



Common Criteria Evaluation and Validation Scheme

Publication #3

Guidance to Validators

8 September 2008
Version 2.0

Foreword

The Common Criteria Evaluation and Validation Scheme (CCEVS) was established to ensure the ready availability of independently evaluated and validated IT products that meet the security needs of the United States Government.

Audrey M. Dale
Director, CCEVS

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

National Security Agency
Common Criteria Evaluation and Validation Scheme
9800 Savage Road, Suite 6757
Fort George G. Meade, MD 20755-6757
E-mail: scheme-comments@missi.ncsc.mil
<http://www.niap-ccevs.org/cc-scheme>

Amendment record

Version	Date	Description
Draft 1.0	20 March 2001	Initial release.
2.0	8 September 2008	Complete revision based on current operations

(This page intentionally left blank)

Table of Contents

1	Introduction	1
1.1	Purpose.....	1
1.2	Scope.....	1
2	Validation Process and Validator Responsibilities.....	2
2.1	Validation Goal	2
2.2	Validation Activities	3
2.3	Validation Process Overview.....	3
2.4	Validator Responsibilities	3
2.4.1	Validate Evaluation Results.....	4
2.4.2	CCEVS Representative.....	4
2.4.3	Validation Project Coordinator.....	5
2.4.4	CCTL Support.....	5
3	NVLAP & CCTL Quality System Role in Validations	6
3.1	NVLAP and ISO Standards	6
3.2	CCTL Quality System & Validators.....	6
3.2.1	Focus Areas for Validators	6
3.2.2	Validators and CCTL Evaluation Procedures and Instructions	7
3.2.3	Validators and CCTL Evaluation Records	7
4	Validators Role and CCTL Evaluation Milestones	8
4.1	Read-ahead Submission (Mandatory).....	8
4.2	Initial VOR (IVOR) (Mandatory).....	8
4.3	Evaluation Acceptance and Kick-off Meeting (Mandatory).....	8
4.4	Procedures and Records Orientation Meeting (Optional).....	9
4.5	Test VOR (TVOR) (Mandatory).....	9
4.6	Testing Oversight (Optional)	9
4.7	Final VOR (FVOR) (Mandatory)	9
4.8	Evaluation Conclusion (Mandatory).....	10
4.8.1.	Security Target (ST) and Proprietary ETR.....	10
4.8.2	Validation Report (VR).....	10
4.8.3	Validated Products List Entry	10
4.8.4	CC Certificate Information	10
4.8.5	Vendor/CCTL Approval for Release of Validation Information.....	11
5	Policy Interpretations and Evaluation Documents.....	11
5.1	CC, CEM and CCEVS Policy Interpretations	11
5.2	Evaluation Technical Report.....	11
6	CCEVS Record System Requirements	12
6.1	Record Identifiers and Indexing.....	12
6.2	Records Handling.....	12
6.3	Records & Proprietary Information	13

6.4	Close Out of Validation Records	13
7	Validation Support Mechanisms	13
7.1	Technical Support	13
7.2	Interpretations	14
7.2.1	Interpretation Sources	14
7.2.2	Applying Interpretations	15
7.3	NVLAP or CCEVS Remedial Action	15
7.4	Resolution Process for Evaluation Issues	15
Annex A: References.....		17
Annex B: Acronyms.....		18
Annex C: Glossary		20
Annex D: Observation Reports.....		23
Annex E: Validator Records.....		27
Annex F: Statement of Personal Responsibility for Non-Disclosure of Proprietary Information.....		29
Annex G: NIAP CCEVS Information Security Policy		30
Annex H: Technical Oversight Panel (TOP).....		31
Annex I: NVLAP & CCTL Quality System Role in Validations.....		33

1 Introduction

The Common Criteria Evaluation and Validation Scheme (CCEVS) for Information Technology Security was established by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) to validate conformance of Information Technology (IT) products and Protection Profiles (PP) to international standards. The CCEVS oversees the evaluations performed by Common Criteria Testing Labs (CCTLs) on information technology products and PP's against the Common Criteria for Information Technology Security Evaluation (CC).

The principal participants in the CCEVS program are the:

- **Sponsor:** The Sponsor may be a product developer, a Protection Profile developer, a value-added reseller of an IT security-enabled product, or another party that wishes to have a product or PP evaluated. The sponsor requests that a Common Criteria Testing Laboratory (CCTL) conduct a security evaluation of an IT product or PP.
- **Common Criteria Testing Laboratory (CCTL):** The CCTL is a commercial testing laboratory accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS to perform security evaluations against the Common Criteria for Information Technology Security Evaluation (CC) using the Common Methodology for Information Technology Security Evaluation (CEM).
- **Common Criteria Evaluation and Validation Scheme (CCEVS):** The CCEVS is the government organization established 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 the CCEVS and that the conclusions of the CCTL are consistent with the evidence presented and are 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 or PP under evaluation.

1.2 Scope

This document is one of a series of technical and administrative CCEVS publications that describes how the scheme operates. It consists of seven chapters and several supporting annexes. Chapter 1 provides a high level overview of the CCEVS. Chapter 2 provides details on the validation process, including validator responsibilities. Chapter 3 provides information related to the validators 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 CCEVS record system requirements and Chapter 7 details the various validator support mechanisms available.

The supporting annexes cover a variety of topics to include an acronym list, a glossary, a list of references, detailed NVLAP and CCTL quality system information, the process for handling Observation Reports, list of validator records, a sample Statement of Personal Responsibility for Non-Disclosure of Proprietary Information, and the Technical Oversight Panel (TOP) process.

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

[Publication #1](#), *Common Criteria Evaluation and Validation Scheme -- Organization, Management, and Concept of Operations*

[Publication #2](#), *Common Criteria Evaluation and Validation Scheme – Quality Manual and Standard Operating Procedures*

[Publication #4](#), *Common Criteria Evaluation and Validation Scheme -- Guidance to Common Criteria Testing Laboratories*

[Publication #5](#), *Common Criteria Evaluation and Validation Scheme -- Guidance to Sponsors*

[Publication #6](#), *Common Criteria Evaluation and Validation Scheme – Assurance Continuity: Guidance for Maintenance and Re-evaluation*

CCEVS related publications and information are available through the CCEVS web site at <http://www.niap-ccevs.org/cc-scheme/index.cfm> .

2 Validation Process and Validator Responsibilities

2.1 Validation Goal

The primary goal of validation is for CCEVS to ensure the technical quality, correctness, and consistency of each evaluation in accordance with the CC, CEM, and all CCEVS guidance

2.2 Validation Activities

Validation activities are used to determine that the results of the evaluation analysis are technically correct and consistent with the CC and the CEM. Validators are responsible for reviewing the CCTL evaluation results, not for performing the evaluation. Validators focus on reviewing the ST or PP and the CCTL ETR in assessing the CCTL's application of the CC and the CEM. In determining a complete, correct and consistent evaluation of a TOE or PP, the validator performs the following additional activities:

- (a) Reviewing CCTL evaluation procedures,
- (b) Interacting and holding discussions with evaluation teams,
- (c) Monitoring CCTL evaluation meetings,
- (d) Observing CCTL testing activities,
- (e) Reviewing evaluation evidence in response to CCTL-generated questions, comments, or records.

The validation activities performed depends on the assurance level and the technology being evaluated.

2.3 Validation Process Overview

Validation Oversight Reviews (VORs) are the primary validation activity used to assess whether evaluations conform to the standards required by the CCEVS. The VOR process and associated validation activities are designed to confirm that the CCTL has performed the evaluation correctly. The VOR process is described in detail in [Validation and Oversight Review \(VOR\): Evaluators and Validators Guide](#).

The VOR process is designed to provide oversight at specific milestones during each evaluation. Evaluations must successfully complete all validation activity associated with each milestone prior to proceeding to the next. The milestones identified by CCEVS include an Initial VOR (IVOR), Kick-off, Test VOR (TVOR), Final VOR (FVOR) and Evaluation Conclusion/VPL Listing.

Although the VOR process is utilized for all evaluations, certain evaluations require additional oversight. CCEVS will utilize Technical Oversight Panels (TOPs) for higher assurance evaluations (EAL6 and EAL7), candidate laboratory evaluations, CCTL reaccreditations, or when CCEVS determines additional validator oversight is necessary. TOPs are similar to VORs but have a greater number of validators for additional oversight. For candidate laboratory evaluations, the TOP process is outlined in *NIST Handbook 150-20:2005, Annex A*. For CCTL reaccreditations, the TOP process is outlined in *NIST Handbook 150-20:2005, Annex B (revised 2008-01-07)*. [Annex H](#) of this document also describes the TOP process.

2.4 Validator Responsibilities

Validators must understand their responsibilities within the CCEVS. The primary responsibility assigned to a validator is to determine that the evaluation was thorough, technically sound, and conducted in accordance with CCEVS guidance. Further, the validator's role is to promote quality in CCTL evaluations and the validation activities should not hinder the CCTLs ability to conduct the evaluation. 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 that evaluation. The senior validator participates in the evaluation as an advisor to the lead validator. Other responsibilities of the validator include serving as a CCEVS representative, a validation project coordinator, and/or providing CCTL support.

2.4.1 Validate Evaluation Results

Validation of the CCTL's evaluation efforts will take place during Initial, Test and Final VORs. The validator will perform the following quality management activities in validating evaluation results:

- Verify that planned evaluation activities, methodologies and procedures are feasible and appropriate;
- Verify that the Common Criteria and the Common Evaluation Methodology are consistently and correctly applied in evaluations;
- Review documented evaluation results, verdicts and rationales for technical accuracy and completeness;
- Review the ST or PP, 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;
- Comment on observation reports (ORs) submitted by the CCTL and assist senior validators in understanding the issues associated with the OR;
- Review ORs submitted to the CCEVS to ensure that observations, problem descriptions, proposed resolutions, decisions, or interpretations are correctly and sufficiently described;
- Review ETR sections for accuracy and completeness; and
- Review evaluation records, as needed, to confirm accuracy or completeness of evaluation reporting.

2.4.2 CCEVS Representative

The validator serves as the primary CCEVS representative interfacing with the CCTL for the duration of an evaluation. As a CCEVS representative, the validator should:

- Serve as CCEVS central point of contact between the CCEVS and the CCTL;
- Confirm that the evaluation team is aware of the latest applicable CCEVS policies, procedures, and guidance documents;

- Ensure that the evaluation team is aware of the latest applicable Common Criteria and CEM interpretations and precedents;
- Maintain awareness of and apply the latest CCEVS policies and procedures;
- Inform scheme management of any deviations from, or needed changes to, CCEVS policies and procedures;
- Inform scheme management of issues adversely affecting evaluations or CCEVS operations;
- Report evaluation-related quality issues to scheme management;
- Forward ORs to the senior validator;
- Forward ODs to the evaluation team;
- Forward evaluation team questions to CCEVS regarding CCEVS policy, procedures, schedules, and decisions;
- Coordinate with the records manager to notify the evaluation team and CCTL management when the scheme has approved the final VPL entry, thereby indicating that validation of the CCTL evaluation activities is complete.

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 CCEVS to document validation activities in accordance with CCEVS requirements and formats; and
- Present the results of validation activity in CCEVS review meetings when requested to do so.

2.4.4 CCTL Support

The validator should support the CCTL to both facilitate the evaluation and to enhance the capabilities of the CCTL. This support may be in the form of technical advice to the CCTL in areas such as information technology and evaluation methodologies. In performing this role, the validator must always maintain a fair and open environment for communication with the CCTLs. To provide such advice, the validator must have sufficient technical understanding of the objectives of the evaluation and hence may need to have access to evidence produced by the sponsor and the evaluator. The validator is responsible for protecting such information appropriately.¹

As CCTL technical support, the validator should:

- Meet, teleconference, or otherwise communicate with the evaluation team as needed;

¹ Access to this information may be accomplished by possessing the actual documentation, although it could be granted in other ways (e.g., at the evaluation facility, on-line, etc.).

- Confirm the evaluation team is aware of applicable evaluation techniques, practices, test methods, processes and procedures available to all CCTLs;
- Suggest, where appropriate, the type of information that should be included in ETRs and records to enable efficient and effective validation of evaluation results;

3 NVLAP & CCTL Quality System Role in Validations

3.1 NVLAP and ISO Standards

The CCEVS 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 Guide 65](#), [NIST Handbook 150:2005](#), [NIST Handbook 150-20](#), and the ISO 9000 series standards. [Annex I](#) 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 CCEVS requirements.

3.2 CCTL Quality System & Validators

The CCEVS 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 CCEVS validator with information for determining adherence to CC, CEM and CCEVS 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 CCEVS 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 CCEVS 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 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. An assessment of the CCTL's Quality System is performed by NVLAP as part of the 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 that the evaluation approach is consistent with requirements of the CC, CEM, and CCEVS, 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 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 keep records of evaluation activities as defined within their quality system. The validation procedures used by the CCEVS 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 that will 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 that 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 the [Validation Oversight Review \(VOR\) Evaluators and Validators Guide](#).

4 Validators Role and CCTL Evaluation Milestones

Validators play a key role in the CCTL evaluation process. The validators provide the analysis that determines whether or not the CCTL can proceed to the next milestone (Initial VOR (IVOR), Kick-off, Test VOR (TVOR), Testing, Final VOR (FVOR) and Evaluation Conclusion/VPL Listing). This section briefly describes the validator role for each CCTL evaluation milestone. Comprehensive details regarding the validator role for each VOR is described in [Validation Oversight Review \(VOR\) Evaluators and Validators Guide](#).

4.1 Read-ahead Submission (Mandatory)

Prior to each VOR the CCTL submits a read-ahead package to the validator. This package includes all completed work units and documentation applicable to that particular VOR. This documentation serves as the primary input into the CCTLs evaluation efforts.

4.2 Initial VOR (IVOR) (Mandatory)

The validator reviews the IVOR Read-ahead package, generates an MR for discussion points and submits it to the CCTL prior to the IVOR, participates in the IVOR, and generates a VOR report. A passing verdict is required to proceed to Evaluation Acceptance and Kick-off.

4.3 Evaluation Acceptance and Kick-off Meeting (Mandatory)

Within 8 business days of a successful Initial VOR, the lead validator should schedule an Evaluation Acceptance Kick-off Meeting. The kick-off meeting provides an opportunity for all parties involved in the evaluation and validation to meet and agree on expectations. The purpose of the evaluation acceptance Kick-off meeting is to introduce the CCTL, scheme and sponsor representatives, and to achieve an understanding among the participants of each organization's roles, expectations, and plans for the evaluation. Technical details of the product or the evaluation criteria to be used should not be the primary focus of the meeting.

The lead validator will conduct the kick-off meeting. The Sponsor representative, CCTL representative, CCEVS management, and others as appropriate, should also participate in the meeting. The validator should coordinate the date of the meeting with both the evaluation team and CCEVS management. If CCEVS management is unavailable for the meeting, the senior validator may be required to serve as the CCEVS management representative. The kick-off meeting should follow the Evaluation Acceptance Kick-off Meeting Agenda (T6006) listed on the NIAP CCEVS website <http://www.niap-ccevs.org/cc-scheme/forms/>

Once the kick-off meeting has occurred and all parties are in agreement, the evaluation will be officially accepted by the scheme and the evaluation may proceed.² The validator must generate Kick-off meeting minutes and submit them to CCEVS within 5 days.

4.4 Procedures and Records Orientation Meeting (Optional)

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 that will 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 within 5 days.

4.5 Test VOR (TVOR) (Mandatory)

The validator reviews the TVOR read-ahead package, generates an MR for discussion points and submits it to the CCTL prior to the TVOR, participates in the TVOR, and generates a VOR report. A passing verdict is required for the CCTL to proceed to Testing and subsequent Final VOR.

4.6 Testing Oversight (Optional)

At the discretion of CCEVS, the validator may oversee testing performed by the evaluators. The subset of testing should include some of the developer tests as well as some of the independent tests. The validator should confirm that the test results are consistent with those reported by the developer in the test documentation.. The validator should also observe and confirm the proper installation of the TOE.

4.7 Final VOR (FVOR) (Mandatory)

The validator reviews the FVOR Read-ahead package, generates an MR for discussion points and submits to the CCTL prior to the FVOR, participates in the FVOR, and generates a VOR report. A passing verdict is required to complete the evaluation.

² If a CCTL begins an evaluation before obtaining official acceptance by the CCEVS, then some evaluation process steps may need to be re-started in order for the Validator(s) to perform his functions.

4.8 Evaluation Conclusion (Mandatory)

After a successful FVOR and after the CCTL finalizes their required evaluation documentation, the validator prepares a final package containing the Security Target (ST), proprietary Evaluation Technical Report (ETR), Validation Report (VR), Validated Products Listing (VPL) entry, certificate, and completed F8002 *Sponsor/CCTL Approval for Release of Information*.

4.8.1. Security Target (ST) and Proprietary ETR

The ST serves to define the TOE and as the baseline against which the TOE is evaluated. The ETR describes how the evaluation was conducted and documents the results of the evaluation. The ST is a publicly releasable document posted to the NIAP CCEVS web site that cannot contain any proprietary or protected information. The ETR is not releasable. Both documents provide the validator with the information necessary to generate the VR.

4.8.2 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 CCEVS 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 the CCEVS for final processing. The format for the *Validation Report* is available at the CCEVS web site <http://www.niap-ccevs.org/cc-scheme/forms/>.

4.8.3 Validated Products List Entry

One of the deliverables from the CCTL is a draft Validated Products List (VPL) entry for the evaluated TOE. The VPL entry provides information for preparation of the Common Criteria certificate and for posting the information on the NIAP CCEVS VPL. It should not contain any proprietary or protected information and it will require a release approval by the CCTL and sponsor. The format for the VPL entry can be found at the CCEVS web site <http://www.niap-ccevs.org/cc-scheme/forms/>. Note that PP validations do not require a VPL summary entry. The validators must review and finalize the VPL entry and receive CCTL and vendor approval prior to submitting to CCEVS

4.8.4 CC Certificate Information

The validator notifies the CCEVS data/records manager that the final package is being prepared. The CCEVS records manager will compose a draft CC certificate and provide it to the validator. The validator shall review the draft certificate and send it to the CCTL for review and concurrence. The CCTL shall have the vendor complete the Certificate

Award Worksheet (F8003) detailing how they would like to receive their certificate. This form is available on the CCEVS web site <http://www.niap-ccevs.org/cc-scheme/forms/>

4.8.5 Vendor/CCTL Approval for Release of Validation Information

The VR, ST or PP, draft certificate, and draft VPL entry will concurrently be submitted to the CCTL and sponsor for accuracy review and release approval prior to submitting to CCEVS. See the CCEVS web site <http://www.niap-ccevs.org/cc-scheme/forms/> for an electronic copy of the latest version of [CCEVS Form F8002](#), *Sponsor/CCTL Approval for Release of Information*. The validator is responsible for coordinating with the CCTL for preparation, signing, and completion of this form.

5 Policy Interpretations and Evaluation Documents

5.1 CC, CEM and CCEVS Policy Interpretations

In the evaluation of a TOE or PP, the evaluation-applicable CC, CEM, and CCEVS policy interpretations must be correctly applied for the evaluation. The CCTL is responsible for identifying and using all applicable interpretations in an evaluation. [Section 7.2.2](#), Applying Interpretations, provides guidance on what interpretations should be applied. The validators 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 effect the evaluation.

5.2 Evaluation Technical Report

The evaluation technical report (ETR) is expected to provide a comprehensive summary of the TOE or PP evaluation, a description of how the evaluation was conducted, and the results of the evaluation. 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 that 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 that enough information is

provided by the CCTL in the rationale to support the verdict. Finally, if applicable, the validator must verify that any Observation Decisions are appropriately described in the ETR, and ensure that there are no inconsistencies between the ETR and the ST or PP.

6 CCEVS Record System Requirements

To comply with the CCEVS 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 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 forwarded to Crecords@missi.ncsc.mil for inclusion in the evaluation folder.

6.1 Record Identifiers and Indexing

It is essential for record management purposes that the validator maintain all files in an organized manner. Therefore, all validator records should contain a unique record identifier.

The record identifier should be located at the top right hand portion of the page and should be present on each page of the document. This identifier has the following format: VIDxxxxx-[unique one-up numbering (four digits)-[activity category acronym]. The VIDxxxxx is the project Validation Identification (VID) number. The first value, noted as “xxxxx”, is a unique number assigned by CCEVS data/records manager at the start of the validation. The second value is a four-digit one-up number, and the last required value identifies the activity category (e.g., MR). If an activity requires one or more revisions of the original record, then a “n” character will be added to the one-up numbering to uniquely identify “versions” of the record. For example, if document A had been updated over the course of an evaluation, the initial version of the plan would have been a record ID of VIDxxxx -nnnn-MR. Each revision of the document A would have been annotated with an alpha character added to the end of the record ID (i.e., VIDxxxx—nnnn.1-MR). See reference [Annex E](#) for a listing of required validator records.

6.2 Records Handling

Validation records should be recorded in electronic form whenever possible and sent to the mail list Crecords@missi.ncsc.mil. Electronic validation records should include in the subject line the record identifier (if it is a single record) or the Validation ID number (if it is for multiple records), and short title of the product name. Each attachment should be saved and titled with the record identifier as the name of the document. For example:

- 1) For a single record:
To: CRECORDS@missi.ncsc.mil
Subj: VIDxxxxx-nnnn-MR, Product A

2) For multiple records:
To: CRECORDS@missi.ncsc.mil
Subj: VIDxxxxx, Date, Product A

If applicable, hardcopy files should be organized, properly labeled with record identifiers and sent to:

NIAP/CCEVS
National Information Assurance Partnership
9800 Savage Road
Suite 6757
Ft. Meade, Maryland 20755-6757

6.3 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 F](#)) and *NIAP CCEVS Information Security Policy* ([Annex G](#)).

6.4 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.

7 Validation Support Mechanisms

Support mechanisms available to the validator in performing the assigned duties include other CCEVS technical resources, interpretations and policies, NVLAP or CCEVS remedial actions, the resolution process for evaluation issues, and CCEVS communication mechanisms.

7.1 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.

7.2 Interpretations

7.2.1 Interpretation Sources

Three primary sources for interpretations of CC, CEM or CCEVS requirements are available to the validator. These are the international interpretations of the CC and CEM issued by the Common Criteria Maintenance Board (CCMB), the NIAP interpretations of the CC and CEM issued through the CCEVS, and CCEVS 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 NIAP CCEVS web site <http://www.niap-ccevs.org/cc-scheme/interpretations/index.html>.
- **CCEVS Interpretations:** CCEVS administers a public National Interpretation Board (NIB) for issuing CCEVS interpretations to offer clarifications to the CC/CEM in the form of proposed changes to the CC/CEM. The board receives CC and CEM issues needing clarification or formal interpretation from the scheme, validator, Observation Decision Review Board (ODRB) or the general public. The NIB drafts interpretations and facilitates public discussion of draft interpretations to ensure that diverse views are considered. Once all views are considered and incorporated as appropriate, the proposed interpretations are submitted to the CCEVS Director for approval. Upon CCEVS management approval, evaluations are to consider the proposed changes contained within the interpretations as the recommended way to understand the requirements. They will have the same status within evaluations as do precedents, in that they will provide an informed opinion describing what the requirements mean and an acceptable use. Because all changes to the words are treated as refinements for which rationales must be provided, the rationale for the word changes resulting from the use of a CCEVS interpretation will simply cite the interpretation.

CCEVS may forward management-approved interpretations to the CCMB for consideration as it strives to produce regular updates to the Criteria and Methodology. Non-concurrence from the CCMB will signal the need for rescission of the interpretation by CCEVS management. Any rescission of NIAP interpretations will be announced in the same manner as approved interpretations; on the CCEVS mailing lists and website. The list of CCEVS CC and CEM national interpretations is available at the CCEVS web site <http://www.niap-ccevs.org/cc-scheme/PUBLIC/>. The details of the NIB operating procedures are described on the CCEVS web site at <http://www.niap-ccevs.org/cc-scheme/PUBLIC/thenib.html>.

The naming/notation system that has been used in the past will be optional when CCEVS interpretation words are used within an evaluation. For cases when the notation convention is not used, there should be a clear note at the point of the use of

the interpretation indicating the interpretation applied to a particular component. This can be a footnote, a tailoring or operation note, or some other informative note.

- **CCEVS Policies:** CCEVS Policies are formally documented statements of CCEVS policy. CCEVS Policy Statements may result from questions for clarification of CCEVS documented processes, policies and procedures, or undocumented practices. Formal questions not associated with a particular evaluation should be submitted in the form of a letter to the CCEVS Director. The CCEVS will answer these questions by return letter.

For CCTL clarification questions associated with a particular evaluation, the questions should be submitted in the form of a CCEVS observation report (OR). Policy statements resulting from an OR will be issued in the form of a CCEVS observation decision (OD) for that evaluation. Note that, like all ODs, such a policy statement is applicable only to the specific evaluation being addressed.

Other forms of documented policies are those issued by the CCEVS in the form of official CCEVS policies or formally issued page changes to CCEVS publications.

7.2.2 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 the CCTL and Sponsor. The validator is responsible for ensuring that all applicable interpretations have been incorporated as part of an evaluation.

7.3 NVLAP or CCEVS Remedial Action

If the validator sees a pattern of deficiencies from a CCTL, the scheme management should be notified. CCEVS 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. If a laboratory fails to effectively correct the problem, NVLAP may suspend the CCTL's accreditation and the Director of the scheme could suspend the CCTL's authorization to conduct evaluations under the CCEVS until the problem is corrected.

7.4 Resolution Process for Evaluation Issues

There are numerous points in an evaluation when technical or process questions are posed to the scheme in the form of a request known as an Observation Report (OR). It is the validator's responsibility to represent the scheme and respond in a timely manner to these requests. It is the scheme's responsibility to maintain a process to support validators in timely responses to the CCTL requests for evaluation decisions.

Issues fall into two broad categories: (1) those in which the validator and the evaluation team/sponsor/developer agree and (2) those in which the validator and evaluator team/sponsor/developer do not agree and therefore, require a decision to be rendered by CCEVS management..

Observation Reports (ORs) are the vehicle for a CCTL to obtain formal scheme approval for a proposed solution to an evaluation technical or process issue. An OR documents the CCTL concern and provides the mechanism for the CCTL to obtain a timely decision from the scheme on potential areas of misunderstanding. The validator is responsible for aiding the CCTL in preparing the OR and for delivering the OR to the scheme for consideration. The scheme will review the OR and issue a response, called the Observation Decision (OD), back to the evaluation team via the validator. An OD is issued for each OR submitted and applies only to the evaluation for which the OR was submitted. The OR/OD Process is described in detail in [Annex D](#).

Annex A: References

The Report of the [President's Commission on Critical Infrastructure Protection](#) (PCCIP), *Critical Foundations: Protecting America's Infrastructures*, October, 1997.

The White House, The Clinton Administration's Policy on Critical Infrastructure Protection: [Presidential Decision Directive 63, May 1998](#).

CEMEB (Common Evaluation Methodology Editorial Board), [Common Methodology](#) for Information Technology Security Evaluation, Version 3.1, September 2007.

CCMB (Common Criteria Maintenance Board), [Common Criteria](#) for Information Technology Security Evaluation, Version 3.1, September 2007.

Part 1 Introduction and general model

Part 2 Security functional components

Part 3 Security assurance components

[NIST Handbook 150:2005](#) 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 Calibration and Testing Laboratories, 2005

[ISO/IEC Guide 65](#) — General Requirements for Bodies Operating Product Certification Systems, 1996

Annex B: Acronyms

CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCMB	Common Criteria Maintenance Board
CEM	Common Evaluation Methodology
CCRA	Common Criteria Recognition Arrangement
CCTL	Common Criteria Testing Laboratory
EAL	Evaluation Assurance Level
EAP	Evaluation Acceptance Package
ETR	Evaluation Technical Report
FVOR	Final Validation Oversight Review
ISO	International Organization for Standardization
IVOR	Initial Validation Oversight Review
NIAP	National Information Assurance Partnership
MR	Memorandum for Record
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Accreditation Program
OD	Observation Decision
OR	Observation Report
ODRB	Observation Decision Review Board
PP	Protection Profile

ST	Security Target
TOE	Target of Evaluation
TTAP	Trust Technology Assessment Program
TOP	Technical Oversight Panel
TVOR	Test Validation Oversight Review
VID	Validation Identification
VOR	Validation Oversight Review
VPL	Validated Products List
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 the CCEVS which can be selected by a CCTL in choosing its scope of accreditation, that is, the types of IT security evaluations that it will be authorized to conduct using CCEVS-approved test methods.

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.

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

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

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 the CCEVS which confirms that an IT product or protection profile has successfully completed 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 the CCEVS 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 the CCEVS 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.

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

National Information Assurance Partnership (NIAP): The partnership that included 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 Common Criteria Evaluation and Validation Scheme (CCEVS).

Observation Decision (OD): The formal documented response from the CCEVS that provides clarification/guidance to the CCTL on a submitted Observation Report.

Observation Reports (OR): A report issued to the CCEVS by a CCTL or sponsor identifying specific problems or issues related to the conduct of an IT security evaluation.

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 a previous evaluation.

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.

Technical Oversight Panel: A panel composed of scheme validators to ensure technical consistency across evaluations and validations performed under CCEVS.

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

Validation Oversight Review: The process for CCEVS to provide validation oversight and to ensure the technical quality of evaluations.

Initial VOR: To ensure that the ST is accurate and clearly specified, meets CCEVS Policies 1, 9, 10, 13, their respective addendums, and the evaluation team correctly performed the Assurance Security Target Evaluation (ASE) analysis

Test VOR: The Test VOR shall be conducted after the TOE passes all the work units except those dependent on team testing. Examples of these exceptions include some (not all) of the guidance documents, testing and vulnerability analysis work units.

Final VOR: The focus of the Final VOR is to ensure all issues have been resolved and to discuss the evaluation team's testing activities.

Validated Products List (VPL): A publicly available listing maintained by the CCEVS Scheme of every IT product/system or protection profile that has been issued a Common Criteria certificate by the CCEVS.

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

Annex D: Observation Reports

1 Observation Reports

An Observation Report (OR) enables the CCTL to obtain approval of a proposed solution to, or scheme direction for, an observed Common Criteria or Common Evaluation Methodology technical evaluation issue or scheme process issue (i.e., CCTL question, concern or problem). See the CCEVS web site <http://www.niap-ccevs.org/cc-scheme/forms> for the OR/OD format and content. The CCTL documents the evaluation or process issue in the OR, provides background information and, where possible, offers a proposed solution. The scheme uses the OR to review the issue and develop clarification/guidance to the CCTL. The scheme uses an Observation Decision (OD) to formally respond to an OR. An OD is issued for each OR. The scheme's OR resolution process should be accomplished within eight (8) working days of the CCEVS receipt of a complete and unambiguous OR.

The OR/OD format and process described herein specifically addresses CCTL observation issues submitted to the scheme; that is, decisions not made by the validator. For decisions made by the validator, any reasonable documentation means may be used, provided that all validator decisions are documented and visible to both the CCTL and the scheme.

The CCTL uses its own procedures for observation reporting (and response) for CCTL to sponsor communications. Any validator observation issues to the sponsor should be addressed through the CCTL.

1.1 Submission of Observation Reports

Observation Reports (ORs) are submitted by CCTLs to document a question on a specific evaluation to receive a quick turn-around resolution from the scheme. The validator may also use the OR mechanism for documenting a question about a specific evaluation for which they need formal resolution from the scheme even if the CCTL does not agree with the need to submit an OR.

Validators may submit an OR to document:

- a disagreement between a validation team and an evaluation team; or
- a noteworthy decision by a validation team in which a formal documented resolution from the scheme is desired.

The CCTLs may submit an OR when the underlying PP, the CC, CEM, or CCEVS policy is incomplete, unclear, inconsistent, or erroneous and existing CCEVS guidance is inadequate and either the:

- Validator is unable or unwilling to provide the decision or
- The CCTL desires a decision from the Scheme.

An OR can be initiated by the evaluation team or by the validation team. Regardless of who initiates an OR, both parties must:

- agree upon the statement of the issue as written in the OR;
- be given the opportunity to provide a resolution to the issue in the OR;
- be given the opportunity to review the other party's proposed resolution; and
- be given the opportunity to provide factors that should be considered by the Scheme when making the resolution.

Additionally, the evaluation team must review the OR for proper marking of proprietary information.

A CCTL must submit ORs to the lead validator assigned to the evaluation for which the OR was generated. An OR should contain, at a minimum, the following:

1. Date of submission,
2. Current projected evaluation completion date,
3. Identity of the CCTL submitting the OR,
4. CCTL point of contact for the issue including contact information (e-mail and phone),
5. CCTL specific tracking ID (optional),
6. Identity of the lead validator for the evaluation including contact information (e-mail and phone),
7. Evaluation for which the OR is being submitted,
8. Evaluation target (which PP ST/TOE),
9. Issue for which a resolution is requested,
10. State whether it is a CCEVS process issue or a technical evaluation issue,
11. Proposed resolution to the issue and impact (may include various resolutions and respective impacts),
12. Background explanation of the issue and of the proposed resolution, and
13. Identification of information sources (i.e., references) used in preparing the OR.

Any information in the OR that is not publicly releasable must be explicitly marked by the CCTL. Each paragraph in the OR that contains proprietary information must be preceded by the notation “(PROP)” or “(P)”.

1.2 Handling of Observation Reports

Upon receiving the OR, the validator will:

1. Verify that the OR submitted meets the format requirements,

2. Add comments/reaction to the opinions expressed by the CCTL to the background section, including whether the validator concurs with the OR and any known precedents, prior guidance, ODs or interpretations on the issue,
3. Submit the OR with validator comments to the CRECORDS@missi.ncsc.mil mail list within three (3) business days. The CCEVS, in turn, will acknowledge receipt, assign a tracking number (i.e., CCEVS-OR-xxxx), and notify the validator of the expected response date. The validator will notify the CCTL that the OR was received and forwarded.

The validator must explicitly mark (as noted in the previous section) any proprietary information used in validator additions to the OR that is not publicly releasable.

The senior validator will forward issues that are primarily scheme processes-related to the CCEVS management for resolution.

1.3 Observation Decisions

An Observation Decision (OD) is issued in response to an OR. The OD is the formal documented response from the scheme that provides clarification/guidance to the CCTL on a submitted OR. Once an OD is rendered, the validator is responsible for forwarding the completed OD to CRECORDS@missi.ncsc.mil and to the CCTL. OR/ODs will use the tracking number assigned by the records manager as the record ID, i.e., CCEVS-OR/OD-xxx.

1.4 Application of Observation Decisions

The OD serves to provide the CCTL with confidence that the currently understood resolution will be honored for the evaluation in question when the final validation of evaluation results is conducted. The OD is applicable only for the issue identified in the OR and only for that evaluation. To this end, the OD represents scheme direction and policy provided. The CCTL is expected to apply the OD if:

1. The associated OR fully disclosed all relevant information that was known or should have been known to the CCTL; and
2. The evaluation has not exceeded its scheduled completion date by more than six months from the expected completion date indicated in the OR.

ODs provide the best answer available at the time, giving timely, good-faith guidance to CCTLs on a given evaluation. An OD is for a specific evaluation and is issued in a short time frame to accommodate the CCTL evaluation schedule. This short time frame for the OD may not provide adequate time to develop confidence that the decision is correct and widely applicable. Therefore, the OD is applicable only to an OR for one evaluation and does not apply to future evaluations even if the same issue should arise. Thus, until

longer-term CCEVS guidance becomes available, the CCTL is expected to resubmit an OR for each evaluation to which the issue applies.

1.5 Observation Decision History Section

The History section of an Observation Decision is recorded for CCEVS informational and reference purposes. The information in the OD History section is considered CCEVS-proprietary and should not be distributed to CCTLs, sponsors, or any other person outside of the validation community.

1.6 Appeal and Resolution of Observation Decision

The OD is the formal documented response from the scheme providing clarification/guidance to the CCTL on a submitted OR. If the CCTL and/or sponsor disagree with an OD and wish to formally appeal it, the scheme will reconsider the OD. To formally appeal the issued OD and request reconsideration, the CCTL and/or sponsor shall:

1. Identify the OD and associated OR being appealed;
2. Identify each item of the OD that the CCTL is appealing;
3. Explain and justify why they disagree with the OD item;
4. Identify specific supporting references (document identification, section & paragraph) for all justifications where applicable;
5. Propose acceptable resolutions, revisions or alternatives to the OD;
6. Attach the original OR and corresponding OD; and
7. Submit the appeal documentation package to the CCEVS management.

Upon receipt of the request for OD reconsideration, the CCEVS Director will acknowledge receipt of the appeal/reconsideration request within 5 business days. The CCEVS director then reviews the request, consults with the involved parties about any clarifications as necessary, consults with other scheme resources as needed, and prepares a resolution for the appealed OD. The resolution may be to uphold the original OD or issue a revised OD. The decision is incorporated into the OD if it represents a change to the previous decision, and the CCTL, senior validator, and the lead validator are notified as to the decision reached.

The OD appeal and resolution process ends when the CCEVS director issues the response to the appeal. The resulting OD is used by the CCTL for the evaluation in question. The scheme will attempt to issue the appeal response within 15 working days from receipt of the OD request for reconsideration.

Annex E: Validator Records

1. VORs

1. Validator comments on read ahead package, titled VIDxxxxx-nnnn-(I,T or F)VOR-valcomments

2. IVOR report containing IVOR verdict, titled VIDxxxxx-nnnn-IVOR-results

If the validation team is required to review updates to the ST or any supporting documentation after the VOR, this is documented and titled VIDxxxxx-nnnn.1-IVOR

2. KICK-OFF (KO) MEETING

1. M/R – kick off meeting minutes, or CCEVS email if traditional KO meeting was waived and done electronically, titled VIDxxxxx-nnnn-KOmtg

2. Form F8001 – Sponsor’s Approval to List Product “in Evaluation”, VIDxxxxx-nnnn-ATL

3. FOLLOW-UP VORs

M/R, titled VIDxxxxx-nnnn-FVOR-followup

If a VOR (initial, test, final) results in a failure and a follow-up VOR is required, the CCEVS documentation will be named, VIDxxxxx-nnnn-(I,T,F)VOR-followup

4. FINAL PACKAGE

1. Final Security Target, VIDxxxxxnnnn-ST-final

2. Final Validated Products List, VIDxxxxx-nnnn-VPL-final

3. Final Validation Report, VIDxxxxx-nnnn-VR-final

4. Final Evaluation Technical Report (proprietary version), VIDxxxxx-nnnn-ETR-final

5. M/R – senior validator concurrence with Final Package, VIDxxxxx-nnnn-srvalapproved

6. CCEVS F8002 – CCLT/Sponsor Release of Information, VIDxxxxx-nnnn-ROI

7. CCEVS F8003 – Certificate Worksheet, VIDxxxxx-nnnn-CW

8. Final CC Certificate, VIDxxxxx-nnnn-Cert-final

5. OBSERVATION REPORT/OBSERVATION DECISION (OR/OD)

1. Observation Report (OR), CCEVS-OR-nnnn (number issued by CCEVS)
2. Observation Decision (OD), CCEVS-OD-nnnn (same number used as OR)
3. Vendor/Lab Appeal (if applicable), CCEVS-OD-nnnn-appeal
4. CCEVS Appeal Decision, CCEVS-OD-nnnn-appealdecision

6. ANY OTHER VALIDATOR DECISION

1. VIDxxxxx-nnnn-MR-description

Annex F: 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 G: 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 CCEVS 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 H: Technical Oversight Panel (TOP)

The purpose of the Technical Oversight Panel (TOP) is to ensure consistency across higher assurance evaluations (EAL6 and EAL7), candidate laboratory evaluations, CCTL reaccreditations, or when CCEVS determines additional validator oversight is necessary. TOPs will be similar to VORs but will have a greater number of validators for additional oversight.

1 Technical Oversight Panel Make-up

The TOPs will normally consist of approximately five validators, including one or two senior members of the validation community and the assigned lead validator for the evaluation. A TOP chairperson, who is responsible for coordinating TOP activities and for producing the written results, will be designated by CCEVS management when the TOP is assigned.

2 TOP Preparation

The TOP members will be provided with the latest draft of the ST and ETR, and will be granted access to the evaluation evidence and evaluation records for the project at least one week prior to the scheduled TOP. The TOP members will hold a 1-2 day TOP Preparation Meeting prior to the TOP meeting for planning purposes. The TOP chairman should make every attempt to provide the evaluation team with the issues that need to be discussed at the TOP meeting as far in advance as possible. During the TOP Preparation Meeting, as issues that will require discussion at the TOP meeting arise, they should be forwarded to the Evaluation Team Leader. At the conclusion of the TOP Preparation Meeting, the TOP will develop an agenda (including the specific areas they would like to discuss) for the TOP meeting and will provide it to the evaluation team at least one day prior to the TOP meeting.

The evidence to be reviewed by the TOP members will be determined based on the focus of the TOP. The review of records and evidence is essential in order for the TOP to provide meaningful feedback to the evaluation team.

3 TOP and Evaluation Team Interaction

The meeting between the TOP and evaluation team will involve an informal, round table discussion between the TOP members and the evaluation team. The goals of the meeting are to:

1. determine whether the evaluation team has the appropriate level of understanding of the TOE;
2. determine that the evaluation team has correctly applied the CEM to the developer's evidence;
3. confirm that the evaluation team has reached the appropriate conclusions;

4. provide the evaluation team the opportunity to solicit feedback on upcoming evaluation activities; and
5. educate evaluators and less-experienced validators as to what is expected in determining if a TOE satisfies the requirements.

The CCTL will provide a presentation of TOE, TOE evidence and CCTL findings. This meeting should take no more than half a day. The expectation is that the evaluation team will be prepared to discuss how they applied the work units to the evidence, and to articulate why they feel they have reached the proper conclusions.

The TOP is expected to discuss any issues (e.g., insufficient rationale in the ETR, disagreement in the verdict) discovered during their preparation and any issues (e.g., the team doesn't fully understand what is required by a work unit, the team's approach to performing a work unit is insufficient) that develop during the meeting. The meeting will also afford the evaluation team the opportunity to ask the TOP any questions they have regarding CC requirements, CEM work units, the approach they are considering in performing upcoming work units, or evaluation issues in general. The CCTL is encouraged to invite CCTL members in addition to the evaluation team to aid the CCTL in training their evaluators.

4 Feedback from TOP

The TOP chairperson will ensure that the TOP panel documents the results of the TOP meeting, including any recommendations (such as Observation Reports which may be written by the TOP, areas that need further analysis by the evaluation team, etc.) and delivers the results to CCEVS within two business days of the TOP. The TOP members are expected to discuss their results with the evaluation team upon completion of the TOP. This oral feedback should not be considered binding, but will provide the evaluators with the opportunity to ask questions about any of the issues that will be documented. The format for the TOP's written recommendation can be found on the NIAP CCEVS web site <http://www.niap-ccevs.org/cc-scheme/forms/>. The recommendation may include technical issues that need to be addressed by the evaluation team and CCEVS process issues that need to be addressed by the CCEVS staff. If appropriate, the recommendation should include guidance to the validator about follow-up activities. Upon receipt of the TOP's recommendation, the CCEVS will review and finalize the recommendation into a TOP decision which will be provided to the TOP, the evaluation team, and a copy maintained in the records for the validation. TOP decisions are considered binding and the evaluation team is expected to follow through with any guidance provided in the decision.

Annex I: NVLAP & CCTL Quality System Role in Validations

1 NVLAP and ISO Standards Overview

The CCEVS 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 validators 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 CCEVS 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 intradepartmental and describe how daily jobs are done. They contain information on topics that include how to perform specific duties, prepare forms, and handle intradepartmental 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 CCEVS personnel.

The CCEVS 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.

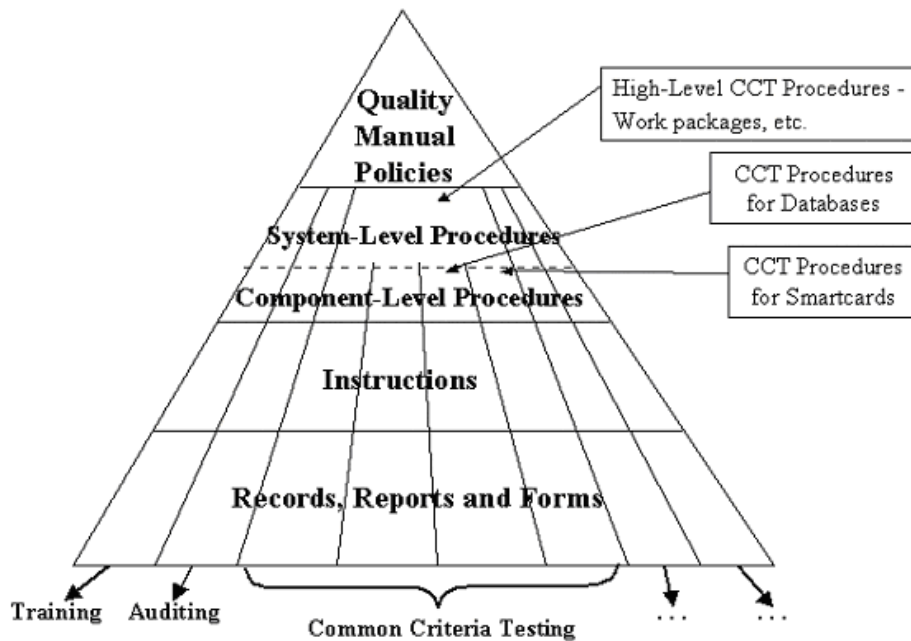


Figure 2: Conceptual View of CCTL Documented Quality System

3.2 Focus Areas for Assessors, Evaluators and Validators

The CCTL Quality System is intended to support three primary parties identified by the CCEVS. 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 CCEVS validator with information for determining adherence to CC, CEM and CCEVS 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 CCEVS 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 CCEVS 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 CCEVS, 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 the CCEVS 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 that 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 the CCEVS.