CCEVS Policy Letter #13

7 February 2006

SUBJECT: Acceptable TOEs for Evaluation

PURPOSE: In response to comments from customers who report that CCEVS evaluation results are oftentimes useless because they exclude useful or expected functionality, CCEVS provides the following policy to define characteristics of "reasonable" targets of evaluation.

POLICY: A TOE is considered reasonable for evaluation if it meets any of the following characteristics:

1. The physical boundary of the TOE is the entire product, including hardware, as commercially available from the developer; no part of the product may be excluded from the boundary of evaluation.
   Note: to exhibit this characteristic, the developer may either have the entire product (as commercially available) evaluated and analyzed, or may have the target of the evaluation made commercially available as a product for purchase. That is, either the TOE boundary must extend to include the whole product, or a (new) product must be defined with a smaller TOE boundary. In either case, the TOE must not require the consumer to use additional special-purpose products from the same vendor in order to make use of the functionality provided by the TOE. For example, a security package whose functionality depends upon proprietary mechanisms unavailable to other vendors of different products would have to include both the security package and those proprietary mechanisms within the TOE boundary. In contrast, an application that requires general purpose hardware, OS, and/or DBMS could exclude those components from the TOE boundary because these are generally available.
2. The logical boundary of the TOE includes all the functionality that would commonly be regarded as security functionality for that product type by the user community. That is, the TOE meets the definition for its Technology Type, as described in Appendix A of this Policy.
3. The TOE claims compliance to any validated Protection Profile. If a TOE drops such a compliance claim, its reasonableness will be reconsidered by CCEVS.
4. The TOE is a "component", as defined by Policy Letter 8.

Any TOE that fails to meet at least one of the above conditions must be accompanied by an explanation of why the reasons prompting this Policy (see Rationale, below) do not exist or are otherwise not of concern.

9800 Savage Road, STE 6740, Ft. Meade, MD 20755-6740
Phone 410-854-4458, Fax 410-854-6615, Email: scheme-comments@missi.ncsc.mil
http://niap.nist.gov/cc-scheme

If a TOE boundary changes during evaluation, its reasonableness will be reconsidered by CCEVS.

Rationale:
This Policy is prompted by two primary factors:

a. the prevalence of TOE boundaries that subset the product that is delivered to end customers. As a consequence, much of the product remains unevaluated. Vulnerabilities that are found outside the TOE boundary nevertheless remain within the product, which does the customer little good.

b. the prevalence of TOEs whose security claims are reduced to the extent that the security functionality that is evaluated omits a notable portion of the functionality typically associated with the product type of the TOE. As a consequence, TOEs are identified and listed as being of a particular TOE type implicitly providing security functions, when in fact those functions are excluded from the boundary of evaluation analysis.

The intent of this Policy is to produce evaluation results that are (more) meaningful to customers, as well as to ensure that validation resources are being used wisely. As such, CCEVS, at its sole discretion, may refuse admission of evaluation of products that fail meet either the letter or the intent of this policy.

Effect:
This policy overturns past practice of allowing arbitrary products, or portions of products, to be the target of evaluation.

Effective Date:
All new evaluations; i.e. those for which the Evaluation Acceptance Package (EAP) has not been received by the time this policy is issued, must conform to this policy.

Grace Period:
CCTLs have one week to notify CCEVS of any on-going negotiations with prospective evaluation sponsors; required adherence by these will be judged on a case-by-case basis.

Relation to other Policies:
While Policy Letter 10 ("Acceptance of Security Targets (STs) Into NIAP CCEVS Evaluation") mandates that TOE boundaries must be clearly drawn (and how this is judged), this policy mandates the characteristics of that clearly-drawn boundary.

This policy continues to permit TOEs conforming to Policy Letter 8.

Original Signed By

AUDREY M. DALE
Director

9800 Savage Road, STE 6740, Ft. Meade, MD 20755-6740
Phone 410-854-4458, Fax 410-854-6615, Email: scheme-comments@missi.ncsc.mil
http://niap.nist.gov/cc-scheme