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*

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*