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

NIST HANDBOOK 150-17 Annex B CHECKLIST

Cryptographic Algorithms and Cryptographic Modules Testing

Instructions to the Assessor: This checklist addresses specific accreditation requirements prescribed in NIST Handbook 150-17, *Cryptographic and Security Testing*, for Cryptographic Algorithms Validation (17CAV), Cryptographic Hardward Modules (17CMH) and Cryptographic Software Modules (17CMS) test methods. It is used in conjunction with the NIST Handbook 150-17 Checklist, which covers the requirements in clauses 4 and 5 of the program handbook.

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

Note: The numbering of the checklist items correlates to the numbering scheme in NIST Handbook 150-17, Annex B, Section B.5.

B.5 Additional technical requirements for accreditation

B.5.2 Additional personnel requirements

___ B.5.2.1 The laboratory shall demonstrate, in addition to the technical expertise required by each test method as described below, that their personnel has basic knolwedge of cryptographic and security practice for information systems and that the laboratory is aware of the govering standards and publications, especially the ones listed in this handbook.

___ B.5.2.2 The laboratory’s personnel shall have experience, training, knowledge, or familiarity in the following areas:

a) 17CAV, 17CMH, and 17CMS:

___ 1) Validation Program’s programmatic guidance and management documents;

___ 2) the cryptographic algorithms listed in FIPS 140-2 Annexes;

___ 3) random bit generators and entropy requirements;

___ 4) key establishment methods and concepts;

___ 5) approved modes of operation;

___ 6) specification of the module (e.g. hardware, software, hybrid and/or firmware);

___ 7) module ports and interfaces;

___ 8) trusted path and direct entry methods;

___ 9) specification of roles and services;

___ 10) authentication methods (role and identity-based) and strengths;

___ 11) bypass mechanisms and concepts;

___ 12) finite state machine model analysis;

___ 13) development of test jigs, software debuggers, binary editors, compilers, and software diagnostic tools;

___ 14) software design specifications, including high-level languages;

___ 15) operating systems and concepts (e.g. Microsoft, UNIX, LINUX, ARM, Apple, etc.);

___ 16) key management techniques and concepts;

___ 17) zeroization methods;

___ 18) key entry and output;

___ 19) the cryptographic protocols including, but not limited to, SSL, TLS, IKE, SSH, OTAR, etc.;

___ 20) FCC EMI/EMC Class A and Class B requirements and intentional emitters such as radio devices;

___ 21) cryptographic self-test techniques, including, but not limited to, power-up, conditional tests, known answer tests, integrity tests, load and bypass tests, etc.;

___ 22) Design Assurance such as configuration management, delivery, operation, and development;

___ 23) mitigation of other attack mechanisms; and

___ 24) Security Policy requirements (e.g. FIPS 140-2 Appendix C);

b) 17CMH1 Security Levels 1 to 3:

___ 1) production grade, tamper evident, and tamper detection techniques;

___ 2) hardware implementations and technologies associated with single-chip and multi-chip embodiments;

___ 3) epoxies, potting materials, adhesives (e.g. tamper evident labels) and their chemical properties;

___ 4) electrical design, schematics and concepts including logic design and HDL representations; and

___ 5) skills associated with tamper mitigation methods and performing test methods of compromising tamper protection mechanisms.

c) 17CMH2 Security Level 4:

___ 1) voltage and temperature measurement (Environmental Failure Protection/Enviromental Failure Testing (EFP/EFT));

___ 2) tamper detection/response envelopes; and

___ 3) formal modeling methods.

d) 17CMS1 Security Levels 1 to 3:

___ 1) evaluated operating systems under the Common Criteria EAL2 through EAL3 or equivalents.

e) 17CMS1 Security Level 4:

___ 1) formal modeling methods; and

___ 2) evaluated operating systems under the Common Criteria EAL4 or equivalent.

B.5.3 Additional accomodation and environmental conditions

___ B.5.3.2 Implementations-under-test, IUT specific documentation, IUT specific test jigs, harnesses, supporting test apparatus or test results, shall be protected from persons outside the laboratory, from visitors to the laboratory, from laboratory personnel without a need to know, and from other unauthorized persons**.**

B.5.5 Additional equipment requirements for the 17CAV, 17CMH, and 17CMS testing

___ B.5.5.1 The laboratory shall own at least one designated workstation and compatible operating system that will run the *CAVS*, *CRYPTIK*, and *METRIX* tools**.**

The workstation or other designated workstation shall have internet access and e-mail capability (for report submission).

Workstations shall have Interfaces for loading images from a digital camera and acquiring scanned document images and/or hard copy printouts.

Workstations must have sufficient storage capability, performance and features as specifed by the tool provider.

___ **B.5.5.2** The laboratory shall also meet the following minimum hardware and software requirements:

a) Hardware: Security Levels 1 to 3:

___ 1) at least 40 GB of available space on the hard drive;

___ 2) X-Acto “Type” knives (including various blades);

___ 3) strong artificial light source (Wavelength range of 400 nm to 750 nm);

___ 4) magnifying glass;

___ 5) Dremmel[1] "Type" rotary tool (including accessory bits: cutting, grinding, drilling, carving, etc.);

___ 6) jeweler's screwdrivers (e.g., flat, Phillips, Robertson, torx, hex key);

___ 7) dentist picks and mirrors;

___ 8) hobbyist saw;

___ 9) small pliers (e.g., needle nose, standard nose, long nose, curved nose, side cutters);

___ 10) hammer;

___ 11) chisels;

___ 12) fine (small) files or rasps;

___ 13) hair dryer/heat source;

___ 14) Volt-Ohm-Meter (VOM) or Digital Multi-Meter (DMM) (basic functions to include an ammeter, voltmeter and ohmmeter): calibration only required as needed on the test method employed;

___ 15) digital camera with flash and MACRO (near focus) features;

___ 16) digital scanner;

___ 17) printer; and

___ 18) miscellaneous protection equipment for chemical testing (e.g., goggles, gloves) – optional.

b) Hardware: Security Level 4:

___ 1) variable power supply;

___ 2) temperature chamber (procured, rented, leased, as needed);

___ 3) digital storage oscilloscope or logic analyzer (procured, rented, leased, as needed); and

___ 4) Reference Text: Formal Model text (Z).

c) Software: Security Levels 1 to 3:

___ 1) appropriate compilers, debuggers, and binary editors;

___ 2) a Validation Program-originated copy of *CRYPTIK* (latest version);

___ 3) a Validation Program-originated copy of CAVS (latest version);

___ 4) a Validation Program-originated copy of *METRIX* (latest version);

___ 5) Microsoft Office Professional (Microsoft Word and Access);

___ 6) Adobe Acrobat Standard (pdf generation tool); and

___ 7) a Validation Program supplied or designated file or e-mail encryption application.

d) Software: Security Level 4:

___ 1) Reference Text: Formal Model text (Z).

B.5.6 Additional measurement traceability

___ B.5.6.3 Test vectors and results for cryptographic algorithm testing shall be generated and checked using the provided CAVS tool**.**

Laboratories shall use the test methods described in the document *Derived Test Requirements for FIPS PUB 140-1, Security Requirements for Cryptographic Modules* (or successor), with clarifications provided in the document *Implementation Guidance for FIPS PUB 140-1 and the Cryptographic Module Validation Program* (or successor).

When exceptions are deemed necessary for technical reasons, the validation authority (CAVP and/or CMVP) shall be informed and details shall be described in the test report.

When the *CRYPTIK* tool cannot support submission of the test result information, the laboratory shall provide documentation to ensure that the correct interpretation of the test assertions is maintained.

Laboratories shall use the test methods and tests for the security functions listed at the websites:
http://csrc.nist.gov/groups/STM/cavp/index.html, and
http://csrc.nist.gov/groups/STM/cmvp/index.html.

When testing is performed at the vendor site or other mutually agreed upon sites, only the laboratory personnel shall use or have access to the CAVS, *CRYPTIK, or METRIX* tools supplied by the validation program.

B.5.10 Additional reporting of results requirements

___ The CAVS tool shall be used for 17CAV test report submission.

The *CRYPTIK* tool shall be used for 17CMH and 17CMS test report submission.

The *METRIX* tool shall be used to submit quarterly, or as specified by the validation program, results of test statistics.

COMMENTS AND NONCONFORMITIES

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

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