achieved via international standards. This includes intrinsic standards of measurement where available.

Where applicable, the methodology of the *Guide to the expression of uncertainty in measurement*: 1993, shall be used as the basis for expression of uncertainty of the measurement. NIST Technical Note 1297; January 1993, *Guidelines for Evaluating and Expressing the Uncertainty of NIST Measurement Results*, is a practical application document written around the *Guide to the expression of uncertainty in measurement*. Where detailed procedures are not used to quantify and combine uncertainties (i.e., use of test accuracy ratio concepts), the sources of uncertainty shall be tabulated and demonstrated to be acceptable for the measurement undertaken.

NOTE: A significant number of intrinsic standards, such as the Josephson Array Voltage Standard and the Iodine-Stabilized Helium-Neon Laser Length Standard, have been developed and are now being used by many national standards laboratories and some industrial laboratories. These standards are based on well-characterized laws of physics, fundamental constants of nature, or invariant properties of materials, and make ideal stable, precise, and accurate measurement standards if properly designed, characterized, operated, monitored and maintained. Where intrinsic standards are used, the laboratory should demonstrate by measurement assurance techniques, interlaboratory comparisons, or other suitable means, that its intrinsic standard measurement results are correlated with those of national or international standards.

_____ (3) Where traceability to national standards of measurement is not applicable, the laboratory shall provide satisfactory evidence of correlation of results, for example by participation in a suitable program of interlaboratory comparisons or proficiency testing [see also (b)(2)(x), (c)(2)(xiv), (c)(6)(ii)].

NOTE: Traceability requirements may also be satisfied by:

(i) internationally accepted standards in the field concerned;

(ii) suitable reference materials;

(iii) ratio or reciprocity measurements; or

(iv) mutual consent standards which are clearly specified and mutually agreed upon by all parties concerned.

_____ (4) Reference standards of measurement held by the laboratory shall be used for calibration only and for no other purpose, unless it can be demonstrated that their performance as reference standards has not been invalidated.

_____ (5) Reference standards of measurement shall be calibrated by a body that can provide traceability to a national standard of measurement. There shall be a program of calibration and verification for reference standards.

_____ (6) Where relevant, reference standards and measuring and testing equipment shall be subjected to in-service checks between calibrations and verifications.

_____ (7) Reference materials shall, where possible, be traceable to national or international standards of measurement, or to national or international standard reference materials.

(h) ***Calibration and test methods***

_____ (1) The laboratory shall have documented instructions on the use and operation of all relevant equipment, on the handling and preparation of items and for calibration and/or testing, where the absence of such instructions could jeopardize the calibrations or tests. All instructions, standards, manuals and reference data relevant to the work of the laboratory shall be maintained up-to-date and be readily available to the staff.

_____ (2) The laboratory shall use appropriate methods and procedures for all calibrations and tests and related activities within its responsibility (including sampling, handling, transport and storage, preparation of items, estimation of uncertainty of measurement and analysis of calibration and/or test data). They shall be consistent with the accuracy required, and with any standard specifications relevant to the calibrations or tests concerned.

NOTES:

(i) Calibration procedures shall contain the required range and tolerance or uncertainty of each item or unit parameter being calibrated or verified. In addition, the procedures shall contain the generic description of the measurement standards and equipment needed with the required parameter, range, tolerances or uncertainties, and specifications for performing the measurement of the calibration or verification, and/or representative types (manufacturer, model, option) that are capable of meeting the generic description for the measurement standards. The procedures shall be consistent with the accuracy required, and with any standard specifications relevant to the calibrations/verifications concerned.

(ii) The laboratory shall ensure that the calibration uncertainties are sufficiently small so that the adequacy of the measurement is not affected. Well-defined and documented measurement assurance techniques or uncertainty analyses may be used to verify the adequacy of a measurement process. If such techniques are not used, then the collective uncertainty of the measurement standards shall not exceed 25% of the acceptable tolerance (e.g., manufacturer's specification) for each characteristic of the measuring and test equipment being calibrated or verified.

_____ (3) Where methods are not specified, the laboratory shall, wherever possible, select methods that have been published in international or national standards, those published by reputable technical organizations or in relevant scientific texts or journals.

_____ (4) Where it is necessary to employ methods that have not been established as standard, these shall be subject to agreement with the client, be fully documented and validated, and be available to the client and other recipients of the relevant reports [see also (k)(2)(x)].

_____ (5) Where sampling is carried out as part of the test method, the laboratory shall use documented procedures and appropriate statistical techniques to select samples [see also (k)(2)(ix)].

_____ (6) Calculations and data transfers shall be subject to appropriate checks.

(7) Where computers or automated equipment are used for the capture, processing, manipulation, recording, reporting, storage or retrieval of calibration or test data, the laboratory shall have written procedures which ensure that:

_____ (i) the NVLAP requirements are complied with;

_____ (ii) computer software, computers or automated equipment is documented and adequate for use;

_____ (iii) procedures are established and implemented for protecting the integrity of data; such procedures shall include, but not be limited to, integrity of data entry or capture, data storage, data transmission and data processing;

_____ (iv) computer and automated equipment is maintained to ensure proper functioning and provided with the environmental and operating conditions necessary to maintain the integrity of calibration and test data [see also (f)(1)];

_____ (v) it establishes and implements appropriate procedures for the maintenance of security of data including the prevention of unauthorized access to, and the unauthorized amendment of, computer records.

_____ (8) Documented procedures shall exist for the purchase, reception and storage of consumable materials used for the technical operations of the laboratory [see also (m)(2)].

(i) ***Handling of calibration and test items***

_____ (1) The laboratory shall have a documented system for uniquely identifying the items to be calibrated or tested, to ensure that there can be no confusion regarding the identity of such items at any time [see also (k)(2)(v)].

_____ (2) Upon receipt, the condition of the calibration or test item, including any abnormalities or departures from standard condition as prescribed in the relevant calibration or test method, shall be recorded. Where there is any doubt as to the item's suitability for calibration or test, where the item does not conform to the description provided, or where the calibration or test required is not fully specified, the laboratory shall consult the client for further instruction before proceeding. The laboratory shall establish whether the item has received all necessary preparation, or whether the client requires preparation to be undertaken or arranged by the laboratory.

_____ (3) The laboratory shall have documented procedures and appropriate facilities to avoid deterioration or damage to the calibration or test item, during storage, handling, preparation, and calibration or test; any relevant instructions provided with the item shall be followed. Where items have to be stored or conditioned under specific environmental conditions, these conditions shall be maintained, monitored and recorded where necessary. Where a calibration or test item or portion of an item is to be held secure (for example, for reasons of record, safety or value, or to enable check calibrations or tests to be performed later), the laboratory shall have storage and security arrangements that protect the condition and integrity of the secured items or portions concerned [see also (e)].

_____ (4) The laboratory shall have documented procedures for the receipt, retention or safe disposal of calibration or test items, including all provisions necessary to protect the integrity of the laboratory.

_____ (5) Tamper-resistant seals shall be affixed to operator-accessible controls or adjustments on measurement standards or measuring and test equipment which, if moved, will invalidate the calibration. The laboratory's calibration system shall provide instructions for the use of such seals and for the disposition of equipment with damaged or broken seals.

NOTE: Tamper-resistant seals are sometimes affixed to equipment to prevent unauthorized access to areas where adjustments or critical components are located.

(j) *Records*

_____ (1) The laboratory shall maintain a record system to suit its particular circumstances and comply with any applicable regulations. It shall retain on record all original observations, calculations and derived data, calibration records and a copy of the calibration certificate, test certificate or test report for an appropriate period. The records for each calibration and test shall contain sufficient information to permit their repetition. The records shall include the identity of personnel involved in sampling, preparation, calibration or testing [see also (c)(2)(iv)].

▸ **EXCEPTION:** The retention of all original observations, calculations, and
▸ derived data in the calibration record system is not a mandatory requirement
▸ for calibration laboratories, although it is encouraged as good laboratory
▸ practice.

_____ (2) All records (including those listed in (f)(4) pertaining to calibration and test equipment), certificates and reports shall be safely stored, held secure and in confidence to the client [see also (b)(2)(ix), (c)(2)(xviii)].

NOTE: The period of retention shall be specified in the quality manual.

Record retention time specified: _____

(k) ***Certificates and reports***

_____ (1) The results of each calibration, test, or series of calibrations or tests carried out by the laboratory shall be reported accurately, clearly, unambiguously and objectively, in accordance with any instructions in the calibration or test methods. The results should normally be reported in a calibration certificate, test report or test certificate and should include all the information necessary for the interpretation of the calibration or test results and all information required by the method used [see also (k)(4)].

NOTE: It is recognized that the results of each calibration do not always result in the production of a calibration certificate or report. Whenever a certificate or report is produced, the above requirements shall be met.

(2) Each certificate or report shall include at least the following information:

_____ (i) a title, e.g., "Calibration Certificate," "Test Report" or "Test Certificate";

_____ (ii) name and address of laboratory, and location where the calibration or test was carried out if different from the address of the laboratory;

_____ (iii) unique identification of the certificate or report (such as serial number) and of each page, and the total number of pages;

_____ (iv) name and address of client, where appropriate;

_____ (v) description and unambiguous identification of the item calibrated or tested [see also (i)(1)];

_____ (vi) characterization and condition of the calibration or test item;

_____ (vii) date of receipt of calibration or test item and date(s) of performance of calibration or test, where appropriate;

EXCEPTION: Although it is encouraged as good laboratory practice, the requirement for inclusion of the date received is not mandatory for calibration laboratories.

_____ (viii) identification of the calibration or test method used, or unambiguous description of any non-standard method used;

_____ (ix) reference to sampling procedure, where relevant [see also (h)(5)];

_____ (x) any deviations from, additions to or exclusions from the calibration or test method, and any other information relevant to a specific calibration or test, such as environmental conditions [see also (c)(2)(xv), (h)(4)];

_____ (xi) measurements, examinations and derived results, supported by tables, graphs, sketches and photographs as appropriate, and any failures identified;

_____ (xii) a statement of the estimated uncertainty of the calibration or test result, where relevant;

_____ (xiii) a signature and title, or an equivalent identification of the person(s) accepting responsibility for the content of the certificate or report (however produced), and date of issue [see also (c)(2)(vi)];

_____ (xiv) where relevant, a statement to the effect that the results relate only to the items calibrated or tested;

_____ (xv) a statement that the certificate or report shall not be reproduced except in full, without the written approval of the laboratory;

_____ (xvi) a statement that the report must not be used by the client to claim product endorsement by NVLAP or any agency of the U.S. Government;

_____ (xvii) the signature of an approved signatory for all test and calibration reports endorsed with the NVLAP logo;

▸ _____ (xviii) special limitations of use; and

▸ _____ (xix) traceability statement.

_____ (3) Where the certificate or report contains results of calibrations or tests performed by subcontractors, these results shall be clearly identified [see also (l)].

_____ (4) Particular care and attention shall be paid to the arrangement of the certificate or report, especially with regard to presentation of the calibration or test data and ease of assimilation by the reader. The format shall be carefully and specifically designed for each type of calibration or test carried out, but the headings shall be standardized as far as possible [see also (k)(1)].

_____ (5) Material amendments to a calibration certificate, test report or test certificate after issue shall be made only in the form of a further document, or data transfer including the statement "Supplement to Calibration Certificate (or Test Report or Test Certificate), serial number ... (or as otherwise identified)," or equivalent form of wording. Such amendments shall meet all the relevant requirements of item (j).

_____ (6) The laboratory shall notify clients promptly, in writing, of any event such as the identification of defective measuring or test equipment that casts doubt on the validity of results given in any calibration certificate, test report, or test certificate or amendment to a report or certificate.

NOTE: Such notification shall quantify the magnitude of error created in the calibration results. The laboratory shall notify customers promptly, in writing, of any customer's measuring and test equipment found significantly out of tolerance during the calibration/verification process. Measurement data shall be reported so that appropriate action can be taken.

_____ (7) The laboratory shall ensure that, where clients require transmission of calibration or test results by telephone, telex, facsimile or other electronic or electromagnetic means, staff will follow documented procedures that ensure that the NVLAP requirements are met and that confidentiality is preserved.

_____ (8) Whenever a laboratory accredited by NVLAP issues a calibration or test report which contains data covered by the accreditation and also data not covered by the accreditation, it must clearly identify in its records, and in the report to the client, specifically which calibration or test method(s), or portion of a calibration or test method(s), was not covered by the accreditation. The laboratory must also inform the client, before the fact, when calibrations or tests requested are not covered by the accreditation.

NVLAP policy regarding calibration and test reports issued by an accredited laboratory, which reference the laboratory's accredited status, requires that any calibration or test report containing data from calibrations or tests which are not covered by the accreditation include:

_____ (i) a statement at the beginning of the report prominently indicating, "This report contains data which are not covered by the NVLAP accreditation"; and

_____ (ii) a clear indication of which data are not covered by the accreditation.

The laboratory must not misrepresent its accreditation. When a client requires or requests accredited services and any of the requested services are not covered by the accreditation, the client must be so advised.

(l) ***Subcontracting of calibration or testing*** [see also (k)(3)]

_____ (1) Where a laboratory subcontracts any part of the calibration or testing, this work shall be placed with a laboratory complying with these requirements. The laboratory shall ensure and be able to demonstrate that its subcontractor is competent to perform the activities in question and complies with the same criteria of competence as the laboratory in respect of the work being subcontracted. The laboratory shall advise the client in writing of its intention to subcontract any portion of the testing to another party.

_____ (2) The laboratory shall record and retain details of its investigation of the competence and compliance of its subcontractors and maintain a register of all subcontracting.

_____ (3) A NVLAP-accredited laboratory intending to subcontract testing or calibration work that will be performed and reported as meeting NVLAP procedures and criteria must:

_____ (i) have in its quality manual a subcontracting policy compatible with the NVLAP policy, with a description of the procedures for administering and implementing those actions to demonstrate the conformance and consistency of the subcontracted laboratory to perform according to NVLAP procedures;

_____ (ii) place the subcontracted work with a laboratory that maintains accreditation established by NVLAP shown by a current NVLAP Lab Code, or provide and maintain current records that demonstrate that the subcontracted laboratory is competent to perform the test(s) or calibration(s) and that it operates in a manner consistent with and in conformance to NVLAP criteria for accreditation;

_____ (iii) clearly identify in its records, and in the report to the client, exactly which data were obtained by the NVLAP-accredited laboratory and which data were obtained by the subcontractor, NVLAP-accredited or not;

_____ (iv) inform its client, before the fact, that it intends to subcontract for completion of all or a portion of the client's work; and

_____ (v) include at the beginning of the report the name, address, and contact person of the subcontracted laboratory(ies), and one of the following statements, as appropriate:

if NVLAP-accredited

"This report contains data which were produced by a subcontracted laboratory **ACCREDITED (NVLAP LAB CODE)** for the calibration or test methods performed"

if not NVLAP-accredited

"This report contains data which were produced by a subcontracted laboratory **NOT ACCREDITED** for the calibration or test methods performed."

The requirements of this section do not supersede any regulation, law, contract specification, or other related conditions which require NVLAP accreditation.

(m) ***Outside support services and supplies***

_____ (1) Where the laboratory procures outside services and supplies in support of calibrations or tests, the laboratory shall use only those outside support services and supplies that are of adequate quality to sustain confidence in the laboratory's calibrations or tests.

_____ (2) Where no independent assurance of the quality of outside support services or supplies is available, the laboratory shall have procedures to ensure that purchased equipment, materials and services comply with specified requirements. The laboratory should, wherever possible, ensure that purchased equipment and consumable materials are not used until they have been inspected, calibrated or otherwise verified as complying with any standard specifications relevant to the calibrations or tests concerned [see also (h)(8)].

_____ (3) The laboratory shall maintain records of all suppliers from whom it obtains support services or supplies required for calibrations or tests.

(n) ***Complaints*** [see also (c)(2)(xvii)]

_____ (1) The laboratory shall have documented policy and procedures for the resolution of complaints received from clients or other parties about the laboratory's activities. A record shall be maintained of all complaints and of the actions taken by the laboratory.

_____ (2) Where a complaint, or any other circumstance, raises doubt concerning the laboratory's compliance with the laboratory's policies or procedures, or with the NVLAP requirements or otherwise concerning the quality of the laboratory's calibrations or tests, the laboratory shall ensure that those areas of activity and responsibility involved are promptly audited in accordance with item (c)(3).

(o) ***Measuring and test equipment (M & TE)***

NOTE: This section applies to the control of measuring and test equipment (M & TE) used to assure that supplies and services comply with prescribed customer requirements. It is based in large part on the requirements found in government audit standards such as MIL-STD 45662A, and is found in Part II of the ANSI/NCSL Z540-1-1994 (Draft) standard.

(1) General requirements for M & TE

_____ (i) The supplier shall establish and document a system to control the calibration/verification of M & TE.

_____ (ii) M & TE used to determine compliance with customer technical specifications shall be calibrated or verified in accordance with sections 285.33(b) through (n).

_____ (iii) The supplier shall have a program to recall for calibration or verification, or remove from service, M & TE that has exceeded its calibration interval, has broken calibration seals, or is suspected to be malfunctioning because of mishandling, misuse, or unusual results.

_____ (iv) All operations performed by the supplier in compliance with these requirements shall be subject to customer verification at unscheduled intervals.

_____ (v) The supplier shall carry out, or arrange to have carried out, periodic quality auditing of the calibration and verification system in order to ensure its continuing effective implementation and compliance with these requirements.

- Based on the results of the audits and any other relevant factors, such as customer feedback, the supplier shall review and modify the system as necessary.

- Plans and procedures for the audits shall be documented. The conduct of the audit and any subsequent corrective action shall also be documented.

(2) Detailed requirements for M & TE

_____ (i) Calibration system description: The supplier shall provide and maintain a written description of the calibration/verification system covering M & TE and measurement standards. The description shall be sufficient to satisfy each requirement of section 285.33(o) and any deviations shall be submitted with supporting documentation to the customer for approval.

_____ (ii) Adequacy of measurement standards: Measurement standards used by the supplier for calibrating M & TE and other measurement standards shall comply with the requirements of items (f)(1), (g)(1), and (h)(2).

_____ (iii) Environmental conditions: M & TE shall be used in an environment controlled to the extent necessary to ensure valid results. Due consideration shall be given to temperature, humidity, lighting, vibration, dust control, cleanliness, electromagnetic interference and any other factors affecting the results of measurements. Where pertinent, these factors shall be monitored and recorded and, when appropriate, correcting compensations shall be applied to measurement results.

_____ (iv) Intervals of calibration and verification: M & TE requiring calibration shall be calibrated or verified at periodic intervals established and maintained to assure acceptable reliability, where reliability is defined as the probability that M & TE will remain in-tolerance throughout the interval. Intervals shall be established for all M & TE requiring calibration unless the equipment is regularly monitored through the use of check standards in a documented measurement assurance process. Check standards must closely represent the item parameters normally tested in the process and the check standard must be verified periodically. Where intervals are used to ensure reliability, the interval setting system must be systematically applied and shall have stated reliability goals and a method of verifying that the goals are being attained. Intervals may be based on usage or time since last calibration or verification. All exemptions from periodic calibration or verification shall be documented. The recall system may provide for the temporary extension of the calibration due date for limited periods of time under specified conditions that do not unreasonably impair the satisfaction of the customer's requirements.

_____ (v) Calibration procedures: Procedures used to calibrate/verify the supplier's M & TE shall comply with the requirements of items (h)(1) and (h)(2).

_____ (vi) Out-of-tolerance conditions: If any M & TE is found to be significantly out of tolerance during the calibration/verification process, the supplier's system shall provide for notification to the user and to the supplier's quality element, if appropriate, of the out-of-tolerance condition with the associated measurement data so that appropriate action can be taken.

_____ (vii) Adequacy of calibration system: The supplier shall establish and maintain documented procedures to evaluate the adequacy of the calibration system and to ensure compliance with these requirements.

_____ (viii) Calibration sources: M & TE requiring calibration shall be calibrated or verified by laboratories that comply with sections 285.33(b) through (n).

_____ (ix) Records: These requirements shall be supported by records documenting that established schedules and procedures are followed to maintain the adequacy of all M & TE. The records for M & TE requiring calibration shall include an individual record of calibration or verification, or other means of control, providing a description or identification of the item, calibration interval, date calibrated, identification of the calibration source, calibration results (data and/or condition status) and calibration action taken (adjusted, repaired, new value assigned, derated, etc.).

_____ (x) Calibration status: M & TE shall be labeled to indicate calibration or verification status. The label shall identify specific date calibrated (day, month, year, Julian date, or equivalent) and the specific calibration due date or usage equivalent. Items not calibrated to their full capability or which have other limitations of use, shall be labeled or otherwise identified as to the limitations. When it is impractical to apply a label directly to an item, the label may be affixed to the instrument container or some other suitable means may be used to reflect calibration status. Tamper-resistant seals are affixed to operator accessible controls or adjustments which if moved will invalidate the calibration. The quality system shall provide instructions for the disposition of equipment with broken tamper-resistant seals.

_____ (xi) Control of subcontractor calibration: The supplier is responsible for assuring that the subcontractor's calibration system conforms to section 285.33 (l) to the degree necessary to assure compliance with contractual requirements. NVLAP accreditation of the subcontractor's laboratory can serve as the basis for compliance with this requirement.

_____ (xii) Storage and handling: M & TE shall be handled, stored, and transported in a manner which shall not adversely affect the calibration or condition of the equipment.

NVLAP LAB CODE: ____

GENERAL OPERATIONS CHECKLIST - COMMENTS AND DEFICIENCIES

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

Item No.	*Comments and/or Deficiencies*

NVLAP LAB CODE: ____

GENERAL OPERATIONS CHECKLIST - COMMENTS AND DEFICIENCIES

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

Item No.	*Comments and/or Deficiencies*

APPENDIX C

SPECIFIC OPERATIONS CHECKLIST

NVLAP LAB CODE: [ ]

CMT LAP SPECIFIC OPERATIONS CHECKLIST

Instructions to the Assessor: This checklist addresses specific criteria prescribed in applicable sections of NIST Handbook 150-17. Included also are instructions and comments sheets used for observing actual demonstrations of the performance of selected test methods. These criteria supplement and **do not** supersede the *Criteria for Accreditation*, based on Section 285.33 of the NVLAP Procedures, which are addressed in the NVLAP GENERAL OPERATIONS CHECKLIST.

Place an "X" beside any of the following items which represent a NVLAP deficiency. Place a "C" beside each item on which you are commenting for other reasons. Record the item number and your deficiency explanation and/or comments directly in this checklist or on the Comments and Deficiencies sheets at the end of this checklist. If the Comments and Deficiencies sheets are used, be sure to unambiguously identify the question or item to which you are referring.

Place a check beside all other items you observed or verified at the laboratory. All items observed or verified must be marked.

1 Organization and management

(See General Operations Checklist)

2 Quality system, audit and review

_____ 2.1 The Quality System requirements

_____ 2.1.1 Quality manual and related documentation contains, or refers to, documentation which describes and details the laboratory's implementation of procedures covering all of the technical requirements in this handbook.

_____ 2.2 The Quality Manual

_____ 2.2.1 contains or references procedures for software handling and integrity;

_____ 2.2.2 contains or references procedures for conduct of conformance testing at client sites;

_____ 2.2.3 provides for or references routine checks of staff competency;

_____ 2.2.4 contains or references procedures for maintaining records of Quality System activities.

_____ 2.3 Reference documents, standards, and publications used by the Quality System include:

_____ 2.3.1 NIST Handbook 150, NVLAP Procedures and General requirements;

_____ 2.3.2 NIST Handbook 150-17, Cryptographic Module Testing;

_____ 2.3.3 NIST Special Publication 810, NVLAP Directory;

_____ 2.3.4 FIPS PUB 140-1, Security Requirements for Cryptographic Modules;

_____ 2.3.5 Derived Test Requirements for FIPS PUB 140-1, Security Requirements for Cryptographic Modules;

_____ 2.3.6 Implementation Guidance for FIPS PUB 140-1 and the Cryptographic Module Validation Program;

_____ 2.3.7 *Cryptik* database;

_____ 2.3.8 Cryptographic algorithm tests and test procedures.

_____ 2.4 The laboratory has documented procedures for the review of contracts between itself and its clients. The contracts meet the requirements of FIPS PUB 140-1.

3 Personnel

_____ 3.1 Record the names of:

_____ 3.1.1 Technical Manager (however titled) _____

_____ 3.1.2 Quality Manager (however titled) _____

_____ 3.1.3 Approved Signatory(s) - Name(s) and title(s) _____

_____

_____ 3.1.4 Technical Staff - Name(s) _____

_____

_____ 3.2 Staff members shall be knowledgeable in the following areas as determined by examining records or by interview and observation:

_____ 3.2.1 general requirements of the test methods;

_____ 3.2.2 familiarity with classes of hardware platforms (for software-based cryptographic algorithms);

_____ 3.2.3 voltage and temperature measurement (EFP/EFT for Level 4 only);

_____ 3.2.4 computer security concepts;

_____ 3.2.5 finite state machine model analysis;

_____ 3.2.6 production grade, tamper evident, and tamper detection and response techniques;

_____ 3.2.7 software design specifications, including high-level languages and formal models;

_____ 3.2.8 key management techniques and concepts;

_____ 3.2.9 EMI/EMC techniques;

_____ 3.2.10 cryptographic self-test techniques;

_____ 3.2.11 FIPS-approved cryptographic algorithms;

_____ 3.2.12 operating system concepts;

_____ 3.2.13 familiarity with all FIPS PUBs relating to cryptography;

_____ 3.2.14 familiarity with cryptographic terminology and families of cryptographic algorithms;

_____ 3.2.15 familiarity with the Common Criteria (ISO/IEC 15408:1999);

_____ 3.2.16 operation and maintenance of *Cryptik* Testing Support Tool; and

_____ 3.2.17 familiarity with the Internet and Internet-related software and the ability to locate and download references and information from the CMVP web site.

4 Accommodation (facilities) and environment

_____ 4.1 Procedures for conformance testing at the client site;

_____ 4.2 Electronic mail capability exists at the laboratory site;

_____ 4.3 Agreement on what constitutes the IUT and the cryptographic boundary of the SUT; and

_____ 4.4 Correct version of the test tool is installed.

5 Equipment and reference materials

_____ 5.1 The laboratory shall meet the following requirements:

_____ 5.1.1 own a properly licensed copy of the *Cryptik* tool;

_____ 5.1.2 have facilities to load the *Cryptik* tool;

_____ 5.1.3 run the *Cryptik* tool; and

_____ 5.1.4 produce a printed output of the test results.

_____ 5.2 The following types of equipment and information are required for conducting the conformance tests:

_____ 5.2.1 standard laboratory bench equipment;

_____ 5.2.2 digital storage oscilloscope or logical analyzer (to view outputs from ports);

_____ 5.2.3 tools to perform physical security conformance tests;

_____ 5.2.4 power supply (variable power supply for Level 4);

_____ 5.2.5 temperature chamber (Level 4 only);

_____ 5.2.6 access to all relevant validated/evaluated products lists and updates;

_____ 5.2.7 formal model texts (Level 4 only); and

_____ 5.2.8 ANSI C Compiler.

_____ 5.3 A laboratory shall also meet the following minimum hardware, software, and operating system requirements for the platform on which the *Cryptik* testing support tool will run. Document here what was used by the laboratory.

_____ 5.3.1 IBM 486 or compatible;

_____ 5.3.2 MS-DOS 6.0 or later;

_____ 5.3.3 Microsoft Windows 3.1 or Microsoft Windows 95 or 98 or compatible;

_____ 5.3.4 minimum of 5 Mb available hard disk space;

_____ 5.3.5 minimum 4 Mb memory; and

_____ 5.3.6 3.5" high-density floppy disk drive.

_____ 5.4 The laboratory shall document procedures for the following actions that involve the *Cryptik* tool;

_____ 5.4.1 updates;

_____ 5.4.2 copying original software onto the appropriate media; and

_____ 5.4.3 transporting database from one site to another.

6 Measurement traceability and calibration

_____ 6.1 Assurance of the use of the latest version of *Cryptik* prior to conducting a test by:

_____ 6.1.1 use of a configuration management system for all involved hardware and software;

_____ 6.1.2 use of software version control; and

_____ 6.1.3 maintenance of records of all hardware and software upgrades and updates.

7 Calibration and test methods

_____ 7.1 Requirements for conducting tests at a client site are properly documented and applied.

_____ 7.2 Test methods and tests for algorithms are in accordance with the information given on the CMVP web site.

_____ 7.3 If applicable, EMI/EMC testing is conducted in accordance with FCC rules and regulations. Subcontracting is in accordance with NVLAP requirements and FCC rules and regulations.

8 Handling of calibration and test items

(See General Operations Checklist)

9 Records

_____ 9.1 Records covering the following are required and will be reviewed during the on-site assessment by selective sampling:

_____ 9.1.1 quality system;

_____ 9.1.2 staff training dates and competency reviews;

_____ 9.1.3 software versions and updates;

_____ 9.1.4 *Cryptik* tool versions and updates;

_____ 9.1.5 *Cryptik* tool documentation;

_____ 9.1.6 statement of policy and conditions for testing;

_____ 9.1.7 test equipment and instrument calibration (software documentation updates if applicable);

_____ 9.1.8 acceptance/rejection of modules submitted for test;

_____ 9.1.9 comprehensive logs for tracking samples and test activities;

_____ 9.1.10 problems with test systems and documentation for off-line until repair to restore status;

_____ 9.1.11 test data (including any diagrams, photos, and graphic images) and official reports; and

_____ 9.1.12 correspondence file including questions submitted, as defined in 140-1: *Implementation Guidance*, and responses.

_____ 9.2 Testing equipment or verification records should include the following:

_____ 9.2.1 equipment name or description;

_____ 9.2.2 model, style, serial number or other unique ID;

_____ 9.2.3 manufacturer;

_____ 9.2.4 date received and date placed in service;

_____ 9.2.5 current location, where appropriate;

_____ 9.2.6 condition when received (e.g., new, used, reconditioned);

_____ 9.2.7 copy of the manufacturer's instructions, where available;

_____ 9.2.8 notation of all equipment variables requiring verification;

_____ 9.2.9 the range of verification;

_____ 9.2.10 the resolution of the instrument and its allowable error;

_____ 9.2.11 date of next calibration and/or verification;

_____ 9.2.12 date and result of last calibration and/or verification;

_____ 9.2.13 details of maintenance carried out to date and planned for the future;

_____ 9.2.14 history of any damage, malfunction, modification or repair;

_____ 9.2.15 identity of the laboratory individual or external service responsible for calibration; and

_____ 9.2.16 source of reference standard and traceability.

10 Certificates and reports

_____ 10.1 Test reports must meet requirements of 140-1: *Derived Test Requirements* and 140-1: *Implementation Guidance.*

_____ 10.2 Test results for cryptographic algorithms must include the values generated by the IUT.

_____ 10.3 The laboratory has the capability to digitally sign or apply an integrity mechanism to electronic copies of test reports.

_____ 10.4 If a test report is digitally signed, the laboratory provides a secure means of conveying the necessary information to NIST/ITL for signature verification.

_____ 10.5 The laboratory has the capability to deliver electronic copies of test reports to NIST/ITL using floppy disks, removable media, or electronic transfer technologies (e.g., electronic mail or ftp).

_____ 10.6 The laboratory uses confidentiality mechanisms to prevent unauthorized disclosure of electronic copies of test reports delivered by any of the available means.

11 Subcontracting of calibration or testing

_____ 11.1 The laboratory has policies and procedures for subcontracting testing and calibration in accordance with NVLAP policy.

_____ 11.1.1 Accredited laboratories are used.

_____ 11.1.2 If non-accredited laboratories are used, the non-accredited laboratories are audited and the results are documented.

_____ 11.2 The laboratory subcontracts EMI/EMC testing to laboratories recognized by the Federal Communications Commission.

12 Outside support services and supplies

(See General Operations Checklist)

13 Complaints

(See General Operations Checklist)

14 Proficiency testing

_____ 14.1 Proficiency testing was conducted according to Section 285.22 (b) of NIST Handbook 150-17 and the performance of the laboratory was satisfactory.

NVLAP LAB CODE: [ ]

SPECIFIC OPERATIONS CHECKLIST - COMMENTS AND DEFICIENCIES

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

Item No.	*Comments and/or Deficiencies*

NVLAP LAB CODE: ____

SPECIFIC OPERATIONS CHECKLIST - COMMENTS AND DEFICIENCIES

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

Item No.	*Comments and/or Deficiencies*

APPENDIX D

TEST METHOD SELECTION LIST

NVLAP LAB CODE: [ ]

INFORMATION TECHNOLOGY SECURITY TESTING
TEST METHOD SELECTION LIST - CRYPTOGRAPHIC MODULE TESTING

Instructions: Check 17/C01 and each Test Method Group for which you are requesting accreditation. Group 1 is required; Group 2 and Group 3 are optional.

For acceptance by the NIST/ITL and CSE Cryptographic Module Validation Program, a laboratory must be accredited for both 17/C01 and 17/C02.

CRYPTOGRAPHIC MODULE TESTING (CMT)

	NVLAP Test Method Code	*Test Method Designation*
_____	17/C01	NIST-CSTT:140-1; National Institute of Standards and Technology - Cryptographic Support Test Tool (CSTT) for the Federal Information Processing Standard 140-1 (FIPS 140-1), "Security Requirements for Cryptographic Modules."
____	17/C01a	**Test Method Group 1:** All test methods derived from FIPS 140-1 and specified in the CSTT, except those listed in Group 2 and Group 3.
____	17/C01b	**Test Method Group 2:** Test methods for Physical Security, Level 4 derived from FIPS 140-1 and specified in the CSTT.
____	17/C01c	**Test Method Group 3:** Test methods for Software Security, Level 4 derived from FIPS 140-1 and specified in the CSTT.
_____	17/C02	FIPS-Approved Cryptographic Algorithms (see <http://csrc.nist.gov/cryptval>) as required in FIPS PUB 140-1.

Complete the Application Supplement on back of this page.

NVLAP LAB CODE: [ ]

INFORMATION TECHNOLOGY SECURITY TESTING
APPLICATION SUPPLEMENT - CRYPTOGRAPHIC MODULE TESTING

QUALITY ASSURANCE MANUAL:

Before your initial on-site and for renewals requiring an on-site assessment, please provide NVLAP with a copy of your laboratory quality manual and test procedures, including specifics for CMT testing. The manual and procedures may accompany this application or may be sent at a later date. The NVLAP on-site assessor(s) will review the manual *before conducting* the on-site assessment of your laboratory and return it afterwards.

PROFICIENCY TESTING:

Proficiency test demonstrations are required during on-site assessments and periodically thereafter. Laboratories will be notified concerning the required proficiency testing schedules and activities.

During the initial on-site assessment, a demonstration of testing capability of a cryptographic artifact will be required. A specially designed artifact will be provided by the assessor(s).

ON-SITE ASSESSMENT

The typical on-site assessment for 17/C01a and 17/C02 will take place during one full day and one or two hours the following morning. 17/C01b and 17/C01c will require an additional day.