National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

CCEVS Policy Letter #20

15 November 2010

SUBJECT: NIAP policy for the use of IEEE Multifunction Function Device Protection Profiles (IEEE 2600.1™ and IEEE 2600.2™)

PURPOSE: Establishes the criteria and process by which NIAP CCEVS will view and apply the IEEE generated 2600 Protection Profiles for use by NIAP Common Criteria Testing Laboratories (CCTL) and how NIAP CCEVS will recognize products that comply with these PPs.

BACKGROUND: IEEE developed a set of Protection Profile for a Multifunction Device (e.g., printer, scanner, copier, and fax), also call Hard Copy Devices (HCD). They developed the PPs based on operational environments. This policy is directed at two of the PPs, IEEE 2600.1, developed for environment A (a restrictive commercial information processing environment in which a relatively high level of document security, operational accountability, and information assurance are required) and IEEE 2600.2, developed for environment B (a commercial information processing environment in which a moderate level of document security, network security, and security assurance are required). In order to support the evolution of NIAP, generic assurance levels defined in Protection Profiles are being reviewed and converted to a more technology specific assurance package. While these tailored assurance packages are in development, NIAP will accept products claiming compliance with a U.S. approved Protection Profile with an EAL no higher than EAL2. Since the IEEE has generated an IEEE 2600.2 at EAL2, NIAP will institute the following policy:

POLICY: NIAP will recognize the IEEE P2600.2 Protection Profile augmented with the changes outlined in Attachment A to this Policy as a U.S. Approved PP. The **IEEE 2600.1 PP will no longer be accepted for new evaluations under NIAP CCEVS** after the effective date of this policy. Products accepted into evaluation under NIAP CCEVS that claim conformance to the U.S. Approved IEEE 2600.2 PP may include additional functional requirements to those of Attachment A but **shall not** include any additional assurance requirements.

Products claiming conformance to either IEEE 2600.1 or IEEE 2600.2 (augmented with Attachment A) under a CCRA Certification Body outside the U.S., will be recognized as IEEE 2600.2 compliant under NIAP CCEVS and will be listed as such on the NIAP website. The IEEE 2600.1 is a superset of the requirements of IEEE 2600.2 and therefore satisfies the minimum requirements defined in the US Approved profile.

EFFECTIVE DATE: All new evaluations are subject to this policy, effective the date of this policy.

Original Signed By

CAROL SAULSBURY HOUCK
Director

9800 Savage Road, STE 6757, Ft. Meade, MD 20755-6757
Phone 410-854-4458, Fax 410-854-6615, Email: scheme-comments@niap-ccevs.org
http://niap-ccevs.org/

Attachment A:

CHANGES FOR DATA IN TRANSIT: To satisfy U.S. government needs, products being evaluated against the IEEE P2600.2 protection Profile must include the changes in their Security Target. The threats, objectives and functional requirements will be modified as listed below:

The following Threats will no longer be considered for User Document Data at rest alone they will include User Document Data at rest and in transit.

Threats, policies, and assumptions	**Summary**	**Objectives and rational**
T.DOC_REST.DIS.	User Document Data at rest in the TOE may be disclosed to unauthorized persons.	O.DOC_REST.NO_DIS protects D.DOC at rest in the TOE from unauthorized disclosure.
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization.
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization.
T.DOC_REST.ALT	User Document Data at rest in the TOE may be altered by unauthorized persons.	O.DOC_REST.NO_ALT protects D.DOC at rest in the TOE from unauthorized alteration.
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization.
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization.
T.FUNC_REST.ALT.	User Function Data at rest in the TOE may be altered by	O.FUNC_REST.NO_ALT protects D.FUNC at rest in the

	unauthorized persons.	TOE from unauthorized alteration.
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization.

The new threat table will include User Document Data at rest and in transit.

Threats, policies, and assumptions	**Summary**	**Objectives and rational**
T.DOC.DIS.	User Document Data may be disclosed to unauthorized persons.	O.DOC.NO_DIS protects D.DOC from unauthorized disclosure.
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization.
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization.
T.DOC.ALT	User Document Data may be altered by unauthorized persons.	O.DOC.NO_ALT protects D.DOC from unauthorized alteration.
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization.
		OE.USER.AUTHORIZED establishes responsibility of the

		TOE Owner to appropriately grant authorization.
T.FUNC.ALT.	User Function Data may be altered by unauthorized persons.	O.FUNC_ NO_ALT protects D.FUNC from unauthorized alteration.
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization.

The following Security Objectives will no longer be considered for User Document Data at rest alone they will include User Document Data at rest or in transit.

> O.DOC_REST.NO_DIS - The TOE shall protect User Document Data at rest (stored) in the TOE from unauthorized disclosure.
> O.DOC_REST.NO_ALT - The TOE shall protect User Document Data at rest (stored) in the TOE from unauthorized alteration.
> O.FUNC_REST.NO_ALT - The TOE shall protect User Function Data at rest (stored) in the TOE from unauthorized alteration.

The new Security Objectives will be as follows:

> O.DOC.NO_DIS - The TOE shall protect User Document Data from unauthorized disclosure.
> O.DOC.NO_ALT - The TOE shall protect User Document Data from unauthorized alteration.
> O.FUNC.NO_ALT - The TOE shall protect User Function Data from unauthorized alteration.

The following Functional requirements used in the PP will be modified as follows:

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **communication of D.DOC, D.FUNC, D.PROT, and D.CONF over any Shared-medium Interface**.

> PP APPLICATION NOTE 118. FTP_ITC.1 is a principal SFR to fulfill O.DOC.NO_DIS, O.DOC.NO_ALT, O.FUNC.NO_ALT, O.PROT.NO_ALT, O.CONF.NO_DIS, and O.CONF.NO_ALT.