CCEVS Policy Letter #9

13 June 2005

SUBJECT: Crypto in Common Criteria Evaluations

PURPOSE: To clarify the CCEVS documentation needed for crypto in a Common Criteria evaluation.

BACKGROUND: All cryptographic algorithms used for encryption must be specified in the FCS.COP requirement section of the ST.

A description of how cryptographic algorithms are used must be included in the TSS section of the ST.

NIAP Interpretation 427 states that:

-Claims about use of a standard must be unambiguous with respect to the source of a metric and the meaning of compliance.

-If a compliance claim is made, the PP/ST author must provide an indication of how compliance is to be determined.

-Compliance may be verified as part of the TOE evaluation, it might be claimed by a developer, or it might be verified by an independent party.

If the cryptography in a product is claiming compliance to a standard by vendor assertion, then it must be stated that the implementation of the encryption was not verified during the evaluation. This information should be included in the **Executive Summary, Testing, and Validator Comments** sections of the **Validation Report**.

Following is the statement to be used: "The cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor."

The **Security Evaluation Summary** section of the **VPL** should include the following caveat:

"For this evaluation, it was appropriate for the Security Target to claim compliance with the external standard for <algorithm> for the definition of the encryption algorithm. There are many ways of determining compliance with a standard. <TOE> has chosen to make a developer claim of compliance. This means that there has been no independent verification (by either the

evaluators or a third party standards body, such as a FIPS laboratory) that the implementation of the cryptographic algorithms actually meets the claimed standards. Potential users of this product should confirm that the cryptographic capabilities are suitable to meet the user's requirements."

Original Signed By

AUDREY M. DALE
Director