

Enter Date:

Enter NVLAP Lab Code:

## NIST HANDBOOK 150-20 CHECKLIST COMMON CRITERIA TESTING

**Instructions to the Assessor:** This checklist addresses specific accreditation requirements prescribed in NIST Handbook 150-20, *NVLAP Common Criteria Testing*.

- All items on this checklist shall be addressed.
- Select "OK" for each item you observed or verified as compliant at the laboratory.
- Select "X" for each item that represents a nonconformity.
- Select "C" for each item on which you are commenting for other reasons.
- Place a "N/A" beside any item that does not apply.
- Record the item number and the nonconformity explanation and/or comment on the appropriate comment sheet.

**Note:** The numbering of the checklist items correlates to the numbering scheme in NIST Handbook 150-20, Clauses 4 and 5 and Annex B.

### 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:
- \_\_\_ a) laboratory staff members cannot both develop and evaluate the same Protection Profile, Security Target, or IT product, and
- \_\_\_ 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.

\_\_\_ 4.1.4 The laboratory shall create and maintain a cross-reference document mapping clauses 4 and 5 and annexes A and B of Handbook 150 and clauses 4 and 5 and annex B of Handbook 150-20 to the laboratory's management system documentation.

## **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 B. *See Annex B located at the end of this checklist.*

## **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.

---

**4.13 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 the applicable assurance activities specified in the associated PPs.
  
- \_\_\_ 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 backups 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 assurance activity and can concur with the verdict. Records include evaluator notebooks, records relating to the product, work-unit and assurance activity 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.

---

**4.14 Internal audits**

- \_\_\_ 4.14.1 The laboratory shall perform a complete internal audit of its management system, including the activities and records related to its evaluations, prior to each full on-site assessment visit.
- \_\_\_ 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.

**4.15 Management reviews**

- \_\_\_ The laboratory shall perform a complete management review prior to each full 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 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. 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 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 or Common Evaluation Methodology changes, as new technology specific assurance activities are defined in NIAP approved PPs, 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.
- \_\_\_ 5.2.8 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) The CCTL shall 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 that 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/biography (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) The laboratory 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 effectively isolated to ensure that there are no external influences on test results.
  
- \_\_\_ 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 guidance and interpretations.
- \_\_\_ 5.3.6 If evaluation activities are conducted outside 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), Protection Profile-specific assurance activities, 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 NIAP-approved Protection Profiles; 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-approved PP assurance activities, 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 NIAP-approved PP assurance activities, 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 changes 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.
- \_\_\_ 5.5.4 The equipment used for conducting security evaluations shall be maintained in accordance with 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.
- \_\_\_ 5.5.5 a) The laboratory shall ensure that its test equipment is calibrated. In Common Criteria testing, calibration means verification of correctness and suitability.
- \_\_\_ 5.5.5 b) 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 that they correctly represent and assess the test assertions they make.

---

\_\_\_ 5.5.5 c) They shall also be examined to ensure that 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.

\_\_\_ 5.5.5 d) Laboratories shall have procedures that ensure appropriate configuration of all test equipment.

\_\_\_ 5.5.5 e) Laboratories shall maintain records of the configuration of test equipment and all analyses to ensure that suitability of test equipment to perform the desired testing.

## **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, including 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 results**

\_\_\_ The laboratory shall have procedures for conducting final review of evaluation results, the final report that satisfies NIAP reporting requirements, 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. *[Information only: Not an assessable clause]*

\_\_\_ 5.10.3 a) Evaluation reports created for submission to the CCEVS shall meet the requirements of the CCEVS and all NIAP reporting requirements.

\_\_\_ 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 reexamination 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.

---

**NIST HANDBOOK 150-20 CHECKLIST****ANNEX B: WRITTEN PROCEDURES****B.1 Overview**

- B.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.
- B.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 NIST Handbook 150-20. Failure to have implemented procedures may lead to delay in granting the initial accreditation or suspension of NVLAP accreditation.

**B.2 General procedures (required, but not limited to)**

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

- B.2 a) staff training and individual development plans, and
- B.2 b) plans for staff who work at home and at alternate work sites outside the laboratory (e.g., telecommuting).

**B.3 Program-specific procedures (required, but not limited to)**

The following program-specific procedures shall be implemented before the activity is undertaken, e.g., procedure for writing PP-specific assurance activity instructions before an evaluation is conducted:

- B.3 a) writing a work plan for an evaluation;
- B.3 b) selecting the members of an evaluation team;

- 
- \_\_\_ B.3 c) writing the Final Evaluation Report;
  
  - \_\_\_ B.3 d) writing an Observation Report (OR);
  
  - \_\_\_ B.3 e) conducting an evaluation at a customer's site (if the laboratory offers such services);
  
  - \_\_\_ B.3 f) conducting evaluations using the assurance activities specified in NIAP-approved Protection Profiles, NIAP-approved collaborative Protection Profiles, and Security Targets and the Common Criteria assurance classes APE, ASE, and assurance package EAL 1 and the corresponding Common Evaluation Methodology;
  
  - \_\_\_ B.3 g) requesting and incorporating CC interpretations;
  
  - \_\_\_ B.3 h) working with NIAP or other validators during an evaluation;
  
  - \_\_\_ B.3 i) keeping records for evaluations; and
  
  - \_\_\_ B.3 j) writing assurance activity-level instructions to describe how the activity will be performed for a given TOE evaluation.

*Note: Most assurance activities will not require CCTL-specific instructions. NIAP tries to provide complete instructions along with the description of the assurance activities in the NIAP-approved PPs. However, that objective might not always be achievable as PPs evolve and the suite of PPs expands.*



