National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

NIAP Policy Letter #5

17 November 2016

SUBJECT: Applicability and Relationship of NIST Cryptographic Algorithm Validation Program (CAVP) and Cryptographic Module Validation Program (CMVP) to NIAP's Common Criteria Evaluation and Validation Scheme (CCEVS).

REFERENCES: Committee on National Security Systems Policy #11

National Institute of Standards and Technology Federal Information Processing Standard 140-2

PURPOSE: This policy defines the applicability and relationship of NIST CAVP and CMVP testing to assurance activities associated with cryptography requirements in NIAP-approved Protection Profiles (PPs).

BACKGROUND: NIAP- approved PPs may specify cryptographic assurance activities that are intended to verify that the cryptography specified in the Target of Evaluation (TOE) satisfies the corresponding PP security functional requirement. Since NIST has programs (CAVP and CMVP) to verify algorithm and cryptographic module implementation, NIAP is issuing this policy to minimize redundancies between the activities of the NIST test facilities and the Common Criteria Test Laboratories (CCTLs).

POLICY: This policy applies to evaluations conducted in NIAP, for all Targets of Evaluation (TOEs) that include cryptography to satisfy requirements contained in NIAP-approved PPs. All cryptography in the TOE for which NIST provides validation testing of FIPS-approved and NIST-recommended cryptographic algorithms and their individual components must be NIST validated (CAVP and/or CMVP). At a minimum an appropriate NIST CAVP certificate is required before a NIAP CC Certificate will be awarded.

To demonstrate that all cryptographic requirements are satisfied, the ST must clearly indicate all SFRs for which a CAVP certificate is claimed and include, at a minimum, the cryptographic operation, the NIST standard, the SFR supported, the CAVP algorithm list name (e.g. AES, KAS, CVL, etc.) and the CAVP Certificate number. The CCTL will verify that the claimed NIST validation complies with the NIAP-approved PP requirements the TOE claims to satisfy. The CCTL verification of the NIST validation will constitute performance of the associated assurance activity.

EFFECT: This policy documents current NIAP evaluation practices and ensures products with cryptography claiming compliance with NIAP-approved PPs are properly evaluated without duplication of effort.

EFFECTIVE DATE: All evaluations submitted to NIAP must conform to this policy immediately.

Original Signed By

JANINE S. PEDERSEN
Director, NIAP