NVLAP LAB CODE: □

NIST HANDBOOK 150-20 CHECKLIST

Information Technology Security Testing
Common Criteria

Instructions to the Assessor: This checklist addresses accreditation criteria prescribed in NIST Handbook 150-20, *Information Technology Security Testing - Common Criteria* and contains additional requirements. The numbering of this checklist generally follows the numbering of NIST Handbook 150-20.

- All items on this checklist shall be addressed.
- Place an “X” beside each item that represents a nonconformity (formerly called "deficiency").
- Place a “C” beside each item on which you are making a comment.
- Place an "OK" beside each item that you observed or verified at the laboratory.
- Record nonconformity explanations and/or comments on the sheet at the end of this checklist.

3 Accreditation process

3.2 Initial accreditation

_____ 3.2.2 The management system documentation was most recently reviewed on __________________. The documentation was found adequate for continuation of the assessment process. Changes and additions required by the reviewers were made by the laboratory.

_____ 3.2.3 (If this is the initial on-site assessment, skip to 4.)

The initial on-site was conducted on ___________________. Resolutions of findings from the initial on-site visit will be reviewed during this assessment visit.

_____ 3.2.4 The results of the initial evaluations have been read and will be reviewed during this assessment visit.

4 Management requirements for accreditation

4.1 Organization

_____ 4.1.1 The laboratory shall establish and maintain policies and procedures for maintaining laboratory impartiality and integrity in the conduct of Information Technology security evaluations. When conducting evaluations under the NIAP Common Criteria Scheme, the laboratory policies and procedures shall ensure that:

_____ 4.1.1 a) laboratory staff members cannot both develop and evaluate the same Protection Profile, Security Target, or IT product, and

_____ 4.1.1 b) laboratory staff members cannot provide consulting services for and then participate in the evaluation of the same Protection Profile, Security Target, or IT product.

_____ 4.1.2 The laboratory shall have physical and electronic controls augmented with an explicit policy and set of procedures for maintaining separation, both physical and electronic, between the laboratory evaluators and laboratory consultants, product developers, system integrators, and others who may have an interest in and/or may unduly influence the evaluation outcome.

_____ 4.1.3 The management system shall include policies and procedures to ensure the protection of proprietary information. This protection shall specify how proprietary information will be protected from persons outside the laboratory, from visitors to the laboratory, from laboratory personnel without a need to know, and from other unauthorized persons.

4.2 Management system

_____ 4.2.1 The management system requirements are designed to promote laboratory practices that ensure technical accuracy and integrity of the security evaluation and adherence to quality assurance practices appropriate to Common Criteria Testing. The laboratory shall maintain a management system that fully documents the laboratory's policies, practices, and the specific steps taken to ensure the quality of the IT security evaluations.

_____ 4.2.2 The reference documents, standards, and publications listed in NIST Handbook 150-20, 1.4 shall be available for use by laboratory staff developing and maintaining the management system and conducting evaluations.

_____ 4.2.3 Each applicant and accredited laboratory shall have written and implemented procedures as described in Annex D of NIST Handbook 150-20. See Annex D located at the end of this checklist.

_____ 4.2.4 Records shall be kept of all management system activities.

4.3 Document Control

Use NIST Handbook 150 Checklist for nonconformities and comments

_____ **4.4 Review of requests, tenders and contracts**

The procedures for review of contracts shall include procedures to ensure that the laboratory has adequate staff and resources to meet its evaluation schedule and complete evaluations in a timely manner.

4.5 Subcontracting of tests and calibrations

Use NIST Handbook 150 Checklist for nonconformities and comments

4.6 Purchasing services and supplies

Use NIST Handbook 150 Checklist for nonconformities and comments

4.7 Service to the customer

Use NIST Handbook 150 Checklist for nonconformities and comments

4.8 Complaints

Use NIST Handbook 150 Checklist for nonconformities and comments

4.9 Control of nonconforming testing and/or calibration work

Use NIST Handbook 150 Checklist for nonconformities and comments

4.10 Improvement

Use NIST Handbook 150 Checklist for nonconformities and comments

4.11 Corrective action

Use NIST Handbook 150 Checklist for nonconformities and comments

4.12 Preventive action

Use NIST Handbook 150 Checklist for nonconformities and comments

4.13 Control of records

_____ 4.13.1 a) The laboratory shall maintain a functional record-keeping system that is used to track each security evaluation. Records shall be easily accessible and contain complete information for each evaluation.

_____ 4.13.1 b) Required records of evaluation activities shall be traceable to Common Criteria evaluator actions and Common Evaluation Methodology work units.

_____ 4.13.1 c) Computer-based records shall contain entries indicating the date created and the individual(s) who performed the work, along with any other information required by the management system.

_____ 4.13.1 d) Entries in laboratory notebooks shall be dated and signed or initialed.

_____ 4.13.1 e) All records shall be maintained in accordance with laboratory policies and procedures and in a manner that ensures record integrity.

_____ 4.13.1 f) There shall be appropriate back-ups and archives.

_____ 4.13.2 There must be enough evaluation evidence in the records so an independent body, including NVLAP and CCEVS, can determine what evaluation work was actually performed for each work unit and can concur with the verdict. Records include evaluator notebooks, records relating to the product, work-unit level records, and client-site records.

_____ 4.13.3 NIAP requires that laboratory records be retained for a period of at least five years. Beyond this requirement, laboratory records shall be maintained, released, or destroyed in accordance with the laboratory's proprietary information policy and contractual agreements with customers.

4.13.4 Records covering the following are required:

_____ 4.13.4 a) all quality system activities;

_____ 4.13.4 b) staff training dates and competency reviews;

_____ 4.13.4 c) all audits and management reviews;

_____ 4.13.4 d) creation of and changes to evaluation procedures and methodology;

_____ 4.13.4 e) acceptance/rejection of products submitted for evaluation;

_____ 4.13.4 f) complete tracking of multiple versions of evaluation evidence and evaluation technical reports;

_____ 4.13.4 g) complete tracking of evaluation activities to the work unit level including initial analysis, verdicts and any subsequent changes to those verdicts (e.g., based upon modifications of evidence or additional analysis);

_____ 4.13.4 h) source code, binary executables , data and configuration Information sufficient to reproduce any testing performed during the evaluation must be retained, this includes source code and binary executables for both the TOE and any test tools (when available) along with test data and configuration information/files;

_____ 4.13.4 i) calibration records for any equipment where reported results include an estimate of error;

Note: These records should include: the range of calibration, the resolution of the instrument and its allowable error, calibration date and schedule, date and result of last calibration, identity of the laboratory individual or external service responsible for calibration; and source of reference standard and traceability.

_____ 4.13.4 j) the configuration of all test equipment used during an evaluation along with analysis of that equipment to confirm the suitability of test equipment to perform the desired testing.

4.14 Internal audits

_____ 4.14.1 The internal audit shall cover the laboratory management system and the application of the management system to all laboratory activities. The audit shall cover compliance with NVLAP, NIAP, contractual, and laboratory management system requirements. Audits shall cover all aspects of the evaluation activities, including the evaluation work performed.

_____ 4.14.2 In the case where only one member of the laboratory staff is competent to conduct a specific aspect of a test method, and performing an audit of work in this area would result in that person auditing his or her own work, then audits may be conducted by another staff member. The audit shall cover the evaluation methodology for that test method and shall include a review of documented procedures and instructions, adherence to procedures and instructions, and review of previous audit reports. External experts may also be used in these situations.

_____ 4.14.3 The most recent internal audit report shall be available for review during NVLAP on-site assessments.

4.14.4 The laboratory shall perform at least one complete internal audit prior to the first full on-site assessment (see NIST Handbook 150-20, 3.2.5). A partial internal audit should be performed prior to the initial on-site assessment (see NIST Handbook 150-20, 3.2.3). The records will be reviewed before or during the on-site assessment visit.

4.15 Management reviews

_____ 4.15.1 The most recent management review report shall be available for review during NVLAP on-site assessments.

_____ 4.15.2 The laboratory shall perform at least one management review prior to the first full on-site assessment (see NIST Handbook 150-20, 3.2.5). A management review should be performed prior to the initial on-site assessment (see NIST Handbook 150-20, 3.2.3). The records will be reviewed before or during the on-site assessment visit.

5 Technical requirements for accreditation

_____ 5.1 **General**

The quality manual shall contain, or refer to, documentation that describes and details the laboratory's implementation of procedures covering all of the technical requirements in NIST Handbook 150 and NIST Handbook 150-20.

5.2 Personnel

_____ 5.2.1 a) The laboratory shall maintain a competent administrative and technical staff appropriate for Common Criteria- based IT security evaluations.

_____ 5.2.1 b) The laboratory shall maintain position descriptions, training records and resumes for responsible supervisory personnel and laboratory staff members who have an effect on the outcome of security evaluations.

_____ 5.2.2 a) The laboratory shall maintain a list of personnel designated to fulfill NVLAP requirements including: laboratory director, Authorized Representative, Approved Signatories, evaluation team leaders and senior evaluators.

_____ 5.2.2 b) The laboratory shall also identify a staff member as quality manager who has overall responsibility for the management system, the quality system, and maintenance of the management system documents. 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.

_____ 5.2.3 The laboratory shall notify both NVLAP and NIAP within 30 days of any change in key personnel. When key laboratory staff are added, the notification of changes shall include a current resume for each new staff member.

_____ 5.2.4 Laboratories shall document the required qualifications for each staff position. The staff information may be kept in the official personnel folders or in separate, official folders that contain only the information that the NVLAP assessors need to review.

_____ 5.2.5 Laboratory staff members who conduct IT security evaluation activities shall have a Bachelor of Science in Computer Science, Computer Engineering, or related technical discipline or equivalent experience.

_____ 5.2.6 Laboratory staff collectively shall have knowledge or experience in the following areas: operating systems, data structures, design/analysis of algorithms, database systems, programming languages, computer systems architectures, and networking. In addition, the laboratory staff shall have knowledge or experience for any specific technologies upon which an evaluation is conducted.

_____ 5.2.7 a) The laboratory shall have documented a detailed description of its training program for new and current staff members. Each new staff member shall be trained for assigned duties.

_____ 5.2.7 b) The training program shall be updated and current staff members shall be retrained when the Common Criteria, Common Evaluation Methodology, or scope of accreditation changes, or when the individuals are assigned new responsibilities. Each staff member may receive training for assigned duties either through on-the-job training, formal classroom study, attendance at conferences, or another appropriate mechanism.

_____ 5.2.7 c) Training materials that are maintained within the laboratory shall be kept up-to-date.

_____ 5.2.7 d) Staff members shall be trained in the following areas:

- general knowledge of the test methods including generation of evaluation reports
- computer science concepts
- computer security concepts
- working knowledge of the Common Criteria
- working knowledge of the Common Methodology

_____ 5.2.8 a) The laboratory shall review annually the competence of each staff member for each test method the staff member is authorized to conduct.

_____ 5.2.8 b) The staff member’s immediate supervisor, or a designee appointed by the laboratory director, shall conduct annually an assessment and an observation of performance for each staff member.

_____ 5.2.8 c) A record of the annual review of each staff member shall be dated and signed by the supervisor and the employee.

_____ 5.2.8 d) A description of competency review programs shall be maintained in the management system.

_____ 5.2.9 a) Individuals hired to perform Common Criteria testing activities are sometimes referred to as “subcontractors.” NVLAP does not make a distinction between laboratory employees and individuals hired under a subcontracting agreement. NVLAP requires that the CCTL maintain responsibility for and control of any work performed within its scope of accreditation.

_____ 5.2.9 b) To that end, the CCTL shall ensure all individuals performing evaluation activities satisfy all NVLAP requirements, irrespective of the means by which individuals are compensated (e.g., the CCTL shall ensure all evaluators receive proper training and are subject to annual performance reviews, etc.).

_____ 5.2.10 The records for each staff member having an effect on the outcome of evaluations shall include: position description, resume/CV/bio (matching person to job), duties assigned, annual competence review, and training records and training plans.

_____ 5.2.11 In order to maintain confidentiality and impartiality, the laboratory shall maintain proper separation between personnel conducting evaluations and other personnel inside the laboratory or outside the laboratory, but inside the parent organization.

5.3 Accommodation and environmental conditions

_____ 5.3.1 The laboratory shall have adequate facilities to conduct IT security evaluations. This includes facilities for security evaluation, staff training, record keeping, document storage, and software storage.

_____ 5.3.2 a) A protection system shall be in place to safeguard customer proprietary hardware, software, test data, electronic and paper records, and other materials. This system shall protect the proprietary materials and information from personnel outside the laboratory, visitors to the laboratory, laboratory personnel without a need to know, and other unauthorized persons.

_____ 5.3.2 b) Laboratories shall have systems (e.g., firewall, intrusion detection) in place to protect internal systems from untrusted external entities.

_____ 5.3.2 c) If evaluation activities are conducted at more than one location, all locations shall meet NVLAP requirements and mechanisms shall be in place to ensure secure communication between all locations.

_____ 5.3.3 a) The laboratory shall have regularly updated protection for all systems against viruses and other malware.

_____ 5.3.3 b) The laboratory shall have an effective backup system to ensure that data and records can be restored in the event of their loss.

_____ 5.3.4 Laboratory networks used to conduct ATE and AVA evaluation activities shall be completely isolated.

_____ 5.3.5 a) If the laboratory is conducting multiple simultaneous evaluations, it shall maintain a system of separation between the products of different customers and evaluations. This includes the product under evaluation, the test platform, peripherals, documentation, electronic media, manuals, and records.

_____ 5.3.5 b) PKI enabled electronic mail (DOD class 3 email certificates) capability is required for communications with the NIAP/CCEVS.

_____ 5.3.5 c) Internet access also is required for obtaining revisions to the Common Criteria, Common Evaluation Methodology, guidance, and interpretations.

_____ 5.3.6 If evaluation activities will be conducted outside of the laboratory, the management system shall include appropriate procedures for conducting security evaluation activities at customer sites or other off-site locations. For example, customer site procedures may explain how to secure the site, where to store records and documentation, and how to control access to the test facility.

_____ 5.3.7 a) If the laboratory is conducting its evaluation at the customer site or other location outside the laboratory facility, the environment shall conform, as appropriate, to the requirements for the laboratory environment.

_____ 5.3.7 b) If a customer’s system on which an evaluation is conducted is potentially open to access by unauthorized entities during evaluation, the evaluation laboratory shall control the evaluation environment. This is to ensure that the systems are in a defined state compliant with the requirements for the evaluation before starting to perform evaluation work and that the systems ensure that unauthorized entities do not gain access to the system during evaluation.

_____ **5.4 Test and calibration methods and method validation**

_____ 5.4.1 For this program, the test methods of ISO/IEC 17025 are analogous to evaluation methodology using the Common Criteria (CC), the Common Evaluation Methodology (CEM), and additional laboratory-developed methodology. The version of the CC and CEM to be used in each evaluation shall be established in consultation with NIAP and the sponsor.

_____ 5.4.2 For the purposes of achieving product validation through the Common Criteria Scheme, laboratories may be required to comply with both international interpretations and NIAP-specified guidance. The CCEVS may issue guidance or interpretations to supplement the evaluation assurance criteria or methodology provided in the Common Criteria and Common Evaluation Methodology; the laboratory shall comply with the guidance or interpretations within the timeframe specified by the CCEVS.

_____ 5.4.3 The Common Criteria, Common Evaluation Methodology, NIAP guidance and interpretations, and the laboratory’s procedures for conducting security evaluations shall be maintained up-to-date and be readily available to the staff.

_____ 5.4.4 a) The laboratory shall have documented procedures for conducting security evaluations using the Common Criteria and Common Evaluation Methodology, and for complying with guidance or interpretations.

_____ 5.4.4 b) The laboratory shall ensure that these procedures are followed.

_____ 5.4.5 a) Security evaluations may be conducted at the customer site, the laboratory or another location that is mutually agreed to by the CCTL, the sponsor, and CCEVS. When evaluation activities are conducted outside the laboratory, the laboratory shall have additional procedures to ensure the integrity of all tests and recorded results.

_____ 5.4.5 b) These procedures shall also ensure that the same requirements that apply to the laboratory and its facility are maintained at the non-laboratory site.

_____ 5.4.6 When exceptions to the evaluation methodology are deemed necessary for technical reasons, NIAP shall be consulted to ensure that the new methodology continues to meet all requirements and policies, the customer shall be informed, and details of these exceptions shall be described in the evaluation report.

5.5 Equipment

_____ 5.5.1 a) The laboratory shall maintain on-site systems adequate to support IT security evaluations in keeping with the tests for which it is seeking accreditation.

_____ 5.5.1 b) The laboratory shall have an electronic report generation capability.

_____ 5.5.2 The laboratory shall document and maintain records on all test equipment or test suites used during Common Criteria Testing. The laboratory is responsible for configuration and operation of all equipment within its control.

_____ 5.5.3 a) Computer systems and other platforms used during the conduct of testing shall be under configuration control.

_____ 5.5.3 b) The laboratory shall have procedures to ensure that any equipment (hardware and software) used for testing is in a known state prior to use for testing.

5.6 Measurement traceablility

_____ 5.6.1 Measurement traceability is required when applicable.

_____ 5.6.2 The equipment used for conducting security evaluations shall be maintained in accordance with the manufacturer's recommendations, or in accordance with internally documented laboratory procedures, as applicable. Test equipment refers to software and hardware products or other assessment mechanisms used by the laboratory to support the evaluation of the security of an IT product.

_____ 5.6.3 a) Laboratories shall calibrate their test equipment. In Common Criteria Testing, calibration means verification of correctness and suitability. Any test tools used to conduct security evaluations that are not part of the unit under evaluation shall be studied in isolation to make sure they correctly represent and assess the test assertions they make. They should also be examined to ensure they do not interfere with the conduct of the test and do not modify or impact the integrity of the product under test in any way.

_____ 5.6.3 b) Laboratories shall have procedures that ensure appropriate configuration of all test equipment. Laboratories shall maintain records of the configuration of test equipment and all analysis to ensure the suitability of test equipment to perform the desired testing.

_____ 5.6.4 For Common Criteria Testing, "traceability" is interpreted to mean that security evaluation activities are traceable to the underlying Common Criteria requirements and work units in the Common Evaluation Methodology. This means that test tools and evaluation methodology demonstrate that the tests they conduct and the test assertions they make are traceable to specific criteria and methodology. This is necessary to ensure that test results constitute credible evidence of compliance with the CC and CEM.

5.7 Sampling

_____ 5.7 a) The laboratory shall use documented procedures for sampling.

_____ 5.7 b) Whenever sampling is used during an evaluation, the laboratory shall document its sampling strategy, the decision-making process, and the nature of the sample.

_____ 5.7 c) Sampling shall be part of the evaluation record.

5.8 Handling of test and calibration items

_____ 5.8.1 a) The laboratory shall protect products under evaluation and calibrated tools from modification, unauthorized access, and use.

_____ 5.8.1 b) The laboratory shall maintain separation between and control over the items from different evaluations, to include the product under evaluation, its platform, peripherals, and documentation.

_____ 5.8.2 When the product under evaluation includes software components, the laboratory shall ensure that configuration management mechanisms are in place to prevent inadvertent modifications to the software components during the evaluation process.

_____ 5.8.3 The laboratory shall have procedures to ensure proper retention, disposal or return of software and hardware after the completion of the evaluation.

_____ 5.9 Assuring the quality of test and calibration results

The laboratory shall have procedures for conducting final review of evaluation results, the ETR, and the laboratory records of the evaluation prior to their submission to the customer and/or CCEVS.

5.10 Reporting the results

_____ 5.10.1 a) The laboratory shall issue evaluation reports of its work that accurately, clearly, and unambiguously present the evaluator analysis, test conditions, test setup, test and evaluation results, and all other required information.

_____ 5.10.1 b) Evaluation reports shall provide all necessary information to permit the same or another laboratory to reproduce the evaluation and obtain comparable results.

_____ 5.10.2 There may be two types of evaluation reports: a) reports that are to be submitted to the CCEVS, and b) reports that are produced under contract and intended for use by the customer.

_____ 5.10.3 a) Evaluation reports created for submission to the CCEVS shall meet the requirements of the Common Criteria Scheme.

_____ 5.10.3 b) The evaluation report shall contain sufficient information for the exact test conditions and results to be reproduced at a later time if a re-examination or retest is necessary.

_____ 5.10.3 c) Evaluation reports shall be submitted in the form and by the method specified by CCEVS.

_____ 5.10.4 Reports intended for use only by the customer shall meet customer-laboratory contract obligations and be complete, but need not necessarily meet all CCEVS requirements.

_____ 5.10.5 In addition to printed reports, laboratories shall submit reports to the CCEVS in electronic form using media such as CDROM. The electronic version shall have the same content as the hardcopy version and use an application format (e.g., Adobe PDF or Microsoft Word) that is acceptable to the CCEVS.

_____ 5.10.6 a) Evaluation reports that are delivered to CCEVS in electronic form via electronic mail 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.

_____ 5.10.6 b) The laboratory shall provide a secure means of conveying the necessary information to CCEVS for the verification of the signature or the message authentication code.

_____ 5.10.6 c) Confidentiality mechanisms shall be employed to ensure that the evaluation report cannot be disclosed to anyone other than the intended recipient(s).

_____ 5.10.7 Changes to evaluation reports produced for the CCEVS shall be made in accordance with CCEVS requirements.

D Annex D (normative) Written procedures

_____ D.1 a) Each applicant and accredited laboratory shall have written and implemented procedures. Implementation is used here to mean that the appropriate management system and technical documents have been written, experts and expertise obtained, training conducted, activity conducted, activity audited, and a management review conducted. Procedures are an integral part of the laboratory management system and shall be included in all aspects of the laboratory operation.

_____ D.1 b) A laboratory shall implement all of the procedures (listed below or not) that are required to meet the accreditation requirements of NIST Handbook 150 and this handbook. Failure to have implemented procedures may lead to suspension of NVLAP accreditation.

D.2 General procedures for the following activities are required and shall be implemented before accreditation can be granted:

_____ D.2 a) internal audits and management review,

_____ D.2 b) writing and implementing procedures,

_____ D.2 c) writing and implementing instructions,

_____ D.2 d) staff training and individual development plans,

_____ D.2 e) contract review,

_____ D.2 f) staff members who work at home and at alternate work sites outside the laboratory (e.g., telecommuting), and

_____ D.2 g) referencing NVLAP accreditation and use of the NVLAP logo.

D.3 The following program-specific procedures shall be implemented before the activity is undertaken, e.g., procedure for writing Common Methodology (CEM) work-unit level instructions before an evaluation is conducted:

_____ D.3 a) writing a work plan for an evaluation,

_____ D.3 b) selecting the members of an evaluation team,

_____ D.3 c) writing an Evaluation Technical Report (ETR),

_____ D.3 d) writing an Observation Report (OR),

_____ D.3 e) conducting an evaluation at a customer's site (if the laboratory offers such services),

_____ D.3 f) conducting evaluations: for ST, PP, and EAL levels 1, 2, 3, and 4 for specific technologies (e.g., firewalls, operating systems, biometric devices),

_____ D.3 g) vulnerability analysis,

_____ D.3 h) conducting independent testing,

_____ D.3 i) requesting and incorporating CC interpretations,

_____ D.3 j) working with NIAP or other validators during an evaluation,

_____ D.3 k) records and record-keeping for evaluations,

_____ D.3 l) writing Common Methodology (CEM) work-unit-level instructions to describe how the work unit will be performed for a given PP or TOE evaluation.

Note: Not all work units will require such instructions. Examples of work units requiring specific instructions for TOE evaluations include: ADV_FSP.1-4, ADV_FSP.2-4, ADV_FSP.1-5, ADV_FSP.2-5, ADV_LLD.1-7, ADV_HLD.2-11, AGD_ADM.1-7, ATE_IND.2-4, and ATE_COV.2-3.

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 comments with a "C" and nonconformities with an "X." If additional space is needed, make copies of this page (or use additional blank sheets).

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