National Information Assurance Partnership/ Common Criteria Evaluation and Validation Scheme

Publication #3

Guidance to Validators

February 2020
Version 4.0

All correspondence in connection with this document should be addressed to:

National Security Agency
Common Criteria Evaluation and Validation Scheme
9800 Savage Road, Suite 6940
Fort George G. Meade, MD 20755-6940
E-mail: niap@niap-ccevs.org
https://www.niap-ccevs.org/

Amendment record

Version	Date	Description
Draft 1.0	20 March 2001	Initial release
2.0	8 September 2008	Complete revision based on current operations
3.0	May 2014	Updates
4.0	February 2020	Updated to reflect minor program changes

(This page intentionally left blank)

Table of Contents

1 Introduction

The Common Criteria Evaluation and Validation Scheme (CCEVS), hereafter referred to as The National Information Assurance Partnership (NIAP), Common Criteria Scheme, or Scheme, was originally established by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) to validate conformance of Information Technology (IT) products to international standards. NIAP, now solely part of NSA, oversees the evaluations performed by Common Criteria Testing Labs (CCTLs) on information technology products against the Common Criteria for Information Technology Security Evaluation (CC).

The principal participants in the NIAP program are the:

- **Sponsor**: The Sponsor may be a product developer, a value-added reseller of an IT security-enabled product, or another party that wishes to have a product evaluated. The sponsor requests that a Common Criteria Testing Laboratory (CCTL) conduct a security evaluation of an IT product.

- **Common Criteria Testing Laboratory (CCTL)**: The CCTL is a commercial testing laboratory accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by NIAP to perform security evaluations against the Common Criteria for Information Technology Security Evaluation (CC) using the Common Methodology for Information Technology Security Evaluation (CEM).

- **National Information Assurance Partnership (NIAP**): NIAP is the US Government organization established by NSA to maintain and operate the Scheme for the U.S. Government and to oversee and validate the evaluations performed by the CCTLs.

1.1 Purpose

The purpose of this document is to provide guidance and assistance to validators in performing their assigned duties. Additionally, the document provides information to the CCTLs and sponsors of evaluations about the activities and responsibilities of assigned validators.

Validation is the independent confirmation that an IT security evaluation has been conducted in accordance with the provisions of NIAP and the conclusions of the CCTL are consistent with the evidence presented and is documented in the CCTL Evaluation Technical Report (ETR). Validation involves confirming the CCTL evaluation results and producing the validation report. To accomplish validation, the Scheme assigns validators for each IT security product under evaluation.

1.2 Scope

This document is part of a series of technical and administrative NIAP publications describing how the Scheme operates. It consists of several chapters and supporting annexes.

- Chapter 1 provides a high level overview of NIAP;

- Chapter 2 provides details on the validation process, including validator responsibilities;
- Chapter 3 provides information related to the validator‘s role in NVLAP and CCTL quality systems;
- Chapter 4 describes the validator‘s responsibilities as they relate to specific CCTL evaluation milestones;
- Chapter 5 discusses policy interpretations and evaluation documentation;
- Chapter 6 explains the NIAP record system requirements; and
- Chapter 7 details the various validator support mechanisms available.

This document complements or references other NIAP publications and documents used in the operation of NIAP. These other publications include:

Publication #1: *Organization, Management, and Concept of Operations*

Publication #2: *Quality Manual and Standard Operating Procedures*

Publication #3: *Guidance to Validators*

Publication #4: *Guidance to CCEVS Approved Common Criteria Testing Laboratories*

Publication #5: *Guidance to Sponsors*

Publication #6: *Assurance Continuity: Guidance for Maintenance and Re-evaluation*

These publications, along with additional information, documents, and guidance are available on the NIAP web site at https://www.niap-ccevs.org/.

2 Validation Process and Validator Responsibilities

NIAP oversees evaluations of commercial IT products for use in National Security Systems. NIAP validation oversight ensures consistency and accuracy throughout the evaluation process, resulting in issuance of a Common Criteria Certificate upon successful evaluation completion. The following sections outline the goals, activities, and responsibilities of a validator.

2.1 Validation Goal

The primary goal of validation is for NIAP to ensure the technical quality, correctness, and consistency of each evaluation in accordance with the CCRA, CC, CEM, and all NIAP guidance. All NIAP evaluations must demonstrate exact conformance to a NIAP-approved PP and adhere to NIAP policies and processes.

2.2 Validation Activities

Validation activities are used to ensure the results of the evaluation analysis are technically correct and consistent with the CCRA, CC, CEM, and Protection Profile (PP). Validators are responsible for reviewing the CCTL evaluation results - not for performing the evaluation. Validators focus on reviewing CCTL testing documentation in assessing the CCTL's application of the PP. In determining a complete, correct and consistent evaluation of a product, or Target of Evaluation (TOE), the validator performs some or all of the following activities:

- Ensuring the evaluation adheres to all NIAP Policies and Processes;
- Reviewing CCTL evaluation procedures;
- Interacting and holding discussions with evaluation teams;
- Monitoring CCTL evaluation meetings;
- Observing CCTL testing activities;
- Ensuring timely resolution to evaluation issues and questions;
- Reviewing evaluation evidence
- Confirm the evaluation team is aware of applicable evaluation techniques, practices, test methods, processes and procedures available to all CCTLs; and
- Suggest, where appropriate, the type of information that should be included in ETRs and records to enable efficient and effective validation of evaluation results

2.3 Validation Process Overview

All NIAP evaluations must claim exact conformance to a NIAP-approved PP. NIAP-approved PPs objectively define security requirements and assurance activities for various technologies and promote consistency within NIAP and among the CCRA Schemes. This expedites the evaluation process, and ensures an achievable, repeatable, and testable evaluation.

2.3.2 Check-In/Check-Out (CICO)

In the Check-In/Check-Out (CICO) process, NIAP oversees the evaluation process by conducting periodic meetings in which those involved in the evaluation will track progress and discuss issues within the context of a specific evaluation.

Details about the CICO process and the documentation requirements are contained in NIAP's Check-In/Check-Out Guidance (CICO Guide).

The CICO process is designed to accommodate evaluations against NIAP-approved PPs, which are more objective and promote consistency in evaluations. Because NIAP-approved PPs have clearly defined tailored assurance activities, NIAP anticipates the evaluation of products against the PPs to proceed more quickly. Products submitted for evaluation against a NIAP-approved PP are expected to have a Check-In package containing the information specified within the CICO Guide. A complete Check-In package mitigates the chance of delays during the evaluation and aligns with the goal of timely NIAP evaluations.

2.4 Validator Responsibilities

The primary responsibility assigned to a validator is to ensure the evaluation is complete, technically sound, and conducted in accordance with NIAP guidance. Furthermore, the validator's role is to promote quality in CCTL evaluations without hindering the CCTL's ability to conduct the evaluation in a timely manner.

All evaluations are assigned a lead validator and a senior validator. The lead validator is the technical point of contact and performs all validation activities for the evaluation. The senior validator provides technical support to the lead validator. Additional validators may also be assigned to an evaluation as needed to support validation activities when evaluation complexities or technical details are warranted.

2.4.1 Validate Evaluation Results

Validation of the CCTL's evaluation efforts will take place during CICO and Sync Sessions. The validator will perform the following quality management activities in validating evaluation results:

- Verify planned evaluation activities, methodologies, and procedures are feasible and appropriate;
- Verify the CC, CEM, and PP are consistently and correctly applied in evaluations;
- Review documented evaluation results, verdicts, and rationales for technical accuracy and completeness;
- Review the ST, as appropriate, for correct application of the CC;
- Provide answers and direction to the CCTL for the conduct of the evaluation when these responsibilities are within the validator's scope of authority;
- Consult with senior validators, when necessary, to gain informal input/guidance relative to technical and/or process issues;
- Review ETR sections for accuracy and completeness; and
- Review evaluation records, as needed, to confirm accuracy or completeness of evaluation reporting

2.4.2 NIAP Representative

The lead validator also serves as the primary interface with the CCTL for the duration

of an evaluation. As such, the validator should:

- Serve as the NIAP central point of contact between NIAP and the CCTL;
- Confirm the evaluation team applies the latest applicable NIAP policies, procedures, and guidance documents;
- Ensure the evaluation team applies the latest applicable Common Criteria and CEM interpretations and precedents;
- Inform NIAP of any deviations from, or needed changes to, NIAP policies and procedures;
- Inform NIAP of issues adversely affecting evaluations or NIAP operations;
- Report evaluation-related quality issues to NIAP;
- Ensure technical inquiries are sent to the appropriate Technical Rapid Response Teams (TRRT) for review and comment;
- Address evaluation team questions regarding NIAP policy, procedures, schedules, and decisions.

2.4.3 Validation Project Coordinator

As the validation project coordinator, the lead validator should:

- Manage and/or coordinate assigned validation project activities;
- Prepare and submit validation records to NIAP to document validation activities in accordance with NIAP requirements;
- Present the results of validation activity in NIAP review meetings when requested to do so; and
- Prepare and submit a CCTL Proficiency Feedback Report after each validation.

3 NVLAP & CCTL Quality System Role in Validations

Quality system standards are essential to successful and repeatable validations. The following chapter outlines quality standards enforced by NIAP and their role in the validation process.

3.1 NVLAP and ISO Standards

NIAP policies, procedures, and concept of operations are built upon and guided by documents issued by the International Organization for Standardization (ISO) and the National Voluntary Laboratory Accreditation Program (NVLAP). These include:

- ISO/IEC 10765
- NIST Handbook 150:2016;
- NIST Handbook 150-20; and
- ISO 9000 series standards.

Annex G provides an overview of the NVLAP and ISO 9000 concepts to promote understanding of how the CCTL quality system is used by validators in performing their validation activities. This section addresses only the parts of ISO 9000 that are of primary interest to validators.

To become NVLAP accredited, CCTLs must develop, use, and maintain a quality system. The CCTL Quality System encompasses the policies, organization, responsibilities, procedures, processes, and resources that the CCTLs use to produce a product that is of consistent quality and that meets defined requirements. The CCTL Quality System describes how the CCTL intends to operate and provides the documentation of operating activities to enable verification of adherence to the quality system and to the CC, CEM and NIAP requirements.

3.2 CCTL Quality System & Validators

NIAP will use various elements of the CCTL Quality System for fulfilling its validation responsibilities under the CC, CEM and CCRA. The following paragraphs provide guidance to validators on how to use information from the CCTL Quality System.

3.2.1 Focus Areas for Validators

The CCTL Quality System provides the NIAP validator with information for determining adherence to CC, CEM and NIAP requirements. The validator typically focuses on quality system documentation that is concerned with procedures, instructions, and records (i.e., the documentation produced by the CCTL) for Common Criteria Testing. A NIAP objective is that the validator can use the products of the CCTL Quality System (i.e., reports, procedures, instructions and records) as the primary evidence for confidence building and for determining conformance to CC, CEM and NIAP requirements. The validator need only to look at the CCTL Common Criteria testing procedures, instructions, and records that are applicable for the evaluation in question. The validator may look at other parts of the CCTL‘s Quality System to aid in general understanding of the CCTL‘s Quality System approach, but should not assess the CCTL‘s Quality System itself. An assessment of the CCTL‘s Quality System is performed by NVLAP as part of the routine laboratory accreditation activities.

3.2.2 Validators and CCTL Evaluation Procedures and Instructions

Each CCTL is expected to conduct evaluations in accordance with the Common Criteria Testing procedures and CCTL instructions established in their Quality System. The validators should review the CCTL procedures and instructions to verify the evaluation approach is consistent with requirements of the CC, CEM, and NIAP, and the procedures and instructions are appropriate for the technology and product being evaluated. The procedure review enables the validator to gain technical confidence in the laboratory‘s evaluation processes.

The CCTL Quality System procedures are expected to continually evolve over time due to changes in the type, range, and volume of activities or evaluations the CCTL undertakes. The validators should allow for this anticipated evolution and should continually seek the latest procedures from the CCTL when conducting validation activities. In addition, as new and modified procedures are documented by the CCTL to address these changes, validators are allowed and expected to work with concepts, notes, or drafts of documented procedures.

3.2.3 Validators and CCTL Evaluation Records

Each CCTL is expected to maintain records of evaluation activities as defined within their Quality System. The validation procedures used by NIAP are highly dependent upon the CCTL‘s Quality System being effectively implemented with comprehensive records. All evaluation results should be entered as records into the CCTL‘s Quality System. The records should contain both the plan and results of the work performed. The plan should include the objective, required inputs, expected outputs, and techniques to be used for the activity. The recorded results are the complete written analysis or other actions performed by the CCTL to complete the work package. The record should also contain information about the findings, the persons who performed the work and the dates during which the work was performed.

In order for the validators to accomplish their tasks, they must have access to all the records related to technical activities of the evaluation. The CCTL is expected to provide these records to the validator in accordance with NIAP procedures.

4 Validators Role and CCTL Evaluation Milestones

Validators play a key role in the CCTL evaluation process. The validators provide the oversight to ensure the evaluation is technically sound and will be successfully completed. This section briefly describes the validator role for each CCTL evaluation milestone.

4.1 Procedures and Records Orientation Meeting

A *Procedures and Records Orientation* may be scheduled to allow the validator to gain an understanding of the CCTL evaluation procedures and record keeping processes to be used for the evaluation. Whether through a meeting, documentation review, or informal discussions with the evaluation team, the validator must understand the CCTL's evaluation approach, specifically focusing on the procedures and records to be used for the evaluation. The validator must obtain information about the types of records to be maintained, the storage and availability of the records, how proprietary data is to be handled and transmitted, and the timing and frequency of record generation by the evaluation team. If a Procedures and Records Orientation meeting is conducted, the validator must generate a Memorandum for the Record (MR) to document the findings and save the MR to NIAP records database.

4.2 CICO

The validator plays a large role throughout the entire CICO process. Details regarding the validator's role can be found in the CICO Guide.

4.3 Sync Sessions

Upon completion of an evaluation activity (ST, AGD, and Testing), the evaluator may initiate a Sync Session. The evaluator will submit questions and issues for discussion to the validator prior to the meeting. These sessions are driven by evaluation team question/issues. Any question regarding the next phase of testing should be included as part of that particular Sync Session. Upon completion of the meeting, the evaluation team documents the outcome of the meeting, which must be agreed and submitted by the validator to NIAP as a project record. The primary Sync Session checkpoints are:

- ST Sync;
- Guidance Sync; and
- Test Sync
    - At the discretion of NIAP, the validator may oversee testing performed by the evaluators. Depending on the PP a product claims, the subset of testing should include some of the developer tests as well as some of the independent tests. The validator should confirm the test results are consistent with those reported by the developer in the test/guidance documentation. The validator should also observe and confirm the proper installation of the TOE.

4.4 Project Check-Out/Final Package Review

After the CCTL finalizes their required evaluation documentation and delivers it to NIAP, NIAP validators perform **Project Check-Out** and review the final package. After a review of all information, the validator will complete the Validation Report (VR). The VR and

Product Compliant List (PCL) entry will concurrently be submitted to the sponsor and CCTL for accuracy and release approval. The validator will submit the final package to NIAP after the sponsor and CCTL have confirmed they approve the release of the VR and PCL Entry.

4.4.1 Evaluation Consistency Reviews (ECRs)

The primary purpose of the Evaluation Consistency Review (ECR) is to ensure the technical consistency of the evaluation and validation processes against the PP(s). Each ECR is performed by the assigned validation team. The ECR process occurs throughout the evaluation but is finalized at Check-Out. If the validation team recognizes the need for a PP update/clarification during an ECR, they initiate a Technical Rapid Response Team (TRRT) inquiry.

4.4.2 Security Target (ST)

The ST serves to define the TOE and provides the baseline against which the TOE is evaluated. The validator reviews the ST to ensure it claims exact conformance to a NIAP-approved PP. The ST is a publicly-releasable document posted to the NIAP website that does not contain any proprietary or protected information. The ST can provide the validator with the information necessary to generate the Validation Report (VR).

4.4.3 Evaluation Technical Report (ETR)

The ETR provides a comprehensive summary of the evaluation, a description of how the evaluation was conducted, and the results of the evaluation. The ETR may contain proprietary information, therefore is not releasable. In reviewing the ETR, the validator may review evaluation records to verify that the verdict given for a particular work unit is consistent with the evidence provided. In cases where the validator determines that the information in the ETR and CCTL work record are insufficient, the validator may need to review evaluation evidence to confirm the evaluation analysis and verdict. If evaluation evidence is reviewed, the validator should then describe to the CCTL the type of information that is expected to be reported in the ETR or evaluation record using the evidence to illustrate.

The ETR review should be comprehensive and the validator must ensure the information presented is complete and consistent with the analysis that was performed by the evaluation team. The validator shall review each verdict and associated rationale described by the CCTL in the ETR. The validator shall ensure enough information is provided by the CCTL in the rationale to support the verdict. Finally, if applicable, the validator must verify that any TRRT queries are appropriately described in the ETR, and ensure there are no inconsistencies between the ETR and the ST.

4.4.4 Assurance Activity Report (AAR)

An AAR, as detailed in NIAP's *Assurance Activity Reporting Guidance*, is used by validators in summarizing the assurance activities of the given evaluation. This document must not contain any protected or proprietary information as it is posted to the NIAP website.

4.4.5 Administrative Guidance Document (AGD)

The AGD gives system integrators and end users valuable information about how to install a product in its evaluated configuration. Validators must ensure that the AGD describes how to put the product in its evaluated configuration.

4.4.6 Validation Report (VR)

The VR summarizes the results of the evaluation and the validation activities performed. The VR contains information confirming that the verdict rendered by the evaluation team was complete and consistent with the evidence presented. The VR is a publicly-releasable document posted to the NIAP web site and cannot contain any proprietary or protected information. Once the VR is written, the validator should obtain CCTL and vendor release approval prior to forwarding it to NIAP for final processing.

4.4.7 Product Complaint List (PCL) Entry

One of the deliverables from the CCTL is a draft Product Complaint List (PCL) entry for the evaluated TOE. The PCL entry provides information for preparation of the Common Criteria certificate and for posting the information on the NIAP PCL. It should not contain any proprietary or protected information. The validators must review and finalize the PCL entry and receive CCTL and vendor approval prior to submitting to NIAP.

4.4.8 CC Certificate Information

The validator notifies the NIAP data/records manager that the final package is being prepared. The CCTL shall generate a draft certificate from the NIAP website and send to the vendor for review and concurrence.

4.4.9 CCTL Proficiency Feedback Report (PFR)

Upon completion of each NIAP evaluation, a CCTL PFR must be completed and submitted to NIAP documenting any non-conformities.

4.4.10 Vendor/CCTL Approval for Release of Validation Information

The VR, ST, AAR, AGD, draft certificate, and draft PCL must be reviewed by the CCTL and sponsor for accuracy and release approval prior to submitting to NIAP. See the NIAP website for an electronic copy of the latest version of NIAP Form F8002b, *Vendor/CCTL Approval for Release of Information*. The validator is responsible for coordinating with the CCTL for completion of this form.

5 NIAP Record System Requirements

To comply with the NIAP Quality System, the validator must keep records of his/her work. The purpose of the validation records is to provide a written history of what activities a validator has performed, including what guidance was provided to the evaluation team. The validator is required to document all validation activities. Any validation guidance or decision must be documented and either saved in the NIAP records database or forwarded to niap@niap-ccevs.org for inclusion in the evaluation records.

5.1 Record Identifiers

It is essential for record management purposes for the validator to maintain all files in an organized manner. Therefore, all validator records should contain the applicable unique Validation Identification (VID) number.

5.2 Records Handling

Validation records are saved in electronic form in the NIAP records database. Each file/document must be saved and titled with the VID number and the name of the document.

5.3 Records & Proprietary Information

The validator is responsible for properly identifying and protecting any proprietary or sensitive information in accordance with the *Statement of Personal Responsibility for Non-Disclosure of Proprietary Information* (Annex E*) and NIAP CCEVS Information Security Policy* (Annex F).

5.4 Close Out of Validation Records

Official validation records must be closed out and transferred to the records manager within 30 days of the validator delivery of the final package.

6 Validation Support Mechanisms

Support mechanisms available to the validator in performing the assigned duties include:

- Other NIAP technical resources;
- Interpretations and policies;
- NVLAP or NIAP remedial actions;
- Resolution process for evaluation issues; and
- NIAP communication mechanisms.

6.1 Technical Support

The senior validator and senior members of the Scheme are available to provide technical support to the lead validator as needed. The lead validator may request the senior validator‘s input prior to rendering guidance to the evaluation team. The support provided by the senior validator and/or senior members of the scheme should be as expeditious as possible. The lead validator should give the senior validator and senior members a recommended deadline for any support that is requested.

6.2 Interpretations

During the evaluation of a TOE, the evaluation-applicable CC, CEM, and NIAP policy interpretations must be correctly applied for the evaluation. The CCTL is responsible for identifying and using all applicable interpretations in an evaluation. The validator must confirm that all applicable interpretations are appropriately applied and must keep the evaluation team informed of any applicable and pending interpretation actions that may affect the evaluation. The following is an outline of procedures taken and considered when applying interpretations.

6.2.1 Interpretation Sources

Three primary sources for interpretations of CC, CEM or NIAP requirements are available to the validator. These are the international interpretations, NIAP interpretations of the CC, CEM, and PPs issued through NIAP, and NIAP policy statements.

- **International Interpretations**: CCMB interpretations of the CC or CEM are the official interpretations of the current written language of the CC or CEM used by all international users of the Common Criteria. CCMB interpretations take precedence over all other CC and CEM language, essentially replacing the text of the current documents. The CCMB list of CC and CEM international interpretations is available at the Common Criteria web site: https://www.commoncriteriaportal.org/cc/.

- **NIAP Policies:** NIAP Policies are formally documented statements of NIAP policy. NIAP Policy Statements may result from questions for clarification of NIAP documented processes, policies and procedures, or undocumented practices. Formal questions not associated with a particular evaluation should be submitted to the NIAP Director.

Other forms of documented policies are those issued by NIAP in the form of official NIAP policies or publications posted to the NIAP website.

- **NIAP Technical Decisions:** Technical Decisions (TDs) are issued to offer clarification and interpretations to Security Functional Requirements (SFRs) and Assurance Activities within NIAP-approved Protection Profiles (PPs).

6.2.2 Applying Interpretations

All final International Common Criteria Interpretations, as of the date of acceptance of the evaluation into the Scheme, are mandatory for that evaluation. Any interpretations accepted/approved after the start of an evaluation can be applied at the discretion of NIAP.

NIAP Technical Decisions are effective upon publication and must be incorporated into all current and future evaluations. Current evaluations include all evaluations except those for which a complete Check-Out package has been submitted to NIAP for final validation team review.

The validator is responsible for ensuring all applicable interpretations have been incorporated as part of an evaluation. If a validator determines an interpretation is not necessary in an evaluation, the validator will document the reasoning why and save it in the NIAP records for future reference.

6.3 NVLAP or NIAP Remedial Action

If the validator sees a pattern of deficiencies from a CCTL, the Scheme management should be notified. NIAP management will investigate and, if necessary, notify NVLAP. In coordination with the Scheme, NVLAP can investigate the source of the deficiencies and require the laboratory to submit a plan to correct the problem(s). If a laboratory fails to effectively correct a problem, NVLAP may suspend the CCTL‘s accreditation and/or the Director of the Scheme could suspend the CCTL‘s authorization to conduct evaluations under NIAP until the problem is corrected.

6.4 Resolution Process for Evaluation Issues

There are numerous points in an evaluation when technical questions are posed to the Scheme in the form of a request known as TRRT inquiries. It is the Scheme's responsibility to maintain a process to support validators in timely responses to the CCTL requests for evaluation decisions.

TRRT inquiries are the vehicle for a CCTL or vendor to obtain formal Scheme approval for a proposed solution to an evaluation technical issue. A TRRT inquiry documents the CCTL or vendor concern and provides the mechanism for the CCTL or vendor to obtain a timely decision from the TRRT on potential areas of misunderstanding. The TRRT will review the inquiry and issue a response to the evaluation team via the NIAP web tools.

An official response is issued for each inquiry submitted and applies only to the evaluation for which the inquiry was submitted.

Annex A: References

Common Criteria for Information Technology Security Evaluation, Version 3.1 Release 5, April 2017.

Part 1 Introduction and general model
Part 2 Security functional components
Part 3 Security assurance components

NIST Handbook 150:2016 Edition, *Procedures and General Requirements*

NIST Handbook 150-20, *Information Technology Security Testing—Common Criteria*

ISO/IEC 17025 (formerly ISO Guide 25)—*General Requirements for the Competence of Testing and Calibration Laboratories.*

ISO/IEC 17065:2012 —(formerly ISO Guide 65)— *Conformity Assessment – Requirements for Bodies Certifying Products, Processes, and Services*.

Annex B: Acronyms

AAR	Assurance Activity Report
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCMB	Common Criteria Maintenance Board
CCRA	Common Criteria Recognition Arrangement
CCTL	Common Criteria Testing Laboratory
ECR	Evaluation Consistency Review
CEM	Common Evaluation Methodology
ETR	Evaluation Technical Report
ISO	International Organization for Standardization
NIAP	National Information Assurance Partnership
MR	Memorandum for the Record
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Accreditation Program
PCL	Product Compliant List
PP	Protection Profile
ST	Security Target
TD	Technical Decision

TOE	Target of Evaluation
TRRT	Technical Rapid Response Team
VID	Validation Identification
VR	Validation Report

Annex C: Glossary

This glossary contains definitions of terms used in the Common Criteria Scheme. These definitions are consistent with the definitions of terms in ISO Guide 2 and are also broadly consistent with the Common Criteria and Common Methodology.

Accreditation Body: An independent organization responsible for assessing the performance of other organizations against a recognized standard, and for formally confirming the status of those that meet the standard.

Agreement Arrangement on the Mutual Recognition of Common Criteria Certificates in the field of IT Security: An agreement in which the Parties (i.e., signatories from participating nations) agree to commit themselves, with respect to IT products and Protection Profiles, to recognize the Common Criteria certificates which have been issued by any one of them in accordance with the terms of the agreement.

Appeal: The process of taking a complaint to a higher level for resolution.

Approved Test Methods List: The list of approved test methods maintained by NIAP which can be selected by a CCTL in choosing its scope of accreditation, i.e., the types of IT security evaluations that it will be authorized to conduct using NIAP-approved test methods.

Assurance Continuity Maintenance Process: A program within the Common Criteria Scheme that allows a sponsor to maintain a Common Criteria certificate by providing a means (through specific assurance maintenance requirements) to ensure that a validated TOE will continue to meet its security target as changes are made to the IT product or its environment.

Assurance Maintenance: The process of recognizing that a set of one or more changes made to a validated TOE has not adversely affected assurance in that TOE.

Assurance Maintenance Addendum: A notation, such as on the listing of evaluated products, that serves as an addendum added to the certificate for a validated TOE. The maintenance addendum lists the maintained versions of the TOE.

Assurance Maintenance Report: A publicly available report that describes all changes made to the validated TOE which have been accepted under the maintenance process.

Check-In/Check Out: The process for NIAP to provide validation oversight and to ensure the technical quality of evaluations. Sync Sessions may be conducted if the Validators deem they are appropriate for the given circumstance. Sync Sessions occur on an as needed basis. For more information, please refer to the CICO Guide.

Common Criteria (CC): Common Criteria for Information Technology Security Evaluation, the title of a set of documents describing a particular set of IT security evaluation criteria.

Common Criteria Certificate: A certificate issued by NIAP which confirms that an IT product or Protection Profile has successfully completed an evaluation by an accredited CCTL in conformance with the Common Criteria standard.

Common Criteria Evaluation and Validation Scheme (CCEVS): The program developed to establish an organizational and technical framework to evaluate the trustworthiness of IT products and protection profiles.

Common Criteria Testing Laboratory (CCTL): Within the context of the Common Criteria Evaluation and Validation Scheme, an IT security evaluation facility, accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by NIAP, to conduct Common Criteria-based evaluations.

Common Evaluation Methodology (CEM): Common Methodology for Information Technology Security Evaluation, the title of a technical document which describes a particular set of IT security evaluation methods.

Evaluation Evidence: Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.

Evaluation Technical Report: A report giving the details of the findings of an evaluation, submitted by the CCTL to NIAP as the principal basis for the validation report.

Evaluation Work Plan: A document produced by a CCTL detailing the organization, schedule, and planned activities for an IT security evaluation.

Impact Analysis Report (IAR): A report which records the analysis of the impact of changes to the validated TOE.

Interpretation: Expert technical judgment, when required, regarding the meaning or method of application of any technical aspect of the Common Criteria and/or Common Methodology.

National Information Assurance Partnership (NIAP): The partnership formed by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) which established a program to evaluate IT product conformance to international standards. Currently, NIST is responsible for the National Voluntary Laboratory Accreditation Program (NVLAP) and NSA is responsible for the National Information Assurance Partnership (NIAP).

National Institute of Standards and Technology (NIST): A federal technology agency that works with industry to develop and apply technology, measurements, and standards.

National Voluntary Laboratory Accreditation Program (NVLAP): The U.S. accreditation authority for CCTLs operating within the NIAP Common Criteria Evaluation and Validation Scheme.

Product Compliant List (PCL): A publicly available listing maintained by the NIAP Scheme of every IT product/system or Protection Profile that has been issued a Common Criteria certificate by NIAP.

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

Re-evaluation: A process of recognizing that changes made to a validated TOE require independent evaluator activities to be performed in order to establish a new assurance baseline. Re-evaluation seeks to reuse results from previous evaluations.

Security Target (ST): A specification of the security required (both functionality and assurance) in a Target of Evaluation (TOE), used as a baseline for evaluation under the Common Criteria. The security target specifies the security objectives, the threats to those objectives, and any specific security mechanisms that will be employed.

Target of Evaluation (TOE): A TOE is defined as a set of software, firmware and/or hardware, possibly accompanied by guidance, which requires evaluation and validation.

Technical Rapid Response Team (TRRT): A panel composed of Scheme validators to ensure technical consistency across evaluations and validations performed under NIAP.

Validation: The process carried out by NIAP leading to the issue of a Common Criteria certificate.

Validation Report (VR): A document issued by NIAP and posted on the VPL, which summarizes the results of an evaluation and confirms the overall results.

Annex D: Technical Rapid Response Team (TRRT)

The mission of the Technical Rapid Response Team (TRRT) Process is to provide timely response to evaluation and protection profile technical issues raised throughout the course of an evaluation.

NIAP assigns individuals to TRRTs for each technology type. Each team has a lead (or co-leads), and multiple members. The lead(s) is/are always drawn from the NIAP or validation community; other team members may be drawn from the validation community, the Technical Community (TC) responsible for the profile, and other technology experts for that technology. It is the responsibility of the lab/vendor to ensure identified issues are cleansed of any proprietary details before being transmitted to TRRT team members that are not part of the validation community (and thus not covered by non-disclosure agreements). We encourage involvement of the lab initiating the question as well as other entities (CCTLs, TCs, etc.) being part of the TRRT process.

An overview of the TRRT Process and submitting a TRRT inquiry can be found on the NIAP website.

Annex E: Statement of Personal Responsibility for Non-Disclosure of Proprietary Information

Statement of Personal Responsibility

For Non-Disclosure of Proprietary Information

Pursuant to your duties as a Validator assigned to the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS), you will be handling information which is proprietary to the specific vendor and/or Common Criteria Testing Laboratory (CCTL) accomplishing the evaluation. Access to this proprietary information by NIAP CCEVS personnel is provided with the understanding that it will be adequately protected and only disclosed to authorized personnel.

By signing this notice you are indicating that you understand and agree to the following:

I agree not to use or disclose proprietary vendor or CCTL information related to NIAP CCEVS evaluations to unauthorized parties.

I agree to protect the confidentiality of this proprietary information and avoid its disclosure and/or unauthorized use.

I agree to safeguard and protect proprietary information in accordance with the NIAP CCEVS Information Security Policy.

I agree that any proprietary markings that may have been placed on vendor or CCTL information by its originator shall be applied to any reproduction or abstract of that information.

I agree to fulfill my duties as a NIAP CCEVS Validator in a fair and impartial manner.

I agree to inform the NIAP CCEVS of any association with or interest in any company or organization that might impact (or might reasonably be perceived to impact) my ability to conduct my responsibilities as a NIAP CCEVS Validator in a fair and impartial manner. If a conflict of interest or perceived conflict of interest exists, the NIAP CCEVS reserves the right to resolve such conflict of interest in its best interest.

I acknowledge that I have read and I understand the Statement of Personal Responsibility.

Printed Name_____ Signature & Date _____

Company Name & Address

Annex F: NIAP/CCEVS Information Security Policy

Personnel assigned to and working with the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) handle information which is proprietary to specific vendors and/or Common Criteria Testing Laboratories (CCTLs). Access to this proprietary information by NIAP CCEVS personnel is provided with the understanding that it will be adequately protected and only disclosed to authorized personnel.

All NIAP CCEVS employees and contractors understand and agree to the following:

1. Not to use or disclose proprietary vendor or CCTL information related to NIAP CCEVS evaluations to unauthorized parties.
2. To protect the confidentiality of proprietary information and avoid its disclosure and/or unauthorized use during storage, handling, distribution, and analysis.
3. Employ encryption for the transmission of all electronic proprietary information.
4. Ensure that any proprietary markings that may have been placed on vendor or CCTL information by its originator shall be applied to any reproduction or abstract of that information.
5. Promptly report to NIAP any loss, damage, suspected compromises, known vulnerabilities, breach of security, or suspected unauthorized disclosure of proprietary information.
6. Follow current commercial best practices to ensure that electronic viruses are not imported into the NIAP/CCEVS/CCTL environment.
7. Follow current commercial best practices to protect data at rest.
8. Properly dispose of proprietary information that is no longer needed.

Annex G:NVLAP & CCTL Quality System Role in Validations

1 NVLAP and ISO Standards Overview

NIAP policies, procedures and concept of operations are built upon and guided by documents issued by the International Organization for Standardization (ISO) and the National Voluntary Laboratory Accreditation Program (NVLAP). These include ISO Guide 65, NIST Handbooks 150 and 150-20, and the ISO 9000 series standards. This section provides a brief overview of the NVLAP and ISO 9000 concepts to promote understanding of how the CCTL quality system is used by validators in performing their validation activities. This section also describes the validator‘s role and differentiates that role from the other roles of CCTL evaluator and NVLAP laboratory assessor. This section addresses only the parts of ISO 9000 that are of primary interest to validators.

NVLAP is designed to be compatible with domestic and foreign laboratory accreditation programs in order to ensure the universal acceptance of test data produced by NVLAP-accredited laboratories. In this regard, the NVLAP procedures are compatible with, among others, the most recent official publications of ISO/IEC 17025 (formally ISO/IEC Guide 25), ISO Guides 2, 30, 43, 45, 49, 58, and ISO standards 8402, 9001, 9002, 9003, and 9004 documents. The criterion in NIST Handbook 150 encompasses the requirements of ISO/IEC Guide 17025 and the relevant requirements of ISO 9002-1994. NVLAP Handbook 150-20 contains information that is specific to Common Criteria testing and interprets the Procedures and General Requirements of NVLAP Handbook 150, where appropriate.

To become NVLAP-accredited, CCTLs must develop, use, and maintain a quality system. The CCTL Quality System encompasses the policies, organization, responsibilities, procedures, processes, and resources that the CCTLs use to produce a product that is of consistent quality and that meets defined requirements. The CCTL Quality System describes how the CCTL intends to operate and provides the documentation of operating activities to enable verification of adherence to the quality system and to the CC, CEM and NIAP requirements. Through the use of audits and management reviews, the CCTL improves its quality system and its service to its customers.

2 Quality System Documentation Pyramid

NVLAP and associated ISO 9000 documents require that the CCTL Quality Systems be documented. The types of documentation found in quality systems include a Quality Manual and various categories/levels of procedures, instructions, records, forms, reports, etc. Figure 3-1 below shows the documentation pyramid used for describing ISO-9000 based quality systems.

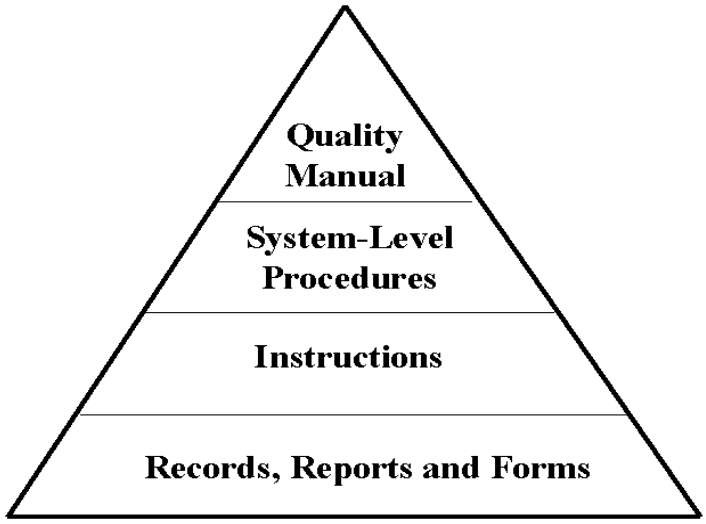

Figure 1: Quality System Documentation Pyramid

- **Quality Manual**: The Quality Manual is the top-level document that states policy, describes the overall quality system, states management commitment, defines authorities and responsibilities, outlines implementation and points to procedures.

- **System-Level Procedures**: System-Level Procedures are high-level instructions that describe how things move through the organization and how the system is implemented, including operating controls for quality processes and systems and interdepartmental (cross-functional) flows and controls (i.e., who, what, where and why). System-Level Procedures may reference other documentation such as specific instructions.

- **Instructions**: Instructions, both technical and work instructions, are intra-departmental and describe how daily jobs are done. They contain information on topics that include how to perform specific duties, prepare forms, and handle intra-departmental activities.

- **Records**: Records are the documentation of evidence of activities performed or results achieved that serve as a basis for verifying that the organization is doing what they say they intend to do. Records include forms, reports, etc.

Each level of the documentation pyramid provides the basis for building documents for the next level; that is, the Quality Manual forms the bases for describing system-level procedures, the system-level procedures define the basis for detail operating instructions, the instructions identify the records that are to be kept.

A quality system contains many different categories of procedures, instructions and records. The various procedures, instructions and records may address distinct areas of the quality system such as contracting, training, auditing, testing, etc.

3 CCTL Quality System

3.1 Overview

A quality system is defined as the organizational structure, responsibilities, procedures, processes, and resources for implementing quality management. Each CCTL must establish, use, and maintain a quality system appropriate to the type, range, and volume of activities that it undertakes. Each CCTL must conduct audits of its activities, at appropriate intervals, to verify that its quality system contains adequate and up-to-date documents, including the Quality Manual, Procedures, Instructions, Records, Reports, and Forms. Regardless of its shape or form, all elements of the quality system must be documented and available to NIAP personnel.

NIAP will use various elements of the CCTL Quality System for fulfilling its validation responsibilities under the CC, CEM and CCRA. The following paragraphs provide guidance to validators on how to use information from the CCTL Quality System. A conceptual view of a documented CCTL Quality System is provided in Figure 3-2.

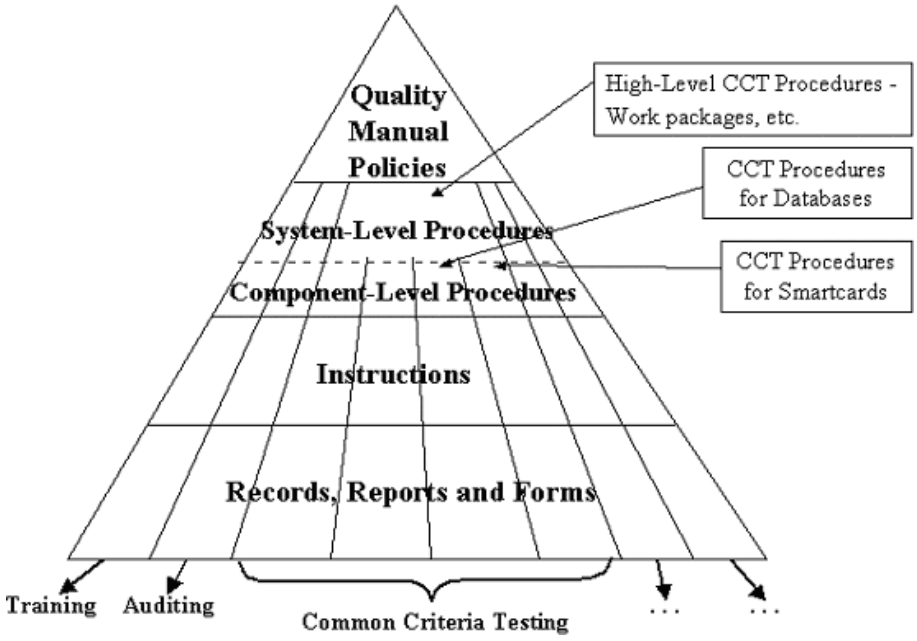

Figure 2: Conceptual View of CCTL Documented Quality System

3.2 Focus Areas for Assessors, Evaluators and Validators

The CCTL Quality System is intended to support three primary parties identified by NIAP. The quality system provides the CCTL evaluators with the organization, responsibilities, procedures, processes, and resources that the CCTL uses to produce a

product of consistent quality that meets defined requirements. It provides the NVLAP

assessors with information for assessing compliance to laboratory accreditation requirements. It also provides the NIAP validator with information for determining adherence to CC, CEM and NIAP requirements. The roles of the assessor, evaluator, or validator focusing on the CCTL Quality System differ for each in the performance of the duties of that role.

- **Assessor Focus**: Quality Manual and Different Types of Procedures, Instructions and Records.

  The NVLAP assessor typically focuses on assessing laboratory competence and on the overall scope of implementation, use and auditing of all levels of the quality system documentation pyramid. The assessor does not look at every procedure, instruction or record, but instead looks for the presence of all quality systems critical elements and evidence of use. The assessor reviews items such as quality manuals, audits, complaints, procedures, etc.

- **Evaluator Focus**: Detail Application of All Elements of the CCTL Quality System.

  The evaluator typically focuses on the customer‘s product and the details for all elements of all levels of the Quality System documentation pyramid.

- **Validator Focus**: Common Criteria Testing Procedures, Instructions and Records.

  The validator typically focuses on the three lower levels of the quality system documentation pyramid that are concerned with procedures, instructions and records (i.e., the documentation produced by the CCTL) for Common Criteria Testing. A NIAP objective is that the validator can use the products of the CCTL Quality System (i.e., reports, procedures, instructions and records) as the primary evidence for confidence building and for determining conformance to CC, CEM and NIAP requirements. The validator only needs to look at the CCTL common criteria testing procedures, instructions and records that are applicable for the evaluation in question. The validator can look at other parts of the CCTL‘s Quality System to aid in general understanding of the CCTL‘s Quality System approach, but should not assess the CCTL‘s Quality System. An assessment of the CCTL‘s Quality System is performed by NVLAP as part of the laboratory accreditation activities.

4 CCTL Evaluation Procedures and Instructions

Each CCTL is expected to conduct evaluations in accordance with the Common Criteria Testing procedures and CCTL instructions established in their Quality System. The validators should review the CCTL procedures and instructions to verify that the evaluation approach is consistent with requirements of the CC, CEM, and NIAP, and that the procedures and instructions are appropriate for the technology and product being evaluated. The procedure review enables the validator to gain technical confidence in the laboratory‘s evaluation processes.

The CCTL Quality System procedures are expected to continually evolve over time. The validators should remain aware of this anticipated evolution and should continually seek the latest procedures from the CCTL when conducting validation activities.

NVLAP accreditation of a CCTL is based on (1) the laboratory‘s demonstrated competence in performing CC evaluations, and (2) the laboratory‘s demonstrated capability to mature its Quality System through continued improvement and population of procedures, instructions and records. The number and quality of CCTL Quality System procedures and instructions are expected to increase/improve as the CCTL gains experience from conducting evaluations and as it finds more effective ways to do testing.

In addition, the CCTL Quality System procedures and instructions are expected to evolve due to changes in the type, range, and volume of activities or evaluations the CCTL undertakes. As security technologies evolve, new and modified procedures will be needed. The validator should allow for this type of evolution and should expect to work with concepts, notes, or drafts of documented procedures and instructions as they are being documented by the CCTL.

5 CCTL Evaluation Records

Each CCTL is expected to keep records of evaluation activities as defined within their quality system. The validation procedures used by NIAP are highly dependent upon the CCTL‘s Quality System being effectively implemented with comprehensive records.

A CCTL is expected to create a work plan as part of each evaluation. A specification list of CEM work packages that are to be performed during the evaluation should be included in the work plan. As these work packages are completed, the results should be entered as records into the CCTL‘s Quality System. The records for each work package should contain both the plan and results of the work performed. The plan should include the objective, required inputs, expected outputs, and techniques that will be used for the activity. These may be drawn from other sources within the quality system such as written CCTL procedures or the CEM.

The recorded results are the complete written analysis or other actions performed by the CCTL to complete the work package. The record should also contain information about the findings, the persons who performed the work and the dates during which the work was performed.

The above paragraphs specify the types of information that the Scheme expects to be contained within those records so that validators can perform their role as required by NIAP.