VALIDATION OVERSIGHT REVIEW (VOR) EVALUATORS AND VALIDATORS GUIDE

Version 2.0
18 March 2008

TABLE OF CONTENTS

Introduction

The primary goal of the Validation Oversight Review (VOR) is for CCEVS to ensure the technical quality and consistency of the evaluation, to confirm that the CCTL correctly applied all CCEVS policies, and to verify the CCTL accomplished all required tasks (including analysis, testing, auditing, etc).

General Guidelines for all VORs

- VORs are intended to promote valuable interaction between evaluators and validators to ensure that validator expectations have been satisfied. This interaction should also demonstrate the evaluator's understanding and successful analysis of the product.

- VORs shall be conducted in the spirit of mutual cooperation and trust, with evaluation and validation personnel treating each other with respect and courtesy at all times.

- All CCEVS evaluations will have an initial VOR (IVOR), a test VOR (TVOR), and a final VOR (FVOR). Details on the requirements for each of these VORs are outlined in this document.

- Milestones for CCEVS evaluations include read-ahead submissions, IVOR, Kick-off, In-Evaluation Listing, TVOR, Testing, FVOR and Evaluation Conclusion/VPL Listing.

- A VOR panel will typically consist of two CCEVS validators to include a lead validator assigned to the project/evaluation and a senior validator assigned to that specific VOR. The lead validator is the technical point of contact and fully participates in all VORs related to that evaluation. Due to resource constraints, CCEVS management cannot guarantee that the same senior validator will participate in all VORs for a specific product.

- For complex products, additional validator personnel may be assigned to the VOR.

- In order to make the most productive use of the limited time allotted for VORs, it is critical that both the evaluators and validators be fully prepared for their VORs.
    - VORs will be based upon the read-ahead material received by CCEVS by the required deadline. Validators may work with the CCTL to accommodate updates to that material but are not obligated to do so. The CCTL assumes the risk of potential VOR failure if the material provided was insufficient or incorrect.
    - The addition or removal of components from the TOE, and/or the addition or removal of significant requirements, after the initial read ahead package is submitted may constitute grounds for a VOR failure.
    - The limited VOR slots will only be scheduled for CCTLs and products that have submitted complete packages.
    - Validators shall review the material provided by the CCTLs in advance of the VOR in order to gain the necessary working knowledge of the product. The validators shall then develop specific questions for the evaluators and submit them to the CCTL prior to the VOR.

- At the conclusion of the VOR, the VOR Report will be written and jointly agreed upon by the evaluation and validation personnel. The report shall contain a pass, conditional pass or fail verdict as determined by the CCEVS Senior Validator.

1 Initial VOR

The Initial VOR shall ensure that the ST is accurate and clearly specified, meets all relevant CCEVS policies and their respective addendums, and that the evaluation team correctly performed the Assurance Security Target Evaluation (ASE) analysis. Failure to successfully satisfy these requirements could result in an Initial VOR failure.

1.1 Evaluator Actions Prior to Initial VOR

The evaluators shall provide the ST and the corresponding ASE ETR sections, any available user/admin guidance, and the evaluation team presentation materials/slides three weeks in advance of VOR week. The ASE ETR must *demonstrably* pass all the work units (i.e., the ETR shall justify all the pass verdicts.) The exception to this will be those work units judged to be inconclusive that can only pass via the formal evaluation of the TOE.

- Evaluators shall be prepared to answer any questions from the validators pertaining to the ST and ASE ETR.
    - At least one of the evaluators shall be able to answer a given validator question.
    - It is acceptable for the evaluators to reference documentation during the VOR.
    - Validators may allow evaluators to respond back via email.

- Evaluators shall understand and be able to explain the TOE as described in the ST.

1.2 Initial VOR Presentation

The evaluators shall prepare the following materials for formal presentation. The material presented shall go well beyond a mere restating of the ST and shall adequately explain how the ST meets all the required CCEVS policies.

- Description of physical and logical boundaries of the TOE:
    - Diagram that depicts all the components of the IT environment that are required to operate the TOE. The TOE components and IT environment components shall be clearly and consistently identified.
    - Description and comparison of the marketed product to the defined TOE (Evaluated Configuration).
        - Include advertised security related capabilities of the product.
        - Description of the TOE boundary, including a sound rationale for the boundary plausibility.
    - Description of any security dependencies that the TOE may have on the environment (IT or otherwise).

- Description of the TSF boundary and a characterization of the TSFI.

- Description of the models/configurations and any distinguishing features

- Description of all interactions among the components of the TOE and IT Environment. Include the following when describing the data flow, as applicable: protocols, integrity, disclosure protection, end point authentication and replay protection. It is important to consider these factors whether the components are distributed or reside on the same machine.

- Description of how each of the SFRs is implemented in the TOE:
    - The description shall focus on, at a minimum; the functioning of the TOE mechanisms used to achieve the SFR.
    - It is not sufficient to simply enumerate the SFRs or provide a mapping of security functions and SFRs; rather, the evaluators must be able to describe the architecture and operation of the TOE in sufficient detail as to rationally justify its security.

- Description and a justification of the inclusion of any explicit SFRs.

- Description of the cryptographic functionality and related requirements.

- Description of the various types of users, and the various aspects for each Security Functional Policy (SFP).

- Description of any changes made to the product, in terms of security features and/or design, as a result of the ASE work.

- Description and justification of how CCEVS Policies 10 and 13 are met.

1.3 Validator Actions Prior to Initial VOR

The validators shall gain a thorough understanding of the TOE's security specification by performing the following actions prior to attending the VOR.

- Thoroughly review the ST:
    - Ensure that a clear physical boundary is drawn. The physical boundary shall define the components that are within the TOE and components outside of the TOE.
    - Ensure that the descriptions of the models/configurations adequately describe the distinguishing features, and that the requirements apply to all models/configurations.
    - Ensure that a clear logical boundary is described. The logical boundary shall define the services/functions that are provided by the TOE and the services that the TOE uses from the IT environment that impact the TSF.
    - Ensure that the SFRs are well specified and correspond to documented TOE functionality, for example:
        - Review TOE description, SFR and TSS for consistency. The TSS shall clearly state how the security functions described in the TSS satisfy the SFRs.
        - Ensure that the distinction among TSF data, user data and security attributes is consistently applied in SFRs, operations on SFRs, the TOE Description and TSS.
        - Ensure that all user roles are defined based on differing security-relevant capabilities and that the SFRs reflect this distinction. Also

ensure that the SFRs capture both the data protection and identification and authorization rules.
        - Ensure the SFRs are described at the appropriate level of detail. Review PD 0133: Level of Detail in SFRs. This provides guidance regarding the level and depth of detail required of the SFRs within an ST.
        - Ensure any cryptographic functionality is specified in accordance with CCEVS policy.
        - Ensure the description of the user identity types as well as various aspects of any SFPs specified in the ST are adequate.
        - Ensure the TSS is plausible and describes how the SFRs are met.

- Review other product documentation (e.g. user guide, admin guide, and marketing literature) to ensure it is consistent with the TOE functionality described in the ST.
    - Determine if the product publicly advertises security-related functionality that is not included in the TOE.
    - Determine if any security related functionality typical of the product type, is excluded from the TOE yet available in the product.

- Review the description of the TSF boundary and characterization of the TSFI and determine if it is consistent with specification contained in the ST.

1.4 Validator Actions after the Initial VOR

See Section 4.1: Validator Actions to Complete a VOR.

2 Test VOR

The Test VOR shall review those activities performed in ADV and ATE. Since the proper identification of the TSF and TSFI are critical to the testing effort, the Test VOR shall address these areas along with the test planning.

The Test VOR shall be scheduled after the ST passes all the required work units (except those dependent on testing activities) and the evaluators have thoroughly reviewed the developer test plan and created the evaluation team test plan.

2.1 Evaluator Actions Prior to Test VOR

- Evaluators shall provide the following materials to CCEVS three weeks prior to VOR week:
    - Documentation describing the resolution to issues resulting from the Initial VOR.
    - Updated ST (with track changes turned on to indicate all changes made to the ST since the Initial VOR).
    - Updated ETR (proprietary) with all work units passing except those requiring a site visit.
    - The evaluation team test plan including:
        - Test configurations/models, along with justification of any configurations/models not fully tested.
        - Testing schedule
        - Developer tests that will be executed by the team, along with a justification of the subset chosen.

        - Functional and penetration test methodology
        - Team test cases (functional and penetration tests), including:
            - Test setup
            - Test step description sufficiently detailed to assess the value and efficiency of the tests
            - Expected test results.
    - All developer test documentation.
    - Developer vulnerability analysis (Version 2.3).
    - Product Functional Spec, Design Docs, and Test Coverage Analysis
    - Evaluation team's records for the activities performed.
    - Evaluation team presentation slides/materials.

- Evaluators shall be prepared to present and allow the examination of all evaluation records.
    - At least one of the evaluators shall be able to answer any given validator question.
    - It is acceptable for the evaluators to reference documentation during the VOR.

2.2 Test VOR Presentation

The evaluators shall prepare and present the following material to the validators:

- Any changes to the ST since the IVOR.

- Description of the architecture at the subsystem level
    - Identification of the data and control flows.
    - Overview of the TSF and its relationship to the TOE
    - Overview of the TSFI and a justification that the functional specification is complete and accurate

- Developer Test Description.
    - Test configurations/models covered in developer's test activity.
    - Developer's test coverage analysis and how the shortcomings were considered in independent testing.

- Team Test Description.
    - Test configuration, listing the IT environment components used and their configuration.
    - Test configurations/models covered in team test activity.
    - Summary of team independent tests.
    - Summary of vulnerability analysis.

- Any other key evaluation findings since the IVOR.

- Identification of any changes to the product, made during the course of the evaluation, in terms of security features and/or design as a result of the evaluation.

2.3 Validator Actions Prior to Test VOR

- Review the ST and ensure that the changes since the Initial VOR are acceptable.

- Review a sample of the functional specification.

    - Review descriptions of TSFI represented in different functional areas (e.g., network, administrative, GUI) and ensure the TSFI are fully described (i.e., parameters, errors, exceptions, and operations are completely described) commensurate with the defined EAL level.

- Review a sample of the design documentation.

- Review the developer's test plan and ensure the developer test configuration is consistent with and representative of the ST.

- Review a sample of the developer's test coverage analysis and ensure each sampled TSFI is adequately tested in terms of parameters, errors, exceptions, and operations.

- Review the team test documents
    - Ensure the evaluation team test configuration is consistent with and representative of the ST.
    - Determine the adequacy of the team's test cases.
        - Examine the purpose of the test case
        - Examine the TSFI that the test stimulates
        - Review the test steps and expected results to determine that the TSFI is exercised to achieve the purpose of the test case.

- Review the vulnerability analysis and team test plan to ensure that:
    - The vulnerability analysis is reasonable in terms of sources searched, the product was fully covered by the search and that the search included similar products.
    - The evaluation team has devised penetration tests to prove or disprove developer claims and to exploit potential vulnerabilities hypothesized by the team.

- Compare the ETR sections to the validator concerns/findings to identify any inconsistencies.

2.4 Validator Actions after the Test VOR

See Section 4.1: Validator Actions to Complete a VOR.

3 Final VOR

The Final VOR shall focus on reviewing and discussing the evaluation team's testing and ensuring all previously identified issues have been resolved.

3.1 Evaluator Actions Prior to Final VOR

- Evaluators shall provide the following materials to CCEVS three weeks in advance of VOR week:
    - Final ST (with track changes turned on to indicate all changes made to the ST since the Test VOR)
    - Final Proprietary ETR and draft Validator Report (VR).
    - Documentation describing the resolution of all action items from prior VORs.
    - Team test results.

    - Evaluation team presentation materials/slides.
    - All final developer evidence.

- Evaluators shall be prepared to answer any questions from the validators pertaining to the evaluation.
    - At least one of the evaluators shall be able to answer a given validator question.
    - It is acceptable for the evaluators to reference documentation during the VOR.

3.2 Final VOR Presentation

The primary focus shall be on the test results, the final ETR, and addressing relevant questions and comments. The evaluators shall prepare the following material for formal presentation.

- Description of any changes to the ST since the previous VOR.

- Description of significant events which occurred during testing.
    - Description of any configuration issues that arose.
    - Description of any failures encountered and what the CCTL did in response.
    - Description and explanation of any deviations from the test plan.

- Identification of changes made to the product, during the course of the evaluation, in terms of security features and/or design as a result of the evaluation.

- Justification that the product defined by the ST is accurately reflected in the ETR and that the ETR accurately reflects the evaluation results.

- Description and explanation of any requirements that have not been addressed since the TVOR.

3.3 Validator Actions Prior to Final VOR

- Review the Final ST.
    - Confirm that the changes made to the ST since the previous VORs were addressed and documented.
    - Compare the ST and user documents to ensure that all security related features in the product are addressed in the ST and draft Validation Report, (specifically with respect to their coverage by the evaluation effort).

- Review the developer and team test results
    - Confirm that the test configuration used during testing matched the test configuration in the test plan.
    - Confirm that the actual tests run were those listed in the test plan.
    - Confirm that the tests generated the expected results.
    - Confirm that the CCTL executed the test suite correctly.

- Review the final ETR to ensure that it adequately describes the evaluation activities.

- Review the draft validation report.

3.4 Validator Actions after the Final VOR

See Section 4.1: Validator Actions to Complete a VOR.

4 VOR Report

All VORs shall conclude with a draft VOR Report containing a list of agreed upon issues and actions written by a designated individual during the course of the VOR.

4.1 Validator Actions to Complete a VOR

- The senior validator, with input from the lead validator, shall determine the VOR verdict at the conclusion of the VOR. In rare cases, the senior validator may need to consult CCEVS management for discussion or coordination prior to rendering a final verdict. Possible VOR verdicts are described below in section 4.2.

- The VOR Report shall include milestone deadlines for all actions including delivery of all required items such as an updated ST and/or other design evidence.

- The lead validator is responsible for ensuring the VOR results are documented in the VOR Report and are coordinated and agreed upon by the evaluation and validation teams. The final VOR report shall be sent to CCEVS (crecords) and the evaluation team within five business days.

4.2 VOR Verdicts

- **Pass:** The evaluation is able to proceed with no action required before the next milestone.
    - Minor issues may exist requiring resolution prior to future milestones (but not the next milestone). These resolutions shall be supplied to the validator as required by the VOR Report. For instance, minor issues could have been identified during the IVOR which need to be resolved before the TVOR or the FVOR but which will not need to be corrected prior to the Kick-off and therefore, would not preclude the Kick-off from being conducted. It is, therefore, necessary for validators to clearly distinguish between issues that need resolution before the next milestone from those that need resolution prior to subsequent milestones. If the identified issues are not resolved as required by the VOR Report, this will constitute a VOR failure.

- **Conditional Pass:** The evaluation is not able to proceed to the next milestone until identified minor issues are resolved.
    - Minor issues exist that must be resolved before the next milestone but which do not merit an additional formal VOR. These resolutions shall be supplied to the validator as required by the VOR Report. If the issues are not resolved as required by the VOR report, this will constitute a VOR failure.

- **Fail:** The evaluation has significant issues that prevent it from proceeding.

- Significant or major issues were identified that prevent the evaluation from proceeding. These issues must be addressed as required by the VOR Report and another VOR must be scheduled.

An evaluation is only permitted a single failure for any one type of VOR and only a total of two overall VOR failures. A third VOR failure will require CCEVS intervention and potential termination of the evaluation.

4.3 Critical Focus Areas for VORs

The following list represents critical areas that must be considered for each evaluation.

- **Initial VOR:**
  - The ST/TOE Description and boundary are clearly represented. It must be clearly discernable what functionality and interfaces are inside and outside of the TOE.
  - All CCEVS policies are applied.
  - SFRs are sufficiently detailed to enable adequate testing (clear, consistent and measurable),

- **Test VOR**:
  - All TSFI are correctly and completely identified.
  - Adequate understanding of the functions, interfaces and design of the product is demonstrated.
  - It is clearly demonstrated that the vendor has run the test suite successfully. The ATE_FUN work units are all pass, and the evidence supports this.
  - Planned test procedures are complete and test what they claim to test.
  - The sampling method chosen from the vendor test suite demonstrates that the full range of TSFI is included.
  - When applicable, a suitable equivalency argument for the platforms being tested adequately represents all the platforms to be listed on the VPL.
  - All action items from the IVOR have been addressed appropriately.

- **Final VOR:**
  - An adequate understanding of all the functions, interfaces, and design of the product is demonstrated.
  - The functional testing and the test results support the CCTL conclusions.
  - The vulnerability analysis evidence supports the work unit conclusion.
  - The guidance documents adequately detail the steps necessary to put the TOE in the evaluated configuration.
  - The ETR contains complete, PASS verdicts.
  - The ETR justification supports the claimed verdicts.
  - All actions from previous VORs have been addressed appropriately.

4.4 VOR Report Template

Record ID: VIDXXXXX-XXXX-VOR

VOR Report

VID#:XXXXX

Product Name:
EAL:
CCTL:
Date of VOR:
Type of VOR: [Initial, Test, or Final**]**
VOR Result: [Pass, Conditional Pass, Fail]
*[Note: a result of **Pass** is issued if the evaluation is able to proceed with no action required before the next milestone. **Conditional Pass** is rendered if the evaluation is not able to proceed to the next milestone until identified issues are resolved, but a follow-up VOR is not required. A VOR verdict of **Fail** is given if the evaluation has significant issues that prevent it from proceeding.]*
VOR members and contact info:
Names, email addresses, phone number

Evaluation Team Participants:

I. Introduction

[*For Initial VORs include the following or similar wording]* The purpose of this Validation Oversight Review (VOR) was to ensure compliance with CCEVS policies 10 and 13 and to ensure [*CCTL*'s] correct performance of the ASE evaluation activities against the [*product name]* Security Target (ST).

[*For Test VORs include the following or similar wording]* The purpose of this Validation Oversight Review (VOR) was to:

- Ensure that the test plans/procedures describe appropriate tests for the functions of the TOE as defined in the ST;
- Ensure that the test material was sufficiently detailed for the VOR panel to understand the tests to be performed; and
- Allow the evaluation team to justify the efficacy of the tests.

[*For Final VORs include the following or similar wording*] The purpose of this Validation Oversight Review (VOR) was to:

- Ensure that the ETR adequately describes the evaluation activities; and
- Ensure that the product is clearly defined by the ST.

II. Documentation Reviewed

The VOR reviewed the following documentation:

[List all materials reviewed, including the evaluation team's presentation]

III. Review Results

[This section presents what the VOR discovered during the course of their review of the read-ahead package, the evaluation team's presentation, and the discussion that took place between the VOR members and the evaluation team. This section must note that the VOR did not perform a complete review/evaluation of the ST, ETR, or vendor evidence; that the evaluation team is expected to consider all comments in the context of how they impact the ST, ETR, and the remaining analysis to be performed on the project; and that the VOR has also not repeated comments when an issue appears multiple times.]

[*If the result was Conditional Pass, describe what needs to happen here. For example, "The evaluation team is expected to address all comments at the next VOR." Or, "The evaluation team is expected to address all comments and provide evidence of correction to the VOR member or validator within XX weeks/prior to a specified milestone."]*

General observations and comments are included in Section IV. The evaluation team must address the issues listed in Sections V and VI. Irresolvable issues are listed in Section VII. Requirements for proceeding with the evaluation are provided in Section VIII.

IV. General Observations

[This section highlights overall observations, such as issues with the quality system (NVLAP related), evaluation methodology, documentation, test plans, etc.]

V. Specific Issues to be Addressed

[Intro paragraph gives direction on how/when the issues must be addressed. The issues are presented as a numbered list, with a unique number for each issue for tracking purposes.]

VI. Observation Report(s) Required

[This section documents any required ORs as a result of the VOR. The OR is not presented here, but rather a summary of the issue, with guidance to the evaluation team about how to proceed with the OR.]

VII. Issues for CCEVS Management

[This section documents issues that were not brought to closure between the VOR members and the evaluation team. The issues documented here are not suitable for ORs but require a CCEVS decision in order for the evaluation to proceed. For example, these may be issues where the VOR members believe there is a problem, and the evaluation team does not agree.]

VIII. Requirements for Proceeding

[This section clearly articulates the required actions for the evaluation to proceed and for the VOR to conclude.]

[*For Initial VORs, include the following sections]*

A. The following issues must be addressed before the kick-off meeting can be held:
[*If none, do not include this section (A)*.]
1.
2.

B. The following issues must be addressed before the testing VOR can be held:
[*If none, do not include this section (B)*.]
1.
2.

C. The following issues must be addressed before the final VOR can be held:
[*If none, do not include this section (C)*.]
1.
2.

[*For Testing VORs, include the following sections]*

A. The following issues must be addressed before testing can be conducted:
1.
2.

B. The following issues must be addressed before the final VOR can be held:
[*If none, do not include this section (B)*.]
1.
2.

[*For Final VORs, include the following section]*
A. The following issues must be addressed before the evaluation is deemed complete:

5 Acronyms and Abbreviations used in this Document

ADV	Assurance development
ASE	Assurance Security-Target Evaluation
ATE	Assurance Tests
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Library
EAL	Evaluated Assurance Level
ETR	Evaluation Technical Report
FSP	Functional Specification
FVOR	Final VOR
IT	Information Technology
IVOR	Initial VOR
NVLAP	National Voluntary Laboratory Accreditation Program
OR	Observation Report
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
TSFI	TOE Security Function Interface
TSS	TOE Summary Specification
TVOR	Test VOR
VOR	Validation Oversight Review
VR	Validation Report