NIST HANDBOOK 150-20
2005 Edition

National
Voluntary
Laboratory
Accreditation
Program

INFORMATION TECHNOLOGY SECURITY TESTING: COMMON CRITERIA

Jeffrey Horlick

National Voluntary Laboratory Accreditation Program
Division of Standards Services
Technology Services

October 2005

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

Technology Administration
Michelle O'Neill, Acting Under Secretary for Technology

National Institute of Standards and Technology
William A. Jeffrey, Director

NVLAP AND THE NVLAP LOGO

Contents

Foreword

The NIST Handbook 150 publication series sets forth the procedures, requirements, and guidance for the accreditation of testing and calibration laboratories by the National Voluntary Laboratory Accreditation Program (NVLAP). The series is comprised of the following publications:

- NIST Handbook 150, *NVLAP Procedures and General Requirements*, which contains the general procedures and requirements under which NVLAP operates as an unbiased third-party accreditation body;

- NIST Handbook 150-xx program-specific handbooks, which supplement NIST Handbook 150 by providing additional requirements, guidance, and interpretive information applicable to specific NVLAP laboratory accreditation programs (LAPs).

The program-specific handbooks are not standalone documents, but rather are companion documents to NIST Handbook 150. They tailor the general criteria found in NIST Handbook 150 to the specific tests, calibrations, or types of tests or calibrations covered by a LAP.

NIST Handbook 150-20, *NVLAP Information Technology Security Testing: Common Criteria*, presents the technical requirements and guidance for the accreditation of laboratories under the NVLAP Common Criteria Testing LAP. The 2005 edition incorporates changes resulting from the release of the newest editions of ISO/IEC 17025, *General requirements for the competence of testing and calibration laboratories*, and NIST Handbook 150, as well as editorial improvements. The 2005 edition of NIST Handbook 150-20 supersedes and replaces all previous editions.

The handbook was revised with the participation of technical experts in applicable fields of testing concerning information technology security and the Common Criteria, and was approved by NVLAP. The following main changes have been made to this handbook with respect to the previous edition:

- all references to applicable international guides and standards have been updated;

- Lab Bulletin LB-5-2001, Written Procedures, has been incorporated into Annex D;

- the sequence of NVLAP assessment activities and the proficiency testing program have been changed;

- on-site assessment checklists and the test method selection list are not included in order that they may be provided as separate documents, which may be updated at different intervals than the handbook;

- the body of the handbook has been restructured to conform with internationally accepted rules for the structure and drafting of standards, where appropriate, to promote ease of use and understanding.

Annexes A through C of this handbook show the sequence of events and the responsible parties for initial accreditation, renewal of accreditation, and changes in scope of accreditation.

This handbook is also available on the NVLAP web site (http://www.nist.gov/nvlap).

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.

Acknowledgments

This document was revised by John Nilles of The Aerospace Corporation under the guidance of Jeffrey Horlick (NVLAP Technical Advisor) and Jean Schaffer (NIAP Director). These revisions include technical changes to update the handbook based upon National Information Assurance Partnership's (NIAP) experience since the start of CCEVS evaluations in 2000, and format changes to match NIST Handbook 150, *NVLAP Procedures and General Requirements*. The author would like to acknowledge the valuable insights and comments provided by James Donndelinger, Ken Elliott, Helmut Kurth, Alton Lewis, Robin Medlock, David Ochel, and Mario Tinto.

The initial technical requirements and checklist for Common Criteria Testing Laboratory (CCTL) accreditation were developed by Julie Connolly of the MITRE Corporation, Robin Medlock of Mitretek Systems, and Christine Cheetham and Charles Menk of the National Security Agency, under the guidance of Jeffrey Horlick (NVLAP) and Keith Brewster (NSA). Those authors would like to acknowledge the valuable insights and comments provided by Ellen Flahavin, Arnold Johnson, Lisa Carnahan, and Annabelle Lee of NIST. The requirements in the previous version of this handbook were also strongly influenced by the NVLAP Cryptographic Module Testing and the NVLAP POSIX Laboratory Accreditation Programs.

Introduction

The National Information Assurance Partnership (NIAP), a partnership between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA), has established a program to evaluate conformance of Information Technology (IT) products to international standards. The program is known as the NIAP Common Criteria Evaluation and Validation Scheme for Information Technology Security, abbreviated as the Common Criteria Evaluation and Validation Scheme (CCEVS), which is responsible for issuing Common Criteria certificates for IT security evaluations. This certificate is issued if the security evaluation has been conducted in accordance with the Scheme requirements using the *Common Criteria for Information Technology Security Evaluation* (Common Criteria or CC) and the *Common Methodology for Information Technology Security Evaluation* (Common Evaluation Methodology or CEM).

NIAP requested that NVLAP establish a program to accredit laboratories conducting security evaluations using the Common Criteria and Common Evaluation Methodology. A laboratory desiring accreditation for Common Criteria Testing shall meet the requirements presented in NIST Handbook 150, *NVLAP Procedures and General Requirements*, and this handbook. NIAP manages the day-to-day operations of the CCEVS, while NVLAP addresses laboratory accreditation. In order to ensure continuing technical competence, NIAP sets additional requirements on Common Criteria Testing Laboratories (CCTLs) during initial evaluation(s) and every two years during ongoing operations.

A CCTL is accredited to perform Common Criteria-based security evaluations of Protection Profiles, Security Targets, and IT products using the Common Criteria assurance classes APE, ASE, and assurance packages EAL levels 1 through 4, and the corresponding Common Evaluation Methodology. An IT product can be a single product or multiple IT products configured as an IT system or system solution to meet certain consumer needs. The testing occurs in a testing facility or a customer's site, but not generally in the actual operational environments.

1 General information

1.1 Scope

1.1.1 The purpose of this handbook is to set out procedures and technical requirements for accreditation of Common Criteria Testing Laboratories (CCTLs).

1.1.2 This handbook complements and supplements the procedures and general requirements found in NIST Handbook 150. The scope of the Common Criteria Testing (ITST CC) program is the conduct of IT security evaluations using the Common Criteria and Common Evaluation Methodology, providing a measure of confidence that such laboratories are capable of performing Common Criteria Security evaluations under the requirements of the National Information Assurance Partnership (NIAP). IT security evaluations assess conformance of a Protection Profile (PP), Security Target (ST), or IT product with a specified set of Common Criteria requirements.

1.1.3 The interpretive comments and additional requirements contained in this handbook make the general NVLAP criteria specifically applicable to the ITST CC program. Specific circumstances under which departures from the NVLAP general procedures are allowable within the scope of the program are also addressed in this handbook.

1.1.4 The requirements identified in this handbook, including the requirements in the annexes, are normative (i.e., mandatory). In addition, the NIST Handbook 150-20 Checklist for the ITST CC program is normative and expands upon the requirements outlined in this document.

1.2 Organization of handbook

1.2.1 The requirements of Handbook 150, the interpretations and specific requirements in this handbook, and the requirements in the program-specific checklist must be combined to produce the criteria for accreditation in the ITST CC program.

1.2.2 The numbering and titles for first and most second level headings of this handbook match those of NIST Handbook 150. Lower level heading are generally specific to the ITST CC program. In some cases upper level headings have been included in the document with no additional text. In these cases, refer to NIST Handbook 150.

1.2.3 Annexes A through D are normative (contain requirements).

1.3 Program description

1.3.1 The Common Criteria is a set of functional and assurance IT security requirements that was developed to provide a common baseline against which IT products and systems can be evaluated. The Common Evaluation Methodology describes a common approach for conducting IT security evaluations using the Common Criteria. The Common Criteria and Common Evaluation Methodology were developed and sponsored by the governments of the United States (represented by NIST and NSA), Canada, France, Germany, the Netherlands, and the United Kingdom. Common Criteria Testing will incorporate new versions of the Common Criteria and Common Evaluation Methodology as they evolve.

1.3.2 NIAP, a partnership between NIST and NSA, requested the development of the Common Criteria Testing program to accredit laboratories that conduct IT security evaluations under CCEVS. CCEVS is the NIAP program to manage the evaluation and validation of IT security products using the Common Criteria and Common Evaluation Methodology. IT security products validated by this program will receive a Common Criteria certificate and be listed on the NIAP Validated Products List. A mutual recognition arrangement signed by United States government agencies and similar agencies representing 14 other economies (as of 2004), promotes the acceptance of products evaluated and validated in one economy by all signatories.

1.4 References

The following documents are referenced in this handbook. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) shall apply within one year of publication or within another time limit specified by regulations or other requirement documents.

1.4.1 NIST Handbook 150, *NVLAP Procedures and General Requirements*, available at <http://www.nist.gov/nvlap>

1.4.2 NIAP scheme publications, available at < http://niap.nist.gov/cc-scheme/GuidanceDocs.html >

— NIAP Scheme Publication #1, *NIAP Common Criteria Evaluation and Validation Scheme for IT Security - Organization, Management, and Concept of Operations*

— NIAP Scheme Publication #2, *NIAP Common Criteria Evaluation and Validation Scheme for IT Security - Validation Body Standard Operating Procedures*

— NIAP Scheme Publication #3, *NIAP Common Criteria Evaluation and Validation Scheme for IT Security - Guidance to Validators of IT Security Evaluations*

— NIAP Scheme Publication #4, *NIAP Common Criteria Evaluation and Validation Scheme for IT Security - Guidance to Common Criteria Testing Laboratories*

— NIAP Scheme Publication #5, *NIAP Common Criteria Evaluation and Validation Scheme for IT Security - Guidance to Sponsors of IT Security Evaluations*

1.4.3 Documents available at the CCEVS web site, < http://niap.nist.gov/cc-scheme/>

— *Common Criteria for Information Technology Security Evaluation, Parts 1 through 3*

— *Common Methodology for Information Technology Security Evaluation (CEM)*

— *Assurance Continuity: CCRA Requirements*

— *Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security*

1.5 Terms and definitions

For the purposes of this handbook, the terms and definitions given in NIST Handbook 150, the Common Criteria, the NIAP Scheme publications, and the following apply.

1.5.1
Common Criteria certificate
Formal recognition by the NIAP Validation Body that the IT security evaluation has been conducted in accordance with the Common Criteria Scheme requirements using the Common Criteria and the Common Evaluation Methodology. A product that has received a Common Criteria certificate is placed on NIAP's Validated Products List.

1.5.2
evaluation
The assessment of a Protection Profile, Security Target, or IT product against a set of Common Criteria requirements using the Common Evaluation Methodology. This term is consistent with the NVLAP notion of "testing."

1.5.3
Evaluation Assurance Level (EAL)
A package of Common Criteria assurance requirements that represents a point on the Common Criteria predefined assurance scale. At present, the Common Criteria defines seven hierarchical EALs, from EAL1 to EAL7; the higher EALs encompass the requirements of the lower EALs. NVLAP accredits for only assurance levels EAL1 through EAL4 at this time.

1.5.4
IT product
A package of IT software, firmware, and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems. An IT product can be a single product or multiple IT products configured as an IT system or system solution to meet certain consumer needs.

1.5.5
Protection Profile (PP)
An implementation-independent set of security requirements for a category of IT products that meet specific consumer needs.

1.5.6
Security Target (ST)
A set of security requirements and specifications to be used as the basis for evaluation under the Common Criteria of an identified Target of Evaluation (TOE). The Security Target specifies the security enforcing functions of the TOE. It also specifies the security objectives, the threats to those objectives, and any specific security mechanisms that are employed.

1.5.7
Target of Evaluation (TOE)
An IT product and its associated administrator and user guidance documentation that is the subject of a security evaluation under the Common Criteria.

1.5.8
validation
The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.

1.6 Program documentation

1.6.1 General

NVLAP checklists enable assessors to document the assessment of a laboratory against the NVLAP requirements found in NIST Handbook 150, this handbook, and in some cases, the checklists themselves. Checklists contain definitive statements or questions about all aspects of the NVLAP criteria for accreditation, and form part of the On-Site Assessment Report (see NIST Handbook 150). Use of checklists helps to ensure the completeness, objectivity, and uniformity of the on-site assessment process. The current version of each checklist is available on the NVLAP web site <http://www.nist.gov/nvlap>.

1.6.2 NIST Handbook 150 Checklist

All NVLAP programs use the NIST Handbook 150 Checklist (formerly called the General Operations Checklist), which contains the requirements published in NIST Handbook 150. The checklist items are numbered to correspond to clauses 4 and 5 and annexes A and B of NIST Handbook 150.

1.6.3 NIST Handbook 150-20 Checklist

The NIST Handbook 150-20 Checklist (also referred to as the Common Criteria Program-Specific Checklist) addresses the requirements specific to the Common Criteria LAP. The checklist items are numbered to correspond to clauses 4 and 5 of NIST Handbook 150-20.

1.6.4 NVLAP Lab Bulletins

NVLAP Lab Bulletins are issued to laboratories and assessors, when needed, to clarify program-specific requirements and to provide information about program additions and changes.

2 LAP establishment, development and implementation

This clause contains no information additional to that provided in NIST Handbook 150, clause 2.

3 Accreditation process

3.1 General

3.1.1 This section discusses the assessment and accreditation process for Common Criteria Testing Laboratories. The accreditation process includes both NIAP and NVLAP components. This handbook documents only the NVLAP portion of the accreditation process. The NIAP portion of this process is documented in NIAP scheme publications.

3.1.2 The assessment process consists of a NVLAP review of the laboratory quality system documentation, an initial on-site assessment visit, proficiency testing, and a full on-site visit assessment.

3.1.3 The proficiency testing program for this LAP is administered by NIAP according to NVLAP requirements. The proficiency test consists of the laboratory conducting an evaluation using the Common

Criteria in accordance with NIAP CCEVS requirements. Successful completion of the evaluation is a requirement for NVLAP accreditation.

3.1.4 Annexes A, B, and C give additional details of the assessment process including the timeline and responsibilities of the parties involved (NVLAP, NIAP, and the laboratory).

3.2 Initial accreditation (see Annex A)

3.2.1 General

3.2.1.1 It is important to note that the candidate laboratory will only be accredited at the EAL of the initial evaluation. For example, if the initial evaluation is at EAL2, then the candidate laboratory will only be accredited to perform evaluations at EAL2 and EAL1 and APE and ASE evaluations. However, an accredited laboratory can change its scope of accreditation (e.g., increase the assurance level to which it is accredited) by submitting a new application to NIAP and NVLAP and successfully completing the initial evaluation at a higher EAL.

3.2.1.2 A laboratory may not perform more than two initial evaluations simultaneously.

3.2.1.3 In order to ensure the independence of the evaluation, neither the candidate laboratory nor other divisions within its parent corporation shall provide consulting services (e.g., develop evaluation evidence), for the products that are evaluated during initial evaluations.

3.2.2 Management system review

3.2.2.1 Prior to applying to NVLAP, the laboratory shall have a fully implemented management system. A copy of the quality manual and relevant associated documents are sent to NVLAP with the application forms.

3.2.2.2 Prior to the initial on-site assessment, one or more NVLAP assessors are assigned to review the documents to ensure they cover all aspects of the management system and, if followed, satisfy the requirements in NIST Handbook 150 and this handbook. During the review, the assessor may identify nonconformities and require changes to the management system so that it meets the requirements.

3.2.3 Initial on-site assessment

3.2.3.1 Once the assessor has determined that the management system meets the requirements, an initial on-site assessment will be scheduled. The purpose of the initial on-site visit is to ensure that the laboratory has the technical staff, capabilities and management system components necessary to successfully complete the initial Common Criteria evaluation.

3.2.3.2 The initial on-site visit may not cover all the NVLAP requirements and may not cite all nonconformities. The laboratory will have the opportunity to make changes and improvements based on the assessment before conducting the initial evaluation.

3.2.3.3 Nonconformities identified during the initial on-site shall be corrected prior to the completion of the accreditation process. Nonconformities that impact the initial evaluation shall be corrected prior to starting the initial evaluation. The laboratory must provide the assessor with a response to the initial on-site assessment report. The assessor will review the response and may ask for additional information.

3.2.3.4 Once the assessor has determined that the management system is mature enough to support the rest of the accreditation process, he or she will notify NVLAP that the laboratory is ready to begin the initial evaluation.

3.2.4 Proficiency testing using an initial evaluation

3.2.4.1 In order to receive NVLAP accreditation, the laboratory shall demonstrate its competence to conduct Common Criteria evaluations. The NVLAP proficiency testing requirement will be met by the laboratory completing a commercial evaluation with the oversight of the NIAP CCEVS. NVLAP and NIAP have cooperated in designing a program that allows the laboratory to enter into a commercial evaluation, meet the NVLAP proficiency testing requirements, and produce an Evaluation Technical Report that can be validated by NIAP.

3.2.4.2 When NVLAP informs NIAP that the initial on-site assessment requirements have been met, NIAP will contact the laboratory to begin planning the initial evaluation. NIAP evaluation and validation requirements are described in NIAP publications.

3.2.4.3 It is important to note that the laboratory cannot be granted accreditation unless:

- the laboratory has evaluated the evidence and provided accurate verdicts for all appropriate assurance classes;
- the laboratory staff has demonstrated its understanding of and competence to apply the Common Criteria and Common Evaluation Methodology during the initial evaluation;
- the laboratory has exercised its quality system and has produced appropriate records of all evaluation activities.

3.2.5 Full on-site visit

3.2.5.1 The laboratory shall perform a complete internal audit and management review of its quality system and the activities and records related to its initial evaluation prior to the full on-site visit. The laboratory may choose to perform portions of the internal audit at regular intervals over the course of its initial evaluation or it may choose to perform it, in its entirety, at the completion of the evaluation. In either case, the internal audit and management review shall be completed prior to the full on-site visit.

3.2.5.2 Once the candidate laboratory successfully completes all other accreditation requirements, NVLAP will schedule the full on-site visit.

3.2.5.3 Typically two NVLAP assessors will perform the full on-site visit over a two-and-one-half day period. The assessment will take place at the laboratory site.

3.2.5.4 The laboratory shall have its facilities and equipment in good working order and be ready for examination according to the requirements identified in this handbook, NIST Handbook 150, the NIST Handbook 150-20 Checklist, and the laboratory's quality manual. Efforts will be made to minimize disruption to the normal working routines during the assessment. The assessors will need time and workspace to complete assessment documentation during their time at the laboratory site.

3.2.5.5 The assessors will use the NIST Handbook 150 Checklist and the NIST Handbook 150-20 Checklist. The checklists, based on NIST Handbook 150 and the technical specifics contained in this handbook, ensure that the assessment is complete and that all assessors cover the same items at each

laboratory. The assessors may request additional information in an effort to clarify checklist responses or delve more deeply into a technical issue.

3.2.5.6 The activities covered during a typical on-site assessment are described below. The assessor, prior to the visit, will provide a specific agenda.

a) *Opening meeting:* The assessors meet with laboratory management and supervisory personnel to explain the purpose of the on-site assessment 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 members may attend this meeting.

b) *Staff interviews:* The assessors will ask the laboratory manager to assist in arranging times for individual interviews with laboratory staff members. While it is not necessary for the assessors to talk to all staff members, they will select staff members representing all aspects of the laboratory. Assessors will also talk to staff members who participated in the initial evaluation.

   Laboratory personnel should not answer any question they do not feel qualified to answer. The assessors usually consider knowing whom to ask or where to find the answer an acceptable response.

c) *Records review:* The assessors will review laboratory documentation, including the quality system, quality manual, equipment and maintenance records, record-keeping procedures, testing procedures, laboratory evaluation records and reports, personnel competency records, personnel training plans and records, procedures for updating pertinent information (e.g., Common Criteria or Common Evaluation Methodology versions, NIAP Validation Body guidance or interpretations, or the validated products list), and safeguards for the protection of vendor-sensitive and proprietary information.

   The assessors do not need access to employee information that may be considered sensitive or private such as salary, medical information, or performance reviews for work done outside the scope of the laboratory's accreditation. However, this information is often stored together with technical information that the assessors will need to check (e.g., job descriptions, resumes, and technical performance reviews). In these cases, the assessors will work with the candidate laboratory to ensure that they are able to perform their review without violating individual privacy. At the discretion of the laboratory, a member of its Human Resources Department may be present during the review of personnel information.

d) *Audit and management review:* The assessors will review and discuss the laboratory's internal audit and management review activities with the laboratory staff. The discussion will include all aspects of those activities including the quality system procedures, the audit findings, the results of the management review, and the actions taken to resolve problems identified.

e) *Proficiency testing:* The assessors will discuss all aspects of the initial evaluation/proficiency test with laboratory staff. Evaluation methodology and the records documenting the laboratory's execution of that methodology will be reviewed and discussed.

f) *Issues from initial on-site:* The assessor will review and discuss the initial on-site assessment. This will normally include verification that all nonconformities have been satisfactorily addressed and a review of concerns and comments previously identified.

g) *Closing meeting:* At the end of the on-site assessment, an exit briefing is held with the laboratory manager and staff to discuss the assessors' findings. During the visit the assessor will have categorized all problems identified as nonconformities, concerns or comments. They will be discussed at the exit briefing and resolutions may be mutually agreed upon. The assessors, in their findings, specifically note items that have been corrected during the on-site assessment along with any recommendations for other action(s). The process for resolving nonconformities identified during the on-site is documented in NIST Handbook 150. Concerns should be given serious consideration by the laboratory. Concerns expressed during one on-site visit may become nonconformities at a subsequent on-site visit.

Any disagreements between the laboratory and the assessors will be referred to NVLAP for resolution.

h) *On-site assessment report:* The assessors complete an on-site assessment report, which summarizes the findings. This report normally consists of the On-Site Report, the NIST Handbook 150 Checklist, and the NIST Handbook 150-20 Checklist. The assessors and the laboratory's Authorized Representative sign the report. A copy of the complete report is given to the laboratory representative.

3.2.6 NVLAP review

3.2.6.1 Once the full on-site visit has been completed and all nonconformities have been resolved, NVLAP will make the final decision on accreditation. The NVLAP decision will be based upon information drawn from the quality system review, on-site visits, and the proficiency testing. This decision may be to grant accreditation, require additional work before accreditation can be granted, or to deny accreditation.

3.2.6.2 The Chief of NVLAP is responsible for all NVLAP accreditation actions. Once a decision has been made, the candidate laboratory is then notified of the outcome.

3.3 NVLAP renewal of accreditation (see Annex B)

3.3.1 Accreditation is renewed annually. The activities and fees associated with renewal will vary depending upon the year in which accreditation is being renewed due to the cost of on-site assessments. NVLAP will send to each laboratory a renewal package and description of required activities and fees.

3.3.2 In the first renewal year and every two years thereafter, an on-site assessment of the laboratory is conducted to determine compliance with the NVLAP criteria and continued competence. The scope and format of this assessment is the same as was previously documented for the NVLAP full on-site assessment visit.

3.3.3 Beginning in the middle of the second year of accreditation and every two years thereafter, NIAP CCEVS requires that the laboratory demonstrate its continued proficiency to perform Common Criteria evaluations by conducting a commercial evaluation under the oversight of a NIAP Technical Oversight Panel (TOP). This evaluation must be pre-arranged with NIAP and must be at the highest EAL for which accreditation has been granted. At the successful completion of the evaluation, NIAP will report to NVLAP the results of the proficiency testing and any nonconformities. This demonstration will serve to meet the NVLAP proficiency testing requirement.

3.3.4 The laboratory scope of accreditation will be based upon the EAL of the proficiency test. If a laboratory does not demonstrate proficiency at its highest scope of accreditation in two consecutive proficiency tests, its scope of accreditation will be reduced to the EAL of the most recent proficiency test.

3.4 Increasing the scope of accreditation (see Annex C)

3.4.1 A laboratory that is not accredited to the highest available scope of accreditation may at any time request to increase its scope of accreditation. To be granted this increase in scope, the laboratory shall conduct an appropriate proficiency test at the higher EAL. The proficiency test process will be similar to the process for an initial evaluation.

3.4.2 NVLAP will review the request for increase in scope and, at its option, may perform an on-site assessment before or after the proficiency testing. NVLAP will notify NIAP CCEVS of the application for increase in scope and the need for proficiency testing. After all activities have been completed NVLAP will review the results and make a decision on accreditation.

3.4.3 In order to ensure the independence of the evaluation, neither the laboratory nor other divisions within its parent corporation shall provide consulting services (e.g., develop evaluation evidence), for the products that are evaluated for the increase in NVLAP scope of accreditation.

3.5 Suspending and revoking accreditation

3.5.1 The NVLAP procedures for suspending and revoking accreditation are given in NIST Handbook 150.

3.5.2 Significant changes in key technical personnel or facilities may result in a NVLAP monitoring visit(s), increased oversight by NIAP, and/or suspension of accreditation. Loss of key personnel may result in immediate suspension.

3.5.3 If the laboratory does not demonstrate continued competence to perform Common Criteria evaluations or the NIAP oversight identifies significant additional areas of concern, the laboratory's accreditation may be suspended or revoked.

3.5.4 Failure to appropriately address and resolve complaints from customers, NIAP, or other interested parties may result in NVLAP surveillance activity, additional proficiency testing, and/or suspension or revocation of accreditation.

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.

4.2 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 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.

4.2.4 Records shall be kept of all management system activities.

4.3 Document control

There are no requirements additional to those set forth in NIST Handbook 150.

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

NVLAP defines subcontracting of tests and calibrations to be the use of testing and calibration services outside of the laboratory to perform tests that are outside the laboratory's scope of accreditation, e.g., EMI testing or FIPS 140 validation. Subcontracting is not used to describe a mechanism by which the laboratory employs staff members.

4.6 Purchasing services and supplies

There are no requirements additional to those set forth in NIST Handbook 150.

4.7 Service to the customer

There are no requirements additional to those set forth in NIST Handbook 150.

4.8 Complaints

There are no requirements additional to those set forth in NIST Handbook 150.

4.9 Control of nonconforming testing and/or calibration work

There are no requirements additional to those set forth in NIST Handbook 150.

4.10 Improvement

There are no requirements additional to those set forth in NIST Handbook 150.

4.11 Corrective action

There are no requirements additional to those set forth in NIST Handbook 150.

4.12 Preventive action

There are no requirements additional to those set forth in NIST Handbook 150.

4.13 Control of records

4.13.1 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. Required records of evaluation activities shall be traceable to Common Criteria evaluator actions and Common Evaluation Methodology work units. 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. Entries in laboratory notebooks shall be dated and signed or initialed. All records shall be maintained in accordance with laboratory policies and procedures and in a manner that ensures record integrity. 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.

4.14 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 3.2.5). A partial internal audit should be performed prior to the initial on-site assessment (see 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 3.2.5). A management review should be performed prior to the initial on-site assessment (see 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 this handbook.

5.2 Personnel

5.2.1 The laboratory shall maintain a competent administrative and technical staff appropriate for Common Criteria- based IT security evaluations. 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. 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 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. 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. Training materials that are maintained within the laboratory shall be kept up-to-date.

5.2.8 The laboratory shall review annually the competence of each staff member for each test method the staff member is authorized to conduct. 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. A record of the annual review of each staff member shall be dated and signed by the supervisor and the employee. A description of competency review programs shall be maintained in the management system.

5.2.9 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. 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 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. Laboratories shall have systems (e.g., firewall, intrusion detection) in place to protect internal systems from untrusted external entities. 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 The laboratory shall have regularly updated protection for all systems against viruses and other malware. 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 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.

PKI enabled electronic mail (DOD class 3 email certificates) capability is required for communications with the NIAP/CCEVS. 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 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. 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 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. The laboratory shall ensure that these procedures are followed.

5.4.5 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. 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 The laboratory shall maintain on-site systems adequate to support IT security evaluations in keeping with the tests for which it is seeking accreditation. 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 Computer systems and other platforms used during the conduct of testing shall be under configuration control. 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 traceability

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 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. 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

The laboratory shall use documented procedures for sampling. Whenever sampling is used during an evaluation, the laboratory shall document its sampling strategy, the decision-making process, and the nature of the sample. Sampling shall be part of the evaluation record.

5.8 Handling of test and calibration items

5.8.1 The laboratory shall protect products under evaluation and calibrated tools from modification, unauthorized access, and use. 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 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. 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 Evaluation reports created for submission to the CCEVS shall meet the requirements of the Common Criteria Scheme. 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. 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 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. 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. 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.

6 Additional requirements

There are no additional requirements beyond NIST Handbook 150 and its associated normative annexes, and any other normative references previously cited in this handbook.

Annex A
(normative)

Initial accreditation

Initial accreditation is the process by which a candidate laboratory (laboratory) attains accreditation. Accreditation requirements are set by both NIAP CCEVS (Annex C of Scheme Publication 1) and NVLAP (NIST Handbook 150, NIST Handbook 150-20, and their associated checklists). Approved Common Criteria Testing Laboratories (CCTLs) are IT security testing laboratories that are accredited by NVLAP and meet CCEVS-specific requirements to conduct IT security evaluations for conformance to the Common Criteria for Information Technology Security Evaluation. The initial accreditation matrix below provides a chronology of the initial accreditation process.

Initial Accreditation Matrix			
No.	**LABORATORY**	**NIAP**	**NVLAP**
1	The laboratory reviews NIAP requirements and verifies that it meets those requirements.	**NIAP Information** http://niap.nist.gov/cc-scheme/ (410) 854-4458 (410) 854-6615 (fax) ccevs-staff@nist.gov	
2	Once the laboratory believes it has satisfied all NIAP requirements, it sends letter indicating its intent to pursue accreditation to NIAP.	NIAP begins planning resources to be used in the validation process. NIAP will send an informal note to NVLAP indicating that the laboratory has expressed its intent to pursue accreditation.	
3	The laboratory reviews NVLAP requirements including NIST Handbooks 150, 150-20, their associated checklists and all NIAP Common Criteria Lab Bulletins.		**NVLAP Information** http://www.nist.gov/nvlap (301) 975-4016 (301) 926-2884 (fax) nvlap@nist.gov
4	The laboratory verifies that it meets all NVLAP requirements for accreditation by creating a mapping between all NVLAP requirements and the laboratory's quality system.		
5	The laboratory completes an application for NVLAP accreditation. The application includes payment of applicable fees identified in the NVLAP fee schedule.		The NVLAP application and fee schedule are available from NVLAP's web site: http://www.nist.gov/nvlap.

Initial Accreditation Matrix			
No.	**LABORATORY**	**NIAP**	**NVLAP**
6	The laboratory sends quality system documents, application, and payment of all applicable fees to NVLAP.		NVLAP processes the application and assigns an assessor to review the quality system documentation submitted. The assessor, through NVLAP, will communicate his/her findings to the laboratory. If quality system documentation does not meet all requirements, those findings may include nonconformities, concerns and comments.
7	The laboratory must resolve all nonconformities and address all concerns.		If the resolution of the assessor's findings requires additional oversight or document review by the assessor, then NVLAP may charge additional fees to the laboratory and the previous step may be repeated.
8			Once NVLAP determines that the quality system documentation meets the NVLAP requirements, the initial on-site visit to the laboratory is scheduled.
9	The NVLAP assessor conducts a one to one-and-one-half day initial on-site assessment visit.		The NVLAP assessor conducts the initial on-site assessment. The assessment will include a review of quality system, staff, environment, equipment, knowledge of CC and CEM, and readiness to conduct initial evaluation(s). At the conclusion of the visit, the assessor will provide the laboratory with a copy of the report. If the laboratory does not meet all requirements, those findings may include nonconformities, concerns and comments.
10	The laboratory must resolve all nonconformities and address all concerns.		If the resolution of the assessor's findings requires an additional visit or significant additional oversight by the NVLAP assessor, then additional fees may be charged to the laboratory and the previous step may be repeated.

Initial Accreditation Matrix			
No.	**LABORATORY**	**NIAP**	**NVLAP**
11			Once NVLAP determines that the laboratory has satisfactorily resolved all nonconformities and concerns related to the initial on-site, NVLAP will send a letter/message to NIAP and the laboratory indicating that the laboratory is ready for proficiency testing (proficiency testing is performed through an initial evaluation monitored by NIAP).
12	Upon receiving notification, the next action for the laboratory is to find a vendor/sponsor and reach agreement to submit their product for NIAP evaluation. Since the initial evaluation will determine the EAL at which the laboratory will be accredited, the laboratory should seek to find work that would lead to the desired level of accreditation. The CCTL must discuss with its prospective vendor/sponsor and with CCEVS management prior to contract signing to ensure that the product (TOE) is acceptable and both the CCTL and the vendor/sponsor understand the conditions of the NIAP initial evaluation.	Upon receiving notification that the laboratory is ready to proceed with proficiency testing, NIAP will work with the laboratory to identify an appropriate evaluation. Because TOEs can fill the entire spectrum from simple to complex, NIAP must ensure that the TOE, and hence the evaluation work involved in evaluating that TOE, will provide the evidence needed for NIAP to determine the lab's proficiency. In order to ensure the independence of the evaluation, CCEVS management will verify that the laboratory and the sponsor understand that neither the laboratory nor other divisions within its parent corporation shall provide consulting services (e.g., develop evaluation evidence) for the products selected for the initial evaluations. CCEVS management will also inform the sponsor of the inherent risks related to the initial evaluation and suggest specific risk-mitigating actions of the sponsor to avoid legal and/or financial hardship. One risk-mitigating factor will be to ensure that the evaluation results are available to the vendor/sponsor to allow the results of an evaluation to be moved to an accredited laboratory should the laboratory experience issues that would cause the CCTL to not be accredited.	

Initial Accreditation Matrix			
No.	**LABORATORY**	**NIAP**	**NVLAP**
13	Once the vendor/sponsor, laboratory, and CCEVS are in agreement, the laboratory submits an evaluation work package for the initial evaluation to NIAP CCEVS.	Upon receipt of the evaluation work package, CCEVS management will then assign a validator and a Technical Oversight Panel (TOP). The TOP will include at least one senior validator and one validator who is also a qualified NVLAP assessor (but not the assessor assigned to the laboratory). The TOP, along with the validator, will provide oversight during the laboratory's initial evaluation. After reviewing the evaluation work package, the assigned senior validator will schedule the kickoff meeting.	
14	The laboratory will conduct the initial evaluation under the oversight of a TOP. The TOP procedures during initial accreditation are documented in the TOP document (CCEVS-TOP-0001). This document identifies the procedures and scope of TOP activities.	The TOP procedures during initial accreditation are documented in the TOP document (CCEVS-TOP-0001). As is noted in the TOP document, one additional validation team activity is to verify the effectiveness of the laboratory's management system. This activity occurs periodically over the course of the evaluation and is reported on the NIAP CCEVS quality system checklist.	NVLAP will monitor the progress of the initial evaluation/proficiency test and may observe TOP meetings. NVLAP will review nonconformities, comments, and concerns from NIAP validation team. As the initial evaluation draws to a conclusion, NVLAP will assign or augment the assessor team in preparation for the full on-site assessment.
15		At the conclusion of the initial evaluation, NIAP CCEVS will notify NVLAP of the outcome and forward a copy of the NIAP CCEVS quality system checklist to NVLAP. NIAP will provide the laboratory notification that the proficiency test is complete.	NVLAP reviews the report of the conduct of the initial evaluation for the purpose of fulfilling the NVLAP proficiency testing requirements and contacts the laboratory to schedule the full on-site assessment.

Initial Accreditation Matrix			
No.	**LABORATORY**	**NIAP**	**NVLAP**
16	In preparation for the full on-site assessment, the laboratory conducts an internal audit and management review. The audit/management reviews must include the quality system, staff, procedures, and records generated during initial evaluation (NVLAP PT) and all requirements in NIST Handbooks 150 and 150-20. Using the results of the audit and management reviews, the laboratory implements improvements identified during PT and internal audit. The laboratory forwards the internal audit report and management review report to NVLAP for assessor review.		NVLAP invoices the laboratory for the full on-site assessment (Admin/Tech support fee and On-site Assessment fee). NVLAP typically assigns two assessors for the full on-site assessment. The assessors review changes to quality system, internal audit and management review reports and the results of proficiency testing activities from NIAP. Typically the assessor who conducted the initial review of the quality system documentation will be one of the two assigned assessors.
17	The laboratory pays the full on-site visit fee and continues to improve its management system, training, competence, etc.		NVLAP schedules the full on-site visit to the laboratory. This is typically two assessors for approximately 2 1/2 days.
18	The NVLAP assessors spend 2 1/2 days at the laboratory conducting the full on-site.		The NVLAP assessors conduct the full on-site assessment. The assessment will include all requirements of NIST Handbook 150, 150-20, all Common Criteria technical and competence requirements, including the results of the initial evaluation. At the conclusion of the visit, the assessor will provide the laboratory with a copy of the on-site report. If the laboratory does not meet all requirements, those findings may include nonconformities, concerns and comments.
19	The laboratory must resolve all nonconformities and address all concerns.		If the resolution of the assessor's findings requires an additional visit or significant additional oversight by the NVLAP assessor, then additional fees may be charged to the laboratory and the previous step may be repeated.

Initial Accreditation Matrix			
No.	**LABORATORY**	**NIAP**	**NVLAP**
20			Once all NVLAP and appropriate NIAP requirements have been met, NVLAP grants initial accreditation for Scope based on Initial Evaluation/proficiency test. NVLAP notifies NIAP CCEVS and the laboratory that the laboratory has been accredited.
21		NIAP CCEVS issue a certification for the product evaluated during the Initial Evaluation.	
22	The accredited laboratory must continue to maintain its quality system, which includes notifications to both NVLAP and NIAP of changes in key staffing positions, ownership, and/or facilities.		

Annex B
(normative)

Renewal of accreditation

Accredited laboratories must renew their accreditation annually. However, the activities and fees associated with renewal will vary depending upon the year in which accreditation is being renewed. In the first renewal year and every two years thereafter, an on-site assessment of the laboratory is conducted to determine compliance with the NVLAP criteria. Beginning six months prior to the third renewal year and every two years thereafter, NIAP CCEVS requires that the laboratory demonstrate its continued proficiency to perform Common Criteria evaluations by performing an evaluation under the oversight of a TOP. In those renewal years when there is no on-site assessment and no renewal TOP, the laboratory completes and returns the NVLAP renewal forms and pays the NVLAP fees.

The matrix below documents the renewal process for the third renewal year and every two years thereafter. This covers all renewal activities (evaluation via NIAP CCEVS TOP, NVLAP on-site assessment, and payment of renewal fees). Renewal of accreditation in other years will be similar, but only the activities relevant to that renewal year will occur.

Renewal Matrix			
No.	**LABORATORY**	**NIAP**	**NVLAP**
1	Six months prior to it renewal date, the CCTL provides NIAP CCEVS with a list of its expected evaluations.	NIAP CCEVS will work with the CCTL to select an appropriate evaluation for the renewal TOP. Because TOEs can fill the entire spectrum from simple to complex, NIAP must ensure that the TOE, and hence the evaluation work involved in evaluating that TOE, will provide the evidence needed for NIAP to verify the laboratory's proficiency. It is important to note that the laboratory must demonstrate proficiency at its current highest scope of accreditation. Failure to do so will result in NIAP CCEVS requiring additional oversight on any subsequent evaluation at an EAL above the level at which the laboratory's accreditation was renewed.	

Renewal Matrix			
No.	**LABORATORY**	**NIAP**	**NVLAP**
2	By the due date, the laboratory submits a renewal package to NVLAP, including all documentation and fees appropriate for the renewal year. If the renewal year activities include an on-site assessment, then the renewal package will include both the Administrative/Technical Support fee and On-site Fee. Otherwise, the package should only include an Administrative Technical Support fee.		NVLAP processes the renewal package but does not renew accreditation until all NVLAP and NIAP requirements are satisfied.
3	The CCTL will conduct the renewal evaluation under the oversight of a TOP. The TOP procedures during renewal of accreditation are documented in the TOP document (CCEVS-TOP-0001). This document identifies the procedures and scope of TOP activities.	The TOP procedures during renewal of accreditation are documented in the TOP document (CCEVS-TOP-0001). As is noted in the TOP document, one additional validation team activity is to verify the effectiveness of the laboratory's quality system. This activity occurs periodically over the course of the evaluation and is reported on the NIAP CCEVS quality system checklist. Upon completion of the renewal TOP, NIAP will inform both NVLAP and the CCTL of the results.	NVLAP will monitor the progress of the renewal evaluation/ proficiency test and may observe TOP meetings. NVLAP will review nonconformities, comments, and concerns from NIAP validation team. As the renewal evaluation draws to a conclusion, NVLAP will assign an assessor team in preparation for the renewal on-site assessment.
4	The NVLAP assessors spend 2 1/2 days at the laboratory conducting the renewal on-site assessment visit.		The NVLAP assessors conduct the renewal on-site assessment. The assessment will include all requirements of NIST Handbook 150, 150-20, all Common Criteria technical and competence requirements, including the results of the initial CC evaluation At the conclusion of the visit, the assessor will provide the laboratory with a copy of the on-site report. If the laboratory does not meet all requirements, those findings may include nonconformities, concerns and comments.

Renewal Matrix			
No.	**LABORATORY**	**NIAP**	**NVLAP**
5	The laboratory must resolve all nonconformities and address all concerns.		If the resolution of the assessor's findings requires an additional visit or significant additional oversight by the NVLAP assessor, then additional fees may be charged to the laboratory and the previous step may be repeated.
6			Once all NVLAP and appropriate NIAP requirements are met, NVLAP renews the laboratory's accreditation for Scope based upon the renewal TOP and proficiency test. If the renewal period did not include a renewal TOP and proficiency test, then the laboratory's scope of accreditation will not change.
7	The accredited laboratory must continue to maintain its quality system, which includes notifications to both NVLAP and NIAP of changes in key staffing positions, ownership, and/or facilities.		

Annex C
(normative)

Increasing the scope of accreditation

If a laboratory's scope of accreditation is below the maximum Evaluated Assurance Level (EAL4) for the CCEVS program, then it may apply to increase its scope of accreditation at any time. If the laboratory has not been accredited to the EAL for which it has applied, then it must follow the procedures documented in Annex A for an initial evaluation in order to increase its scope of accreditation. Otherwise, the matrix below provides a chronology of the steps a laboratory must follow to increase its scope of accreditation.

Increasing the Scope of Accreditation			
No.	**LABORATORY**	**NIAP**	**NVLAP**
1	The laboratory performs an internal audit and management review of its quality system and procedures to ensure that they will support evaluation activities at the higher EAL. The laboratory sends a request to increase its scope of accreditation to NVLAP along with the results of its internal audit and management review.		Upon receiving the request for an increase in scope NVLAP will notify CCEVS that the laboratory wishes to increase its scope of accreditation and begin review of the documentation submitted.

Increasing the Scope of Accreditation			
No.	**LABORATORY**	**NIAP**	**NVLAP**
2	The next action for the CCTL is to find a vendor/sponsor and reach agreement to submit their product for NIAP evaluation at the higher assurance level. The CCTL must discuss with its prospective vendor/sponsor and with CCEVS management prior to contract signing to ensure that the product (TOE) is acceptable and both the CCTL and the vendor/sponsor understand the conditions of the NIAP initial evaluation.	Upon receiving notification that the CCTL wishes to increase its scope of accreditation, NIAP will work with the laboratory to identify an appropriate evaluation. Because TOEs can fill the entire spectrum from simple to complex, NIAP must ensure that the TOE, and hence the evaluation work involved in evaluating that TOE, will provide the evidence needed for NIAP to determine the laboratory's proficiency at the intended assurance level. In order to ensure the independence of the evaluation, CCEVS management will verify that the laboratory and the sponsor understand that neither the laboratory nor other divisions within its parent corporation shall provide consulting services (e.g., develop evaluation evidence) for the products that are evaluated for the increase in NVLAP scope of accreditation.. CCEVS management will also inform the sponsor of the inherent risks related to the evaluation and suggest specific risk-mitigating actions of the sponsor to avoid legal and/or financial hardship. One risk-mitigating factor will be to ensure that the evaluation results are available to the vendor/sponsor to allow the results of an evaluation to be moved to a laboratory accredited to perform work at the EAL of the TOE, should the laboratory experience issues that would cause it not to be accredited at the higher EAL.	

Increasing the Scope of Accreditation			
No.	**LABORATORY**	**NIAP**	**NVLAP**
3	Once the vendor/sponsor, CCTL and CCEVS are in agreement, the laboratory will submit an evaluation work package for the initial CC evaluation to NIAP CCEVS.	Upon receipt of the evaluation work package, CCEVS management will then assign a validator and a Technical Oversight Panel (TOP). The TOP will include at least one senior validator and one validator who is also a qualified NVLAP assessor (but not the assessor assigned to accrediting the laboratory). The TOP, along with the validator, will provide oversight during the CCTL's evaluation. After reviewing the evaluation work package, the assigned senior validator will schedule the kickoff meeting.	
4	The laboratory will conduct the evaluation under the oversight of a TOP. The TOP procedures during accreditation are documented in the TOP document (CCEVS-TOP-0001). This document identifies the procedures and scope of TOP activities.	The TOP procedures during accreditation are documented in the TOP document (CCEVS-TOP-0001). As is noted in the TOP document, one additional validation team activity is to verify the effectiveness of the laboratory's quality system. This activity occurs periodically over the course of the evaluation and is reported on the NIAP CCEVS quality system checklist.	NVLAP will monitor the progress of the initial CC evaluation/proficiency test and may observe TOP meetings. NVLAP will review nonconformities, comments, and concerns from NIAP validation team. As the evaluation draws to a conclusion, NVLAP will assign an assessor team to review the results of the internal audit and management review, and the NIAP CCEVS quality system checklist.
5		At the conclusion of the initial CC evaluation, NIAP CCEVS will notify NVLAP and the CCTL of the outcome and forward a copy of the NIAP CCEVS quality system checklist to NVLAP.	NVLAP reviews all documentation and, at its option, determines whether or not an on-site assessment is necessary. If NVLAP decides that an on-site assessment is required, it will contact the laboratory to schedule it.

Increasing the Scope of Accreditation			
No.	**LABORATORY**	**NIAP**	**NVLAP**
6	The NVLAP assessors spend 2 1/2 days at the laboratory conducting the on-site assessment.		The NVLAP assessors conduct the on-site assessment. The assessment will include all requirements of NIST Handbook 150, 150-20, all Common Criteria technical and competence requirements, including the results of the initial evaluation. At the conclusion of the visit, the assessor will provide the laboratory with a copy of the report. If the laboratory does not meet all requirements, those findings may include nonconformities, concerns and comments.
7	The laboratory must resolve all nonconformities and address all concerns.		If the resolution of the assessor's findings requires an additional visit or significant additional oversight by the NVLAP assessor, then additional fees may be charged to the laboratory and the previous step may be repeated.
8			Once all NVLAP and appropriate NIAP requirements have been met, NVLAP will notify NIAP of the outcome and increase the laboratory's accreditation for Scope based upon the TOP/proficiency test.
9	The accredited laboratory must continue to maintain its quality system, which includes notifications to both NVLAP and NIAP of changes in key staffing positions, ownership, and/or facilities.		

Annex D
(normative)

Written procedures

D.1 Overview

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. 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 (required, but not limited to)

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

a) internal audits and management review,

b) writing and implementing procedures,

c) writing and implementing instructions,

d) staff training and individual development plans,

e) contract review,

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

g) referencing NVLAP accreditation and use of the NVLAP logo.

D.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 Common Methodology (CEM) work-unit level instructions before an evaluation is conducted:

a) writing a work plan for an evaluation,

b) selecting the members of an evaluation team,

c) writing an Evaluation Technical Report (ETR),

d) writing an Observation Report (OR),

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

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

g) vulnerability analysis,

h) conducting independent testing,

i) requesting and incorporating CC interpretations,

j) working with NIAP or other validators during an evaluation,

k) records and record-keeping for evaluations, and

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.