

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-C** SC **2** P **2** L **18** # **5**
 Sukert, Alan Xerox

Comment Type **E** Comment Status **D**

The title of IEEE Std. 2600 in the Normative References is incorrect. It is stated as 'Information Technology: Hardcopy System and Device Security'; it should be 'Information Technology: Hardcopy Device and System Security'

SuggestedRemedy

Change the title for IEEE Std. 2600 in the Normative References clause as indicated above.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **PP-C** SC **3.1** P **3** L **10** # **10**
 Sukert, Alan Xerox

Comment Type **E** Comment Status **D**

Typographical error: missing space on line 10 between 3.2 and and. Should read "...identified in clause 3.2 and which may..."

SuggestedRemedy

Correct as indicated above.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **PP-C** SC **3.2** P **3** L **14** # **11**
 Sukert, Alan Xerox

Comment Type **T** Comment Status **D**

As an example, the title page lists IEEE P2600.3 as the ""Draft Standard for a Protection Profile in Operational Environment C"" while page 3, line 14 indicates that P2600.3 is the ""Protection Profile for Hardcopy Devices, Operational Environment B"". We seem to be overloading the use of the P2600.3 designation.

I am concerned we may be creating some confusion as to what P2600.3 actually refers to because we are using the designation P2600.3 to represent both the Standard for a Protection Profile in Operational Environment C and the actual Protection Profile itself.

SuggestedRemedy

Eliminate the use of the P2600.3 designation to stand for both the Standard for the PP and the actual PP itself.

Note that what we decide to do here can have ripple effects on everywhere in the standard where P2600.3 is referenced. For example, see page 4, line 41.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

The PP should be referenced as P2600.3-PP (somewhat consistent with the references to SFR packages P2600.1-PRT, P2600.1-SCN, etc.).

Cl **PP-C** SC **5.1** P **5** L **19** # **22**
 Sukert, Alan Xerox

Comment Type **T** Comment Status **D**

Since the NVS SFR package is not included in PP-C it is not clear why nonvolatile storage is included as one of the TOE functions for Operational Environment C in subclause 5.1.

SuggestedRemedy

Remove the discussion of nonvolatile storage as a TOE function in subclause 5.1.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

IEEE P2600 Hardcopy Device and System Security Comments

CI **PP-C** SC 5.1 P 5 L 21 # 16
 Sukert, Alan Xerox

Comment Type **T** Comment Status **D**

There is an inconsistency between the statement of the shared-medium interface (SMI TOE function between subclause 5.1 and subclause 11.2 (page 28, line 19).

Subclause 5.1 says that SMI applies to ""transmitting and receiving documents and data between the HCD and external devices over communications media that are or can be shared by other users""; subclause 11.2 states that the SMI package applies to HCD products that ""transmit and receive data over a communications medium that are or can be shared by other users"". The key difference is that subclause 5.1 indicates SMI applies to both documents and data while subclause 11.2 indicates SMI applies only to data.

SuggestedRemedy

Make the statements for the SMI function consistent between subclauses 5.1 and 11.2.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

Change "documents and data" to "User Data or TSF Data" and change everywhere in the PP where similar text occurs.

CI **PP-C** SC 5.2 P 5 L 33 # 26
 Smithson, Brian Ricoh

Comment Type **E** Comment Status **D**

[NIAP] ""Users == Subjects"" conflicts with many CC concepts.

SuggestedRemedy

Change ""Users == Subjects"" to ""the Subject security attributes used in access control decisions are identical to the security attributes of the User that requested access"".

Proposed Response Response Status **W**

PROPOSED ACCEPT.

CI **PP-C** SC 5.2 P 6 L 8 # 6
 Sukert, Alan Xerox

Comment Type **E** Comment Status **D**

Grammatical error -- Lines 8 and 9 have ""There may be cases where User Data and TSF Data is generated outside of the TOE and transmitted to the TOE, as well as cases where User Data and TSF Data is generated and/or processed..."".

It should be ""There may be cases where User Data and TSF Data are generated outside of the TOE and transmitted to the TOE, as well as cases where User Data and TSF Data are generated and/or processed...""

SuggestedRemedy

Correct this sentence as indicated above.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

CI **PP-C** SC 5.3.2.1 P 7 L 13 # 12
 Sukert, Alan Xerox

Comment Type **T** Comment Status **D**

The definition of User Document Data in Table 3 deviates slightly from the corresponding definition of User Document Data in Annex A, page 47, line 19. Subclause 5.3.2.1 has ""information contained in a User's document in hardcopy or electronic form"" while Annex A has ""information contained in a User's document.""

SuggestedRemedy

Make the definition of User Document Data in subclause 5.3.2.1 consistent with the corresponding definition in Annex A.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

CI **PP-C** SC P 9 L 14 # 1
 aubry, carmen oce

Comment Type **T** Comment Status **D**

"Administrators authorize Users to use of functions of the TOE."
 Is it really required? I'm afraid that an evaluator might ask for user I&A in this case. Previously (35a) we had: "U.ANONYMOUS A User who is authorized to perform User Document Data processing functions of the TOE without identification and authentication."

SuggestedRemedy

Remove this security feature.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-C** SC **5.4** P **9** L **14** # **7**
 Sukert, Alan Xerox

Comment Type **E** Comment Status **D**
 Grammatical error - this line has ""Administrators authorize Users to use of functions of the TOE"". Should be something like ""Administrators authorize Users to use the functions of the TOE"" instead.

SuggestedRemedy
 Correct line as indicated above.

Proposed Response Response Status **W**
 PROPOSED ACCEPT.

Cl **PP-C** SC **6.4** P **10** L **23** # **8**
 Sukert, Alan Xerox

Comment Type **E** Comment Status **D**
 The acronyms 'PRT' and 'SMI' are used here but aren't defined until later in clause 11.3.

SuggestedRemedy
 Define the acronyms 'PRT' and 'SMI' when they are first used.

Proposed Response Response Status **W**
 PROPOSED ACCEPT.

Cl **PP-C** SC **7.2** P **11** L **11** # **27**
 Smithson, Brian Ricoh

Comment Type **T** Comment Status **D**
 [NIAP] P.CHANNEL.MANAGEMENT cannot be fulfilled by the TOE (at first, it was a circular definition; now it makes a policy that the TOE will be able to fulfill undefined TOE Owner policies).

SuggestedRemedy
 Change definition of P.CHANNEL.MANAGEMENT to ""To prevent unauthorized use of the input-output channels of the TOE, operation of the channels will be controlled by the TOE or its operating environment"". Access controls and OE's fulfill this in all cases except for when an SMI is present, and then FTP_ITP_EXP.1 is added.

Proposed Response Response Status **W**
 PROPOSED ACCEPT.

Cl **PP-C** SC **7.3** P **12** L **1** # **25**
 Smithson, Brian Ricoh

Comment Type **E** Comment Status **D**
 [NIAP] The administrator should also be trained and implement a secure configuration of these devices.

SuggestedRemedy
 Change A.ADMIN.TRAINING from ""...documentation to configure..."" to ""...documentation, and configure..."".

Change OE.ADMIN.TRAINED from ""...documentation to correctly..."" to ""...documentation, and correctly...""

Proposed Response Response Status **W**
 PROPOSED ACCEPT.

Cl **PP-C** SC **10.6** P **20** L **35** # **23**
 Smithson, Brian Ricoh

Comment Type **E** Comment Status **D**
 [NIAP] ""Nobody"" is a special term, but is not defined.

SuggestedRemedy
 Add a definition to the glossary: Nobody - a pseudo-role that cannot be assigned to any user.

Proposed Response Response Status **W**
 PROPOSED ACCEPT IN PRINCIPLE.

We will add a definition of "Nobody"

Cl **PP-C** SC **10.6** P **21** L **11** # **2**
 Chen, Nancy Oki Data

Comment Type **T** Comment Status **D**
 This App. Note states "The dependency on FDP_ACF.1", but in fact, this SFR does not depend on FDP_ACF.1.

SuggestedRemedy
 Remove this App. Note.

Proposed Response Response Status **W**
 PROPOSED ACCEPT.

Note to editor: sort this out.

IEEE P2600 Hardcopy Device and System Security Comments

CI **PP-C** SC 10.6 P 21 L 25 # 13
 Sukert, Alan Xerox

Comment Type **T** Comment Status **D**

The PP Application Note for FMT_MTD.1 indicates that FMT_MTD.1.1(b) applies to TSF data that is associated with a Normal User. In reading the actual SFR it indicates that the SFR applies to TSF data that is associated with a Normal User and to jobs owned by a Normal User.

SuggestedRemedy

Revise the PP Application Note for FMT_MTD.1 to indicate that FMT_MTD.1.1(b) applies to both TSF data that is associated with a Normal User and to jobs owned by a Normal User.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

CI **PP-C** SC 10.6 P 21 L 29 # 9
 Sukert, Alan Xerox

Comment Type **E** Comment Status **D**

Administrator is spelled incorrectly in subclause 10.6, page 21, lines 29 and 34.

SuggestedRemedy

Correct the spelling of administrator in the indicated lines.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

CI **PP-C** SC 10.6 P 21 L 36 # 14
 Sukert, Alan Xerox

Comment Type **T** Comment Status **D**

It is not clear why in this PP Application Note it states that FMT_MTD.1 is a principal SFR to "one or more" of the three objectives listed. Per Table 18 this SFR is a principal SFR for all three objectives, so why not just state it that way.

SuggestedRemedy

Revise this PP Application Note to read that FMT_MTD.1 is a principal SFR of the three objectives listed.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

CI **PP-C** SC 10.6 P 22 L 17 # 3
 Chen, Nancy Oki Data

Comment Type **T** Comment Status **D**

Depending on implementation, ""nobody"" may not be a role that need to have and be maintained.

SuggestedRemedy

Delete ""nobody"" from the SFR.

Proposed Response Response Status **W**

PROPOSED REJECT.

This is a pseudo role that will be defined

CI **PP-C** SC 10.6 P 22 L 17 # 24
 Smithson, Brian Ricoh

Comment Type **E** Comment Status **D**

The role ""Nobody"" is inconsistently capitalized.

SuggestedRemedy

Capitalize ""Nobody"" (multiple places).

Proposed Response Response Status **W**

PROPOSED ACCEPT.

CI **PP-C** SC 10.11 P 24 L 4 # 15
 Sukert, Alan Xerox

Comment Type **T** Comment Status **D**

It is not clear why the statement used to indicate that there are no FTP SFRs is different than the corresponding statement used for other classes. For FTP the statement is that ""There are no Class FTP security functional requirements among the Common Security Functional Requirements"" whereas, for example, for class FRU (subclause 10.9, page 23, line 27) the statement used is ""There are no Class FRU security functional requirements for this Protection Profile""

SuggestedRemedy

Use a consistent statement when indicating that a class has no SFRs that are used in the PP.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Use the statement:

"There are no Class FTP security functional requirements for this Protection Profile."

IEEE P2600 Hardcopy Device and System Security Comments

CI **PP-C** SC **12.2** P **30** L **9** # **28**
 Smithson, Brian Ricoh

Comment Type **T** Comment Status **D**

(1) Permission to execute functions like PRT, SCN, etc. is distributed among the SFR packages. This results in many redundant SFRs for establishing the access control rules and for managing them. (2) NIAP did not like to see distributed administrative functions in the old family of PPs approach, and we have partially duplicated that here. (3) There may be some implication that all TOEs must provide an administrative function that permits or denies each authorized user to execute each function, but in practice, some products will allow all authorized users to execute all available functions. Function-by-function administrative control is not one of the security objectives of the PP, so it should not be a requirement (even by implication).

SuggestedRemedy

Rewrite the access controls for function execution as proposed by Helmut Kurth (reference document <http://grouper.ieee.org/groups/2600/presentations/Comas2008/Function%20access%20control%20policy.doc>).

NOTE that this will make it unnecessary to have SFR packages for PRT, SCN, CPY, FAX, and DSR, in PP-C.

Proposed Response Response Status **W**
 PROPOSED ACCEPT.

We will use the SFRs to define the policy.

CI **PP-C** SC **12.3** P **31** L **21** # **17**
 Sukert, Alan Xerox

Comment Type **T** Comment Status **D**

The description for O.USER.AUTHORIZED in Table 23 is not consistent with the corresponding description for O.USER.AUTHORIZED in Table 18 (subclause 10.12, page 25, line 1). Table 23 states ""Authorization of Users and Administrators to use the TOE"" while Table 18 states ""Authorization of Normal Users and Administrators to use the TOE"". The two should be consistent.

A similar comment applies to Table 26 (subclause 13.3, page 33, line 21); Table 29 (subclause 14.3, page 35, line 19); Table 32 (subclause 15.3, page 37, line 21); Table 35 (subclause 16.3, page 39, line 19)

SuggestedRemedy

Make sure the description for O.USER.AUTHORIZED is consistent between Table 18 and Tables 23, 26, 29, 32, 35.

Proposed Response Response Status **W**
 PROPOSED ACCEPT.

(note that for PP-C, table 18 is correct)

CI **PP-C** SC **17.1** P **40** L **12** # **18**
 Sukert, Alan Xerox

Comment Type **T** Comment Status **D**

My understanding of SFR FMT_ITP_EXP.1.1 was that this was the requirement that will be used for ""bridging"" issues like assuring one can't use a FAX phone line to access the network.

If that is the case, then it is not clear why this requirement is written as it is. I would think that the requirement should be stated in terms of protecting user and TSF data received from a listed external interface (in the case of the Fax the PSTN) from being forwarded to a listed external interface (in the case of Fax the ""network""). Grammatically that doesn't appear to be what the current requirement is saying.

SuggestedRemedy

Revise SFR FMT_ITP_EXP.1.1 to read something like ""The TSF shall protect user and TSF data received on [assignment: list of external interfaces] from being directly forwarded to [assignment: list of external interfaces].""

Proposed Response Response Status **W**
 PROPOSED ACCEPT IN PRINCIPLE.

See #48

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-C** SC **17.5** P **42** L **16** # **4**
 Chen, Nancy Oki Data

Comment Type **T** Comment Status **D**

In FTP_ITC.1.3, the communication function does not specify which data (among D.CONF, D.PROT) must be protected from disclosure, which data must be protected from alteration.

SuggestedRemedy

For consistency with the security objectives, clarify the communication function to state which data must be protected from disclosure, which must be protected from modification.

Proposed Response Response Status **W**

PROPOSED REJECT.

Everything is protected (confidentiality & integrity) and therefore meets the objective. Breaking it up is not possible.

Cl **PP-C** SC **17.5** P **42** L **17** # **21**
 Sukert, Alan Xerox

Comment Type **T** Comment Status **D**

I noted that in PP-A the corresponding SFR FTC_ITC.1.3 included D.DOC and D.FUNC in the list of data entities for which a trusted channel should be used for communication over any shared-medium interface. In PP-C neither of these two entities were included.

SuggestedRemedy

Determine whether D.DOC and D.FUNC should be added to the list of data entities in SFR FTC_ITC.1.3 for which a trusted channel should be used for communication over any shared-medium interface.

Proposed Response Response Status **W**

PROPOSED REJECT.

Note to editor: Make sure this is consistent throughout PP-C.

Cl **PP-C** SC **17.6** P **43** L **1** # **19**
 Sukert, Alan Xerox

Comment Type **T** Comment Status **D**

The description for O.CHANNELS.MANAGED in Table 38 is not consistent with the corresponding description for O.CHANNELS.MANAGED in Table 18 (subclause 10.12, page 25, line 1). Table 38 states ""Authorization of Users and Administrators to use the TOE"" while Table 18 states ""Management of input-output channels"". The two should be consistent.

SuggestedRemedy

Make sure the description for O.CHANNELS.MANAGED is consistent between Table 18 and Table 38.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Fix cut and paste error

Cl **PP-C** SC **Annex B** P **48** L **5** # **20**
 Sukert, Alan Xerox

Comment Type **T** Comment Status **D**

For consistency with the other notational prefix conventions listed in Table 1 (subclause 1.4, page 2, line 6), the prefix 'F' standing for Function is not included in the list of acronyms in Annex B.

SuggestedRemedy

Add 'F' for Function to the list of acronyms in Annex B

Proposed Response Response Status **W**

PROPOSED ACCEPT.