12 June 2015

Frequently Asked Questions for NIAP Policy #5

1. ***Why is this policy being issued?***

   This policy is being issued to help streamline the NIAP evaluation process, help reduce cost, and eliminate redundant activities. This policy does not provide an exemption from protection profile-mandated documentation (e.g., Security Target, required entropy documentation, etc.), but does provide an exemption for the testing that is conducted by the CCTL if that testing is conducted as part of a NIST CAVP or CMVP validation.

2. ***How is this policy applicable for products evaluated against NIAP-approved PP/cPPs, but outside of NIAP?***

   All assurance activities described in the PP/cPP must be performed in order to successfully complete a Common Criteria evaluation and be listed on the NIAP PCL. Validation activities that are performed during a cryptographic algorithm or module validation which results in a NIST CAVP/CMVP certificate may be used to demonstrate compliance to some PP/cPP assurance activities. Additional Common Criteria testing will be unnecessary for these assurance activities. NIAP will continue to list products on the PCL which have been evaluated outside the US as long as the ST demonstrates exact compliance with NIAP PP/cPPs. A CCRA Compliant Certification Body with a NIST FIPS program or willing to accept NIST validation results can also take advantage of the NIST testing activities to satisfy compliance to PP/cPP assurance activities.

3. ***When can a CAVP certificate be applied to a PP assurance activity?***

   In NIST's draft Frequently Asked Questions For the Cryptographic Algorithm Validation Program Concerning the Validation of Cryptographic Algorithm Implementations, Last Update: July 10, 2014, GEN.7 provides guidance on the relationship between the operating environment for cryptographic algorithm implementation validations and the operating environment for cryptographic modules. NIAP has adapted this guidance for NIST validated cryptographic algorithm implementations (i.e. NIST-approved algorithm implementations that have CAVP certificate number) used in the Target of Evaluation (TOE).

   For a validated cryptographic algorithm implementation to be applicable to a TOE, the following requirements must be met:

   a. The implementation of the validated cryptographic algorithm has not been modified upon integration into the TOE; and

   b. The operational environment under which the validated cryptographic algorithm implementation was tested must be equivalent to the operational environment that the TOE is being tested by the CCTL.

4. ***What are examples of an equivalent operational environment?***

NIAP will rely on NIST to establish guidance and to determine when operational environments are equivalent. The following examples are adapted from NIST's Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program, Last Update: March 2, 2015, section 1.4, Binding of Cryptographic Algorithm Validation Certificates.

a. If an implementation has been tested on an X-bit processor (e.g. 32-bit, 64-bit), can a claim be made that the implementation also runs on different bit size processors?

   Maybe. An algorithm implementation was tested and validated on a 32-bit platform. Now the algorithm implementation is in a TOE using a 64-bit platform. This algorithm implementation **cannot operate** on the TOE's 64-bit platform without change. In this case, the operational environments are not the same. Therefore the algorithm implementations **must be re-tested** on the TOE's 64-bit platform. Memory size, processor frequency, etc. are not relevant.

   An algorithm implementation was tested and validated on a 32-bit platform. Now the algorithm implementation is in a TOE using a 64-bit platform. This algorithm implementation **can operate** on the TOE's 64-bit platform without change because the TOE's 64-bit platform supports execution of code in a 32-bit mode. In this case, the algorithm implementation **does not have to be re-tested.**

b. If an algorithm implementation has been tested on one processor, can a claim be made that the implementation also runs on a different processor?

   If the untested processor supports the same instruction set and operates on the same word size as the tested processor and the algorithm implementation can operate on the untested processor without change, then the algorithm implementation **does not have to be re-tested.**

c. If an algorithm implementation has been tested on one operating system, can a claim be made that the implementation also runs on another operating system?

   The algorithm implementation must be tested on every major release of an operating system used by the TOE. A vendor may re-use algorithm implementations between like operational environments. However if the algorithm implementation testing was only performed on Windows 7, and the algorithm implementation is to be re-used in a TOE using Windows 8, the algorithm implementations **must be re-tested** on Windows 8.

   On the other hand, if the algorithm implementation testing was performed on the initial release of Windows 7, and the algorithm implementation is to be re-used in a TOE using Windows 7 Service Pack 1, then the algorithm implementation **does not have to be re-tested.**

5. How is a CAVP certificate applied to a PP assurance activity?

The following PP requirements must be addressed by obtaining a CAVP certificate number:

FCS_CKM (except .4)
FCS_COP
FCS_RBG_EXT.1

The vendor shall list the CAVP certificate number in the description of how the appropriate TOE SFR is met in the Security Target.

> When the CCTL addresses an assurance activity where the vendor has indicated in the associated SFR that there is a relevant CAVP certificate number, the CCTL shall consult the appropriate Validation System document and Algorithm Validation List. If the CCTL finds that the associated tests, implementation, operational environment and modes, states and key sizes cover elements of the assurance activity, then the CCTL does not need to test those elements. The CCTL shall indicate in the Assurance Activity Report that those elements were tested as part of the CAVP validation.

6. *How is a CMVP certificate applied to a PP assurance activity?*

If a vendor wants to use the results from a FIPS 140-2 cryptographic module validation in which a CMVP certificate number was awarded, then the vendor must:

a. Provide the CMVP certificate number in the Security Target;

b. Provide the relevant assertions, AS, from the draft NIST Derived Test Requirements for FIPS PUB 140-2, dated January 4, 2011, in the description of how the appropriate TOE SFR is met in the Security Target; and

c. Provide the CCTL with a copy of the submission package prepared by the CST laboratory and reviewed by the CMVP which resulted in the awarding of this CMVP certificate number.

When the CCTL addresses an assurance activity where the vendor has indicated in the associated SFR that there is a relevant NIST DTR assertion, the CCTL shall consult the copy of the vendor provided submission package (6.c). If the CCTL finds that the associated Required Test Procedures, TEs, cover elements of the assurance activity, then the CCTL does not need to test those elements. The CCTL shall indicate in the Assurance Activity Report that the PP assurance activities were conducted as part of the FIPS 140-2 validation.