



National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

CCEVS Policy Letter #19

8 September 2008

SUBJECT: Requirements for Evaluations with Components above Evaluated Assurance Level (EAL) 4

PURPOSE: Provide clarification on the Common Criteria Evaluation and Validation Scheme (CCEVS) approach for approved Common Criteria Testing Laboratories (CCTLs) who have Sponsors desiring evaluations with components above EAL4 that require NSA evaluation resources. In addition, to clarify how NSA evaluation resources are allocated to these evaluations.

BACKGROUND: Many Security Targets (STs) and validated Protection Profiles (PPs) are developed with augmentations of individual assurance components above EAL4. The NVLAP accreditation program only supports test methods based on the Common Evaluation Methodology (CEM) up through EAL4. The guidance for International Common Criteria members under the Common Criteria International Recognition Arrangement (CCRA) for evaluations above EAL4 requires member nations to use their own national methodologies.

Evaluations with components above EAL4 may require NSA involvement. NSA evaluation resources are required for evaluations that include any of the following assurance requirements:

CC version 2.3 component	CC version 2.3 component description	CC version 3.1 component	CC version 3.1 component description
ADV_FSP.4	Formal Functional specification	ADV_FSP.6	Complete Semi-formal Functional Specification with additional formal specification
ADV_HLD.5	Formal high-level design	ADV_TDS.6	Complete semiformal modular design with formal high-level design presentation
ADV_LLD.3	Formal low-level design		
ADV_RCR.3	Formal correspondence demonstration		
ADV_SPM.3	Formal security policy	ADV_SPM.1	Formal TOE security

9800 Savage Road, STE 6757, Ft. Meade, MD 20755-6757
 Phone: (410) 854-4458 Fax: (410) 854-6615 E-mail: scheme-comments@missi.ncsc.mil
<http://www.niap-ccevs.org/cc-scheme>

	model		policy model
AVA_VLA.3	Moderately resistant	AVA_VAN.4	Methodical vulnerability analysis
AVA_VLA.4	Highly resistant	AVA_VAN.5	Advanced Methodical vulnerability analysis
Any explicitly-stated component that specifies formal methods		Any Extended component that specifies formal methods	

NSA evaluation resources are only committed to evaluations that NSA deems necessary and are completely separate from CCEVS resources. CCEVS serves as liaison between the NSA evaluators and the vendor whose product is being evaluated. Typically, the vendor will not interact with NSA evaluators until immediately prior to the start of the NSA evaluation of the product. See Appendix A for an overview of the NSA Evaluation Process for CCEVS evaluations.

POLICY: After CCEVS approval, CCTLs will conduct evaluations with components above EAL4 that require NSA resources in accordance with the following:

1. NSA evaluation resources will be assigned only when the following conditions are met:

- a. The evaluation shall claim compliance to a Medium or High Robustness U.S. Government Protection Profile, if a validated PP for the technology type exists¹;
- b. The evaluation shall be coordinated with the CCEVS prior to the CCTL signing a contract with a sponsor to perform the evaluation. This will preclude potential problems and misunderstandings that could lead to contractual issues for the CCTL. The CCTL evaluation results will feed into the NSA evaluation of the higher assurance components;
- c. The Security Target shall be provided to NSA evaluators for review prior to the assignment of NSA resources. This review will verify that the configuration to be evaluated and the defined environment are both reasonable, and that the stated threats and assumptions are appropriate for the described configuration and environment; and
- d. The vendor agrees to the conditions for NSA evaluations. At a minimum, these conditions include vendor submission of configured hardware & software and signature of the NSA Bailment agreement

¹ ¹ If no PP exists for the product technology type, then CCEVS will determine whether there is an existing PP to which the product should conform.

(copy available upon request), all evaluation results from the CCTL (including relevant vendor test results), all source code, and vendor technical support (as needed to support the evaluation). NSA may impose additional requirements, depending on the technology, complexity of the TOE, and assurance requirements.

When the above four conditions are met, NSA evaluation resources will be assigned to the project, an evaluation point of contact will be identified, NSA will establish an estimated completion date, and the vendor will be notified by CCEVS.

2. All evaluations should use the published evaluation methodology for components above EAL4, where that methodology exists. Where no methodology exists, the CCTL must develop this methodology and submit it for approval to CCEVS. In addition, these evaluations will have increased government involvement that may impact the CCTL proposed schedule and deliverables.

3. The level of government involvement will be determined by CCEVS based upon factors such as the technology type and its potential use within the Federal government. At the discretion of NSA, there are three possible courses of action for these evaluations:

- a. The CCTL will conduct all evaluation activities;
- b. The government will augment the CCTL team with seasoned evaluators and together they will conduct all evaluation activities; or
- c. The government will independently conduct selected evaluation activities providing results of the activities to the CCEVS for incorporation into the evaluation records.

4. Because CCEVS has no direct control over NSA evaluation resources, any slippage in the CCTL evaluation schedule may result in the removal of NSA evaluation resources from the project and will invalidate any previously established NSA testing schedule. The CCTL must notify CCEVS of any schedule slippages as early as possible in order to mitigate the risk of losing resources and in order to determine whether NSA testing can be rescheduled.

Effective Date:

All new evaluations (i.e. those for which the Evaluation Acceptance Package (EAP) has not been received by the date of this policy) must conform to this policy.

Original Signed By

AUDREY M. DALE
Director

Appendix A

NSA Evaluation Process Overview for CCEVS Evaluations

I. Evaluation Preparation

Begins before the official NIAP CCEVS evaluation commences

- CCEVS receives a draft Security Target (ST) and a Letter of Interest (LOI) from the CCTL.
- CCEVS notifies the NSA evaluation office and a copy of the ST is provided to them.
- The NSA evaluation office reviews the ST (30 days allocated for this task).
- The NSA evaluation office makes a determination on whether or not the submitted product meets their requirements and if they have sufficient resources to accomplish the work. If they do, the NSA evaluation office will provide CCEVS with the name of the NSA evaluation point of contact (POC).
- NSA evaluation office provides CCEVS with the requirements for NSA training, product delivery, and projected schedule. CCEVS shares these requirements with the vendor.
- CCEVS prepares and sends a Bailment Agreement to the vendor for signature. This agreement outlines the details of product delivery and return of the product after completion of the NSA evaluation.

II. Kick-Off Meeting

Signifies the official start date of the NIAP CCEVS evaluation with the CCTL

- The NSA evaluators may participate in the CCEVS kick-off meeting in order to meet the project participants and to discuss any questions or issues specific to their portion of the evaluation.
- The vendor POC for the NSA portion of the evaluation must be identified at the kick-off meeting.

III. Pre-Evaluation

Occurs during the CCTL portion of the evaluation but before the official start of NSA evaluation activities

- NSA evaluators receive the requested product training.
- The vendor and NSA evaluators (with assistance as needed by CCEVS) coordinate the logistics for the delivery and receipt of the product.

- All CCTL evaluation results (including relevant vendor analysis and testing) and tested product configuration information is delivered to the NSA evaluation POC.

IV. NSA Evaluation

At this point, the CCTL evaluation is complete (additional CCTL work may be necessary if the NSA evaluation results in product updates). This NSA Evaluation activity begins after all required deliverables have been received and the product is properly configured

- NSA evaluators conduct their portion of the evaluation.
- The NSA evaluators document their results in an Evaluation Technical Report (ETR) and deliver it to CCEVS.
- NSA shares the NSA evaluation results/findings with the vendor.

V. Post Evaluation

This phase is only required when fixes to the product are necessary

- CCEVS and NSA evaluators coordinate all necessary product fixes with the vendor.
- After product revisions are made, re-testing by NSA evaluators will be scheduled
- After NSA testing is completed, a final ETR will be produced by the NSA evaluators and submitted to the CCEVS.

VI. Evaluation Wrap-Up

All evaluation activities have been completed.

- The product software and/or hardware will be handled in accordance with the Bailment Agreement.
- CCEVS Validator writes the final Validation Report (VR).
- The Final VR is posted to the CCEVS website & certificate is issued.