



**VALIDATION OVERSIGHT PROCESS: EVALUATORS AND VALIDATORS GUIDE**  
Version 1.1, October 26, 2006

## TABLE OF CONTENTS

<b>1</b>	<b>General Rules</b> .....	<b>3</b>
<b>2</b>	<b>Initial VORs - EALs 2 though 4</b> .....	<b>3</b>
2.1	Evaluator Action Prior to Initial VOR .....	4
2.2	Initial VOR Briefing .....	4
2.3	Validator Action Prior to Initial VOR .....	5
<b>3</b>	<b>Final VOR – EAL 2</b> .....	<b>5</b>
3.1	Evaluator Action Prior to Final EAL 2 VOR .....	5
3.2	Final VOR Briefing – EAL 2.....	6
3.3	Validator Action Prior to Final VOR – EAL 2 .....	7
<b>4</b>	<b>Final VOR – EAL 3</b> .....	<b>8</b>
4.1	Evaluator Action Prior to Final VOR – EAL 3 .....	8
4.2	Final VOR Briefing – EAL 3.....	8
4.3	Validator Action Prior to Final VOR – EAL 3 .....	9
<b>5</b>	<b>Test VOR – EAL 4</b> .....	<b>10</b>
5.1	Evaluator Action Prior to Test VOR – EAL 4 .....	10
5.2	Test VOR Briefing – EAL 4.....	11
5.3	Validator Action Prior to Test VOR – EAL 4 .....	12
<b>6</b>	<b>Final VOR – EAL 4</b> .....	<b>13</b>
6.1	Evaluator Action Prior to Final VOR – EAL 4 .....	13
6.2	Final VOR Briefing – EAL 4.....	13
6.3	Validator Action Prior to Final VOR – EAL 4 .....	14

## 1 General Rules

- Validation Oversight Reviews (VORs) were designed to replace traditional NIAP CCEVS oversight by focusing validator efforts on the most critical aspects of the evaluations at EALs 2-4.
- EAL 2-4 evaluations will receive initial and final VORs while EAL 4 evaluations will also receive test VORs. Details on the requirements for each of these VORs are outlined in this document.
- The primary goal of the VORs is for CCEVS to provide validation oversight and to ensure the technical quality of evaluations. The VORs will allow CCEVS to determine whether the CCTL evaluators understand the product and its security features through evaluator presentations explaining the analysis that was performed to evaluate the product's security features. The VORs will also provide an opportunity for the validators to share their extensive expertise with the labs.
- VORs should always 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.
- In order to make the most productive use of the very limited time allotted for VORs (2-4 hours), it is critical that both the evaluators and validators be fully prepared for their VORs.
  - Evaluators must submit the required material (ETR and vendor evidence) to the validators on or before the required date in order to give validators time to review these documents and prepare for the VOR
  - Validators must have reviewed the material provided by the CCTLs in advance and be prepared with their questions
- A VOR panel will typically consist of two CCEVS validators (a lead validator assigned to the project and a senior validator assigned to that specific VOR). CCEVS may invite other validators or CCEVS personnel to attend as observers for training purposes. If the CCTL wishes to invite other observers, CCEVS must be notified ahead of time.
- If a product is complex, additional validator personnel may be assigned to the VOR and the senior validator may divide the components or functions of the product amongst them based on their expertise.

## 2 Initial VOR – EALs 2-4

The guidelines for Initial VORs are the same for EALs 2, 3, and 4.

- Purpose: To ensure that the ST is accurate and clearly specified, meets CCEVS Policies 10 and 13, and that the evaluation team correctly performed the ASE analysis.

## 2.1 Evaluator Actions Prior to Initial VOR

- Evaluators must provide a final ST and ASE ETR, any available user/admin guidance, and the evaluation team presentation materials/slides two weeks in advance of the VOR date. The ASE ETR must pass all the work units.
- Evaluators must be prepared to answer any questions from the validators on the ST and ASE ETR.
  - At least one of the evaluators must be able to answer a given validator question. It is not necessary for all evaluation team members to be able to answer all of the validator's questions
  - It is acceptable for the evaluators to research and reference documentation during the VOR
  - In some instances, if evaluators are not able to answer a question during the VOR, they can reply back via e-mail – note that this may impact the VOR outcome
- Evaluators must understand and be able to explain the TOE as articulated in the ST.

## 2.2 Initial VOR Briefing

The evaluator(s) must prepare the following materials for formal presentation. The evaluators may prepare additional formal material as they see fit.

- Description of physical and logical boundaries of the TOE:
  - Provide a diagram that depicts all the components of the IT Environment which are required to operate the TOE
  - The TOE components and IT Environment components must be clearly and visibly delineated
  - The TOE components and IT Environment components must be clearly named with their commonly referred to names
- Description of all interactions among the components.
  - Use visual aids to describe interactions among the various components of the TOE and how those interactions are secured
    - Consider the following when describing security: integrity, disclosure protection, end point authentication, replay protection – It is important to consider these whether the components are distributed or reside on the same machine
  - Use visual aids to describe interactions among the various components of the TOE and the IT Environment and how those interactions are secured
    - Consider the following when describing security: integrity, disclosure protection, end point authentication, replay protection – It is important to consider these whether the components are distributed or reside on the same machine

- Description of secure usage assumptions.
- Description of how the secure usage assumptions, IT Environment, and TOE work together to meet the SEP requirements, i.e., TOE self-protection and maintaining domain separation for users.
  - Must address TOE in execution, TOE executables, TSF Data (including audit, I&A data, and other applicable items), and Security Attributes
- Description of how each of the SFRs is implemented in the TOE.
  - Description should focus on, as a minimum, how the SFR is implemented in the TOE at an architectural level
  - It is not sufficient to just provide a mapping of security functions and SFR
  - It is not sufficient to enumerate the SFRs
- Identify any changes to the product made in terms of security features and/or design as a result of the ASE work.
- Provide a justification about how CCEVS Policies 10 and 13 are met.

### **2.3 Validator Actions Prior to Initial VOR**

The validator shall perform the following actions prior to attending the VOR

- Get an understanding of the TOE.
  - What the TOE does?
  - How it does it?
  - Is it secure?
- Review TOE Description, SFR and TSS for consistency.
- Ensure that the distinction among TSF data, user data, security attributes is consistently applied in SFRs, operations on SFRs, TOE Description and TSS.
- Ensure TSS is plausible and describes how the SFRs are met.
- Prepare all questions to evaluators in writing.

## **3 Final VOR – EAL 2**

### **3.1 Evaluator Actions Prior to Final EAL 2 VOR**

- Evaluators must provide the following materials two weeks prior to the Final VOR:
  - Final ST (with track changes since the ST from the Initial VOR)
  - Final ETR (proprietary and non-proprietary)
  - Team test plan
  - Developer functional specification
  - Developer test plan
  - Developer vulnerability analysis
  - User/admin guidance

- Documentation describing the resolution of all action items from Initial VOR
- Draft VR
- All other evaluation evidence (except source code)
- Evaluation team presentation materials/slides
- Evaluators must be prepared to share, show, and examine all the developer evidence used in the evaluation.
- Evaluators must be prepared to answer any questions from the validators on the ETR.
  - At least one of the evaluators must be able to answer any given validator question. It is not necessary for all evaluation team members to be able to answer all of the validator's questions.
  - It is acceptable for the evaluators to research and reference documentation during the VOR.
  - In some instances, if evaluators are not able to answer a question during the VOR, they can reply back via e-mail – this may impact the VOR outcome.
- Evaluators must understand the TOE as articulated in the ST and in the developer ADV, AGD and other applicable evidence.

### **3.2 Final VOR Briefing – EAL 2**

The evaluator(s) must prepare the following material for formal presentation. The evaluators may prepare additional formal material as they see fit.

- Any changes to the ST since the Initial VOR.
- TSFI Description.
  - Summary list of interfaces by command, API and other interfaces
  - How the team determined that each TSFI is accurate
  - How the team determined that all the TSFI are included in the Functional Specification
- Administrator Guidance.
  - Summary of how to operate the TOE securely
  - Summary of functions and privileges that should be controlled
- Developer Test Description.
  - Test configuration listing IT Environment components used and their configuration
  - Test configuration listing TOE components used and their configuration
  - List of TSFI tested by developer and how the shortcomings were considered in independent testing
  - List of SFR tested by developer and how the shortcomings were considered in independent testing
- Team Test Description.
  - Test configuration listing IT Environment components used and their configuration

- Test configuration listing TOE components used and their configuration
- Summary of team independent tests
  - Description of tests
  - Description of how the functional tests augment the developer testing
  - Description of how the penetration tests augment the developer vulnerability analysis
- Summary of developer vulnerability analysis.
  - Public Domain Sources Searched
  - Key words and products used in search
  - Identified TOE vulnerabilities
  - Identified related vulnerabilities
  - Disposition of the vulnerabilities
- Identify any changes to the product made 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.

### **3.3 Validator Actions Prior to Final VOR – EAL 2**

- Review the ST.
  - Ensure that the changes since the Initial VOR are acceptable
  - Brush up on the TOE
- Determine the quality of the TSFI.
  - Are all TSFI identified (i.e., use the Functional Specification, other knowledge and ETR to make this determination)?
  - How well is each TSFI described (i.e., are all inputs, outputs, errors, exceptions, and side effects described completely)?
  - Are all SFRs implemented by the TSFI (i.e. use own analysis and ETR)?
- Review developer and team test documents and ensure that:
  - Developer test configuration is consistent with ST
  - Developer test configuration is representative of ST
  - Team test configuration is consistent with ST
  - Team test configuration is representative of ST
  - Team has tried to augment developer functional tests
  - Key security SFRs and TSFI are covered by a combination of developer and team tests
- Review developer vulnerability analysis and team test plan and ensure that:
  - Vulnerability analysis is reasonable in terms of sources searched
    - The Product (TOE) is covered by the search
    - Version number and product name is not overly restrictive
  - The evaluation team has devised penetration tests to prove or disprove developer claims and to test for obvious vulnerabilities not covered by developer

- For example, the developer may have searched for vulnerabilities too narrow for the product and version number and not considered other versions of the product or related products

## **4 Final VOR – EAL 3**

### **4.1 Evaluator Actions Prior to Final VOR – EAL 3**

- Evaluators must provide the following materials two weeks prior to the Final VOR:
  - Final ST (with track changes since the ST from the Initial VOR)
  - Final ETR (proprietary and non-proprietary)
  - Team test plan
  - Developer functional specification
  - Developer test plan
  - Developer vulnerability analysis
  - User/admin guidance
  - Draft VR
  - Documentation describing the resolution of all action items from Initial VOR
  - All other evaluation evidence (except source code)
  - Evaluation team presentation materials/slides
- Evaluators must be prepared to share, show, and examine all of the developer evidence used in the evaluation.
- Evaluators must be prepared to answer any questions from the validators on the ETR.
  - At least one of the evaluators must be able to answer any given validator question. It is not necessary for all evaluation team members to be able to answer all of the validator's questions
  - It is acceptable for the evaluators to research and reference documentation during the VOR
  - In some instances, if evaluators are not able to answer a question during the VOR, they can reply back via e-mail – this may impact the VOR outcome
- Evaluators must understand the TOE as articulated in the ST and in the developer ADV, AGD, and other applicable evidence.

### **4.2 Final VOR Briefing – EAL 3**

The evaluator(s) must prepare the following material for formal presentation. The evaluators may prepare additional formal material as they see fit.

- Any changes to the ST since the Initial VOR.
- TSFI description.
  - Summary list of interfaces by command, API and other interfaces
  - How the team determined that each TSFI is accurate

- How the team determined that all the TSFI are included in the Functional Specification
- Administrator Guidance.
  - Summary of how to operate the TOE securely
  - Summary of functions and privileges that should be controlled
- Developer Test Description.
  - Test configuration listing IT Environment components used and their configuration
  - Test configuration listing TOE components used and their configuration
  - List of TSFI tested by developer and how the full TSFI is tested
- Team Test Description.
  - Test configuration listing the IT Environment components used and their configuration
  - Test configuration listing the TOE components used and their configuration
  - Summary of team independent tests
    - Description of tests
    - Description of how the functional tests augment the developer testing
    - Description of how the penetration tests augment the developer vulnerability analysis
- Summary of developer vulnerability analysis.
  - Public Domain Sources Searched
  - Key words and products used in search
  - Identified TOE vulnerabilities
  - Identified related vulnerabilities
  - Disposition of the vulnerabilities
- Identification of any changes to the product made 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.

#### **4.3 Validator Actions Prior to Final VOR – EAL 3**

- Review the ST.
  - Ensure that the changes since the Initial VOR are acceptable
  - Brush up on the TOE
- Determine the quality of the TSFI.
  - Are all TSFI identified (i.e., use the Functional Specification, other knowledge and ETR to make this determination)?
  - How well is each TSFI described (i.e., that is, are all inputs, outputs, errors, exceptions, and side effects described completely)?
  - Are all SFRs implemented by the TSFI (i.e., use own analysis and ETR)?

- Review developer and team test documents and ensure that.
  - Developer test configuration is consistent with ST
  - Developer test configuration is representative of ST
  - Team test configuration is consistent with ST
  - Team test configuration is representative of ST
  - Developer has tested the full TSFI
  - Team has tried to augment developer functional tests
  - Key security SFR and TSFI are covered by a combination of developer and team tests
  
- Review developer vulnerability analysis and team test plan to determine if.
  - Vulnerability analysis is reasonable in terms of sources searched
    - Product is covered
    - Version number and product name is not overly restrictive
  - The evaluation team has devised penetration tests to prove or disprove developer claims and to test for obvious vulnerabilities not covered by developer
    - For example, the developer may have searched for vulnerabilities too narrow for the product and version number and not considered other versions of the product or related products

## **5 Test VOR – EAL 4**

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 AGD, ATE and AVA\_VLA work units. The Test VOR is conducted after the receipt and successful review of the Developer Testing.

- The team test plan must include the following:
  - Test configuration
  - Test schedule
  - Developer test suites that will be executed by the team
  - Team tests (functional and penetration tests), including
    - Test cases
    - Test setup
    - Test description sufficiently detailed to assess the value and efficacy of the tests
    - Origin of team's penetration tests
    - Test results (for the Final VOR)

### **5.1 Evaluator Actions Prior to Test VOR – EAL 4**

- Evaluators must provide the following materials two weeks prior to the Test VOR:
  - Final ST (with track changes since the ST from the Initial VOR)
  - Final ETR (proprietary) with all work units except team testing related
  - Team test plan (minus test results)
  - Developer functional specification
  - Developer test plan

- Developer vulnerability analysis
- Documentation describing the resolution of all action items from Initial VOR
- All other available evaluation evidence (except source code)
- Evaluation team presentation slides/materials
- Evaluators must be prepared to share, show, and examine all of the developer evidence used in the evaluation.
- Evaluators must be prepared to answer any questions from the validators on the ETR.
  - At least one of the evaluators must be able to answer any given validator question. It is not necessary for all evaluation team members to be able to answer all of the validator's questions.
  - It is acceptable for the evaluators to research and reference documentation during the VOR
  - In some instances, if evaluators are not able to answer a question during the VOR, they can reply back via e-mail – this may impact the VOR outcome
- Evaluators must understand the TOE as articulated in the ST and in the developer ADV, AGD, and other applicable evidence.

## 5.2 Test VOR Briefing – EAL 4

The evaluator(s) must prepare the following material for formal presentation. The evaluators may prepare additional formal material as they see fit.

- Any changes to the ST since the Initial VOR.
- TSFI description
  - Summary list of interfaces by command, API and other interfaces
  - How the team determined that each TSFI is accurate
  - How the team determined that each TSFI fully describes inputs, outputs, errors, exception, effects, and side effects
  - How the team determined that all the TSFI are included in the Functional Specification
- Administrator Guidance.
  - Summary of how to operate the TOE securely
  - Summary of functions and privileges that should be controlled
- Developer Test Description.
  - Test configuration listing IT Environment components used and their configuration
  - Test configuration listing TOE components used and their configuration
  - List of TSFI tested by developer and how the full TSFI is tested
    - Each TSFI is tested
    - Each error, exception, effect, and side effect for each TSFI is tested
- Team Test Description.

- Test configuration listing the IT Environment components used and their configuration
- Test configuration listing the TOE components used and their configuration
- Summary of team independent tests
  - Description of tests
  - Description of how the functional tests augment the developer testing
  - Description of how the penetration tests augment the developer vulnerability analysis
  - Description of other sources and experiences considered in vulnerability analysis
  - Description of broader searches made for vulnerability analysis
- Summary of developer vulnerability analysis.
  - Public Domain Sources Searched
  - Key words and products used in search
  - Identified TOE vulnerabilities
  - Identified related vulnerabilities
  - Disposition of the vulnerabilities
- Identification of any changes to the product made in terms of security features and//or design as a result of the evaluation.

### **5.3 Validator Actions Prior to Test VOR – EAL 4**

- Review the ST.
  - Ensure that the changes since the Initial VOR are acceptable
  - Brush up on the TOE
- Determine the quality of the TSFI.
  - Are all TSFI identified (i.e., use the Functional Specification, other knowledge and ETR to make this determination)?
  - How well is each TSFI described (i.e., are all inputs, outputs, errors, exceptions, and side effects described completely)?
  - Are all SFRs implemented by the TSFI (i.e., use own analysis and ETR)?
- Review developer and team test documents to ensure that:
  - Developer test configuration is consistent with ST
  - Developer test configuration is representative of ST
  - Team test configuration is consistent with ST
  - Team test configuration is representative of ST
  - Developer has tested the full TSFI/FSP in terms of each interface
  - Each TSFI is tested fully in terms of inputs, outputs, errors, exceptions, and side effects
  - Team has tried to augment developer functional tests
- Review developer vulnerability analysis and team test plan to ensure that:
  - Vulnerability analysis is reasonable in terms of sources searched
    - Product is covered

- Search goes beyond the evaluated version number
- Search includes similar products
- Search includes similar IT Environment to which the TOE operates on
- The evaluation team has devised penetration tests to prove or disprove developer claims and to test for obvious vulnerabilities, not covered by the developer.
  - For example, the developer may have searched for vulnerabilities too narrow for the product and version number and not considered other versions of the product or related products.
- Team has devised penetration tests based on team experience and other sources
- Any other ideas that come to validator should be noted and shared during the Test VOR

## **6 Final VOR – EAL 4**

### **6.1 Evaluator Actions Prior to Final VOR – EAL 4**

- Evaluators must provide the following two material weeks prior to the Final VOR:
  - Final ST (with track changes since the ST from the Test VOR)
  - Final ETR (proprietary and non-proprietary)
  - Team test results
  - Final VR
  - Documentation describing the resolution of all action items from Test VOR
  - Evaluation team presentation materials/slides
  - All evaluation evidence (except source code)
- Evaluator must be prepared to share, show, and examine all the developer evidence used in the evaluation.
- Evaluators must be prepared to answer any questions from the validators on the ETR:
  - One of the evaluators must be to answer any questions – All the members of the evaluation team need not be able to answer all the questions.
  - It is acceptable for the evaluators to research and reference documentation during the VO.
  - In some instances, if evaluators are not able to answer a question during the VOR, they can reply back via e-mail – this may impact the VOR outcome.
- Evaluators must understand the TOE as articulated in the ST and in the developer ADV, AGD, and other applicable evidence.

### **6.2 Final VOR Briefing – EAL 4**

Because Test VORs will occur for EAL4, the primary focus of the Final VOR at this EAL is to review of the team testing. The evaluator(s) must prepare the following material for formal presentation. The evaluators may prepare additional formal material as they see fit.

- Any changes to the ST since the Test VOR
- Any changes to the TSFI description since the Test VOR
- Any changes to the developer Test Descriptions since the Test VOR
- Any changes to the team test plan since the Test VOR
- Team test results
- Any changes to the developer vulnerability analysis since the Test VOR
- Any other significant changes to the TOE or developer evidence
- Any changes to the product made in terms of security features and/or design as a result of the evaluation.

### 6.3 Validator Action Prior to Final VOR – EAL 4

- Review the ST.
  - Ensure that the changes since the Test VOR are acceptable
  - Brush up on the TOE
- Determine that the TOE changes are appropriate.
  - TSFI, if applicable
  - Developer test plan, if applicable
  - Team test plan, if applicable
  - Developer vulnerability analysis, if applicable
- Review team test results.

## 7 VOR Completion

### 7.1 Validator Action to Complete VOR

- The lead validator is responsible for documenting the VOR results in the required M/R format and sending them to the evaluation team leader and the senior validator for review and comment within 3 days of the VOR meeting.  
**NOTE: if agreed upon prior to the VOR meeting, the validator may delegate the writing of all or part of the draft M/R to the evaluation team.**
- The evaluation team and senior Validator will review and provide updates to the lead Validator within 2 days of receipt of the draft M/R.

- Updates will be made (if necessary) and the final version of the M/R will be forwarded by the lead validator to CCEVS (crecords) and to the evaluation team within 6 days of the VOR meeting.