

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-D** SC **5.2** P **5** L **18** # **21**
 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.

Cl **PP-D** SC **5.2** P **6** L **5** # **3**
 Sukert, Alan Xerox

Comment Type **E** Comment Status **D**
 Grammatical error -- Lines 5 and 6 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.

Cl **PP-D** SC **5.3.2** P **7** L **1** # **16**
 Sukert, Alan Xerox

Comment Type **T** Comment Status **D**
 There is no User Data that PP-D needs to protect. I wonder, however, if there still needs to be a User Data subclause which states that there is no User Data that needs to be protected (or some such wording).

SuggestedRemedy

Consider adding a User Data subclause as indicated above.

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

Cl **PP-D** SC **6.4** P **9** L **30** # **4**
 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-D** SC **7.2** P **10** L **10** # **22**
 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-D** SC **7.3** P **10** L **15** # **20**
 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.

IEEE P2600 Hardcopy Device and System Security Comments

CI **PP-D** SC **8.1** P **11** L **4** # **7**
 Sukert, Alan Xerox

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

In Table 8 there is a typo in the O.ADMIN.AUTHORIZED row - "...and shall ensure that Administratorsare authorized to..." should be "...and shall ensure that Administrators are authorized to..."

SuggestedRemedy

Correct as indicated above.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

CI **PP-D** SC **10.6** P **15** L **25** # **17**
 Sukert, Alan Xerox

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

FMT_MTD.1.1 is an altered SFR as defined in subclause 1.4, page 1, line 20 but the convention stated in subclause 1.4 for documenting altered SFRs was not followed in this case.

SuggestedRemedy

Define FMT_MTD.1.1 in subclause 10.6 using the proper convention for documenting an altered SFR defined in subclause 1.4.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

CI **PP-D** SC **10.6** P **15** L **27** # **18**
 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.

Add a definition of the pseudo-role "nobody"

CI **PP-D** SC **10.6** P **15** L **27** # **5**
 Sukert, Alan Xerox

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

Administrator is spelled incorrectly in subclause 10.6, page 15, line 27.

SuggestedRemedy

Correct the spelling of administrator in the indicated line.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

CI **PP-D** SC **10.6** P **15** L **29** # **9**
 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-D** SC **10.6** P **16** L **9** # **19**
 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.

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-D** SC **10.11** P **17** L **12** # **10**

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 17, line 2) 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."

Cl **PP-D** SC **12.1** P **21** L **12** # **12**

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 in A

Cl **PP-D** SC **12.4** P **22** L **15** # **1**

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-D** SC **12.4** P **22** L **16** # **15**

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-D 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-D

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-D** SC **12.5** P **23** L **1** # **13**
Sukert, Alan Xerox

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

The description for O.CHANNELS.MANAGED in Table 18 is not consistent with the corresponding description for O.CHANNELS.MANAGED in Table 14 (subclause 10.12, page 18, line 1). Table 18 states ""Authorization of Users and Administrators to use the TOE"" while Table 14 states ""Management of input-output channels"". The two should be consistent.

SuggestedRemedy

Make sure the description for O.CHANNELS.MANAGED is consistent between Table 14 and Table 18.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Fix cut and paste error

Cl **PP-D** SC **Annex B** P **28** L **5** # **14**
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.