CCEVS Policy Letter #13
Addendum #1

24 May 2007

SUBJECT: Acceptable TOEs for Evaluation - Clarification

PURPOSE: To clarify Policy 13's discussion of what constitutes a "reasonable" TOE.

POLICY: Reasonability is measured against the expectations of potential customers who will be using evaluated products based upon the findings of the evaluations. These expectations are based upon the description of the product as found in materials and information readily available on the developer's website.

The security functions described on the website must be included within the boundary of the TOE and must be covered by one or more SFRs. During evaluation, the analysis and testing of each security function must verify that it works as described. Exclusion of advertised security features from the TOE boundary requires the written approval of CCEVS before the start of evaluation.

RATIONALE and BACKGROUND: Policy 13 described four scenarios concerning acceptable TOEs. These were presented as "characteristics" which has led to the reasonable, yet incorrect, understanding of the intent of Policy 13.

Scenario 1 addresses the case where the TOE consisted of the entire product as delivered. This was meant to be an acceptable TOE on the grounds that the entire TOE would be analyzed, as described above. This addendum clarifies that the intent is based on logical as well as physical boundaries; i.e., that the entire product as described from a security point of view is considered to be the TOE, not just that the physical boundary of the device.

Scenario 2 addresses the case where the TOE includes all the functionality that would commonly be regarded as security functionality for that product type by the user community. This was meant to say, in a more formal style, that something being promoted as, say, a firewall cannot have any of the firewall functionality excluded from analysis. Policy 13 attempted to head off arguments about what "firewall functionality" would be, by defining it, along with several other technology types, in the Appendix. This addendum clarifies that the expectation of the security functionality to be included in the TOE is to be whatever is advertised to potential customers in addition to the security functionality that customers would expect based on the product type, as codified by the definitions in the Appendix.

Scenario 3 addresses the case where the TOE claims compliance to a PP. The intent behind this scenario was that, since the PPs were presumed to codify the expectations of the customer, compliance to the PP would be sufficient to meet those expectations. However, that only captures the expectations of the product type described by the PP. Products often include additional security features for product

differentiation; it is the expectation of CCEVS that these additional security features would also be covered by the evaluation.

Scenario 4 addresses the case where the TOE is a component, as defined by Policy 8. Since such components are not listed, there are no customer expectations. This scenario was included solely to convey explicitly that Policy 8 was unaffected by Policy 13.

These four scenarios were not meant to be understood as mutually-exclusive; the intent is that in cases where more than one is applicable, all the corresponding mandates are to be followed. For example, a TOE might be an entire product that promises security functions and claims compliance to a PP (the first three scenarios apply), in which case the entire security functionality must be analyzed and the claims verified.

RELATED POLICIES: Policy 15 requires that FAU_GEN be included[1] in all STs by asserting that the generation of audit data is a reasonable expectation in virtually all TOE technology types.

EFFECTIVE DATE: This policy addendum takes effect immediately for all EAPs that are submitted to CCEVS.

Original Signed By

AUDREY M. DALE
Director

[1] As an SFR for the TOE, not for the environment.