

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-B** SC **2** P **2** L **20** # **4**
 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-B** 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-B** SC **3.2** P **3** L **14** # **12**
 Sukert, Alan Xerox

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

As an example, the title page lists IEEE P2600.2 as the ""Draft Standard for a Protection Profile in Operational Environment B"" while page 3, line 14 indicates that P2600.2 is the ""Protection Profile for Hardcopy Devices, Operational Environment B"". We seem to be overloading the use of the P2600.2 designation.

I am concerned we may be creating some confusion as to what P2600.2 actually refers to because we are using the designation P2600.2 to represent both the Standard for a Protection Profile in Operational Environment B and the actual Protection Profile itself.

SuggestedRemedy

Eliminate the use of the P2600.2 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 P2600.2 is referenced. For example, see page 4, line 41.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

The PP should be referenced as P2600.2-PP (somewhat consistent with the references to SFR packages P2600.1-PRT, P2600.1-SCN, etc.).

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-B** SC 5.1 P 5 L 20 # 21
 Sukert, Alan Xerox

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

There is an inconsistency between the statement of the nonvolatile storage TOE function between subclause 5.1 and subclause 11.2 (page 29, line 18).

Subclause 5.1 says that nonvolatile storage applies to ""persistent or temporary document storage on devices that could practicably be removed and analyzed when the HCD is powered off""; subclause 11.2 states that the NVS package applies to ""a storage device which can practicably be removed from the HCD by unauthorized people for analysis and recovery of deleted data"". There are two main areas where the two differ:

1. Does NVS apply to both persistent and temporary document storage as indicated in subclause 5.1 or not.
2. Does NVS apply just when the device is powered down as indicated in subclause 5.1 or when the device is powered up or powered down as implied in subclause 11.2.

SuggestedRemedy

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

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

Neither is correct, they should be consistent with 17.1

Cl **PP-B** SC 5.1 P 5 L 21 # 22
 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 29, line 30).

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.

(Should match resolution from PP-D)

Cl **PP-B** SC 5.2 P 5 L 33 # 35
 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-B** SC 5.2 P 6 L 8 # 5
 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.

(Should match resolution from PP-D)

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-B** SC **5.3.2.1** P **7** L **10** # **13**
 Sukert, Alan Xerox

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

The definition of User Document Data in Table 1 deviates slightly from the corresponding definition of User Document Data in Annex A, page 55, 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.

Use what is in Std-2600

Cl **PP-B** SC **5.4** P **9** L **12** # **33**
 Smithson, Brian Ricoh

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

Some statements in the PP make it impossible for HCDs with fax to receive incoming faxes from unidentified, unauthenticated, unauthorized users. However, this is the typical case for fax systems.

SuggestedRemedy

P9 L12 change bullet item to ""All Users that want to perform an access-controlled function or a management function are identified and authenticated, and are authorized before being granted permission to perform TOE functions other than those allowed for unauthenticated users.""

P13 table 10 change P.USER.AUTHORIZATION to ""The TOE shall require identification and authentication of Users, and shall ensure that Users are authorized in accordance with security policies before allowing them to use the functions of the TOE reserved for identified and authenticates users.""

P30 table 21: Change +FAX into two attributes, +FAXIN ""Indicates data that is associated with a fax job for faxes being received by the TOE"", and +FAXOUT ""Indicates data that is associated with a fax job for faxes being sent by the TOE"".

P40 L8 add an app note for the FAX package that says ""Typical fax systems allow unidentified, unauthenticated users outside of the TOE to send fax documents to the TOE. To allow this, the ST Author should consider adding fax reception to the list of TSF-mediated actions that are allowed in FIA_UAU.1.1 in the Common PP.""

P40 table 31 change the D.DOC rules as follows:

- +FAXIN Read U.ADMINISTRATOR Allowed
- +FAXOUT Create, Delete U.NORMAL Allowed for his/her own documents

P40 L11 add an app note ""For +FAXIN, the ""owner"" of an incoming fax job is considered to be U.ADMINISTRATOR. The ST Author may refine this role if a conforming TOE provides a specific role for fax administration.

P40 L11 add an app note ""If a conforming TOE provides a feature that allows an administrator to transfer ownership of an incoming fax job to one or more normal users -- typically, the intended recipients of the fax documents -- then the ST Author should consider adding a rule to the FAX Access Control SFP such as ""+FAXIN Read U.NORMAL Allowed if this User is authorized by U.ADMINISTRATOR"". Alternatively, the ST Author may define and use attributes for this purpose in the FAX Access Control SFP, provided that the initialization and management of such attributes are specified in such as in FMT_MSA.1 and FMT_MSA.3.""

P40 L11 replace the app note with ""For +FAXIN, ""Read"" refers (as a minimum) to the release of pending hardcopy output to a Hardcopy Output Handler or the retransmission of User Document Data through an Interface for faxes that have been received by the TOE. For +FAXIN and +FAXOUT, ""Read"" may also refer to previewing User Document Data on

IEEE P2600 Hardcopy Device and System Security Comments

CI **PP-B** SC **10.4** P **18** L **8** # **39**

Smithson, Brian

Ricoh

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

The access control SFPs give administrators various permissions for accessing user documents. For example, the common AC SFP allows admins to Delete, and the PRT AC SFP allows admin to Read. In practice, some administrative interfaces may not provide such access to admins, but other administrative interfaces may provide more access (e.g., Create or Modify). If an ST does not provide the access that we specify in the SFPs, then it would not be compliant. Administrator permissions for document access is not among the security objectives of the PP, and so it should not be specified.

SuggestedRemedy

(1) Remove D.DOC permissions for U.ADMINISTRATOR in the common AC SFP and in all SFR package AC SFPs.

(2) Change D.DOC permissions for U.NORMAL from ""Allowed for his/her own documents"" to ""Denied for documents that are not owned by that user"". (exception: DSR Read access should be ""Denied for documents that are not owned by that user, unless access to the document is permitted for this user by [assignment: the authorized identified roles]"")

(3) Add an app note which explains that the default rules ensure that a normal user cannot access another's documents, but the ST Author may add a rule that permits access to administrators.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

This is being addressed by the re-writing of the access control tables in terms of "deny" rather than "allow"

CI **PP-B** SC **10.4** P **18** L **11** # **14**

Sukert, Alan

Xerox

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

The PP Application Note on this line refers to Table 15. Since it is discussing the applicable SFPs I believe the table reference here should be to Table 16 instead.

A similar comment applies to the table reference in the PP Application Note on page 18, line 17.

SuggestedRemedy

Reference the proper table in these two PP Application Notes.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

CI **PP-B** SC **10.4** P **18** L **28** # **15**

Sukert, Alan

Xerox

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

The PP Application Note for FDP_ACC.1 indicates that this SFR is a dependency of FMT_MSA.1. For completeness it should be noted here that this SFR is also a dependency of FDP_ACF.1.

SuggestedRemedy

Indicate in this PP Application Note that FDP_ACC.1is also a dependency of FDP_ACF.1.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

CI **PP-B** SC **10.6** P **22** L **7** # **16**

Sukert, Alan

Xerox

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

In line with the conventions used elsewhere in Clause 10, since FMT_MSA.1.1 has been modified to specifically reference the Common Access Control SFP, you should use here the notational convention indicated for SFRs that have been altered (see clause 1.4, page 1, line 21)

A similar comment applies to FMT_MSA.3.1 (clause 10.6, page 22, line 23).

SuggestedRemedy

Define FMT_MSA.1.1 and FMT_MSA.3.1 as altered SFRs using the appropriate notational convention.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

CI **PP-B** SC **10.6** P **22** L **14** # **36**

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.

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-B** SC 10.6 P 23 L 6 # 17
 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.

Cl **PP-B** SC 10.6 P 23 L 10 # 8
 Sukert, Alan Xerox

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

Administrator is spelled incorrectly in subclause 10.6, page 23, lines 10 and 15.

SuggestedRemedy

Correct the spelling of administrator in the indicated lines.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **PP-B** SC 10.6 P 23 L 17 # 18
 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 objcyives, 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.

Cl **PP-B** SC 10.6 P 23 L 35 # 37
 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.

Cl **PP-B** SC 10.11 P 25 L 12 # 19
 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 25, 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."

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-B** SC **10.12** P **26** L **1** # **20**
 Sukert, Alan Xerox

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

I was curious why the purpose for FIA_UID.1 indicated for the O.DOC.NO_DIS / O.DOC.NO_ALT / O.FUNC.NO_ALT objectives (Supports security roles by requiring user identification) is different from the purpose indicated for the O.CONF.NO_DIS / O.PROT.NO_ALT / O.CONF.NO_ALT objectives (Supports access control and security roles by requiring user identification). I would think that the purpose would be the same in both cases since this SFR deals with user identification which would be needed in the same manner for both sets of objectives that doesn't directly deal with access control.

SuggestedRemedy

Make the purpose for FIA_UID.1 consistent within Table 19 for the NO_DIS and NO_ALT objectives.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Both should mention Access Controls.

Cl **PP-B** SC **11.2** P **29** L **21** # **23**
 Sukert, Alan Xerox

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

I am still concerned that the NVS package only applies to data stored on removable NVS devices. First of all there still is no clear definition of what NVS devices this applies to, especially given the inconsistency between subclauses 5.1 and 11.2 regarding the NVS function defined in an earlier comment. Second, we still don't have a clear definition of what constitutes a ""removable"" NVS device in this context - does it apply only to an NVS device which it is designed to be removed; does it apply to an NVS device which can easily be removed but which is not designed specifically to be removable; etc.

Most importantly the threat to NVS applies equally whether the NVS device is designed to be removable or not - we want to protect data stored in an NVS device whether it is located in the TOE or removed from the TOE from unauthorized disclosure or alteration.

SuggestedRemedy

Change the NVS package to apply to NVS devices whether or not they are a ""removable NVS device"".

Proposed Response Response Status **W**

PROPOSED REJECT.

This comment was WITHDRAWN by the commenter.

Cl **PP-B** SC **12.2** P **31** L **9** # **38**
 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/Camas2008/Function%20access%20control%20policy.doc>).

Proposed Response Response Status **W**

PROPOSED ACCEPT.

We will use the SFRs to define the policy.

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-B** SC **12.2** P **31** L **10** # **32**
 Smithson, Brian Ricoh

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

The requirement for local authentication before retrieving hardcopy output ("PIN printing") should not have been made using FIA_UAU.6. FIA_UAU.6 is for re-authentication on the same Interface. The requirement is actually for authentication on a different interface. Therefore, it should be covered by the existing FIA_UAU.1. However, it may not be clear that the requirement local authentication is required when a user has submitted a print job from a non-local interface.

SuggestedRemedy

P31 L13 add an app note "A User will need to authenticate on using the operator controls on the TOE to perform "Read" operations. If the User authenticated using operator controls when submitting a print job, and that session is still active, then re-authentication is not necessary. However, if that session is no longer active or the User authenticated and submitted the print job over a different Interface, then the User will need to authenticate using operator controls in order to establish a new session before being permitted to perform the "Read" operation."

Remove FIA_UAU.6 from PRT package.

Remove FIA_UAU.6 from tables 23 and 24.

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

Cl **PP-B** SC **12.4** P **33** L **7** # **24**
 Sukert, Alan Xerox

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

The description for O.USER.AUTHORIZED in Table 24 is not consistent with the corresponding description for O.USER.AUTHORIZED in Table 19 (subclause 10.12, page 27, line 1). Table 24 states "Authorization of Users and Administrators to use the TOE" while Table 19 states "Authorization of Normal Users and Administrators to use the TOE". The two should be consistent.

A similar comment applies to Table 27 (subclause 13.4, page 36, line 1); Table 30 (subclause 14.4, page 39, line 1); Table 33 (subclause 15.4, page 42, line 1); Table 36 (subclause 16.4, page 45, line 2)

SuggestedRemedy

Make sure the description for O.USER.AUTHORIZED is consistent between Table 19 and Tables 24, 27, 30, 33, 36.

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

table 19 is correct

Cl **PP-B** SC **15.2** P **40** L **10** # **43**
 Smithson, Brian Ricoh

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

[NIAP] transmission through an interface should be a "write" operation.

SuggestedRemedy

Modify rules to the FAX SFP as follows:

U.NORMAL: Create, Read, Delete.

Change app note on line 11 to say:

öReadö refers (as a minimum) to the release of pending hardcopy output to a Hardcopy Output Handler for receiving faxes and to the transmission of User Document Data through an Interface for receiving faxes. "Create" refers (as a minimum) to submission of User Document Data to be sent and implies transmission of User Document Dat through an Interface for delivering the fax. "Read" may also be used to refer to previewing documents on a display device, if such a feature is present in a conforming TOE."

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

Cl **PP-B** SC **16.2** P **43** L **9** # **1**
 Chen, Nancy Oki Data

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

In Table 34 DSR Access Control SFP, the very last D.DOC's "Read" rule for U.NORMAL, the statement "à or by another authorized user for that user's own document" is redundant." Because the previous "Read" rule for U.NORMAL already states that "allowed for his/her own document".

SuggestedRemedy

Delete "or by another authorized user for that user's own document" from this "Read" SFP.

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

the rule is unclear, but not redundant. It would be more clear to say "Allowed for another User's document if this user is authorized by . . ."

This will be fixed in the rewrite of the Access Control Tables

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-B** SC 16.2 P 43 L 9 # 40
 Smithson, Brian Ricoh

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

The DSR AC SFP does not allow a user to store a document.

SuggestedRemedy

Add a rule D.DOC / +DSR / Create / U.NORMAL / Allowed if this user is authorized to execute the DSR function.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **PP-B** SC 17 P 46 L 1 # 2
 Chen, Nancy Oki Data

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

Since there is no common baseline requirement for protection of data stored on "removable non-volatile storage", it should be ST author's responsibility to describe their customer's specific requirements for protection of data store on removable NVS.

SuggestedRemedy

Remove NVS SFR package.

Proposed Response Response Status **W**

PROPOSED REJECT.

As per our previous discussion with Helmut this will remain.

Cl **PP-B** SC 17.1 P 46 L 9 # 27
 Sukert, Alan Xerox

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

It is not clear why removable NVS is designed to be removed by only authorized non-service personnel. You would certainly want service personnel to be able to remove any removable NVS which seems to be excluded by the current definition.

SuggestedRemedy

Change the definition to read "...is designed to be removed from the TOE by authorized personnel." This would include both service and non-service personnel.

Proposed Response Response Status **W**

PROPOSED REJECT.

it was not the intention to prohibit service personnel from removing devices, but we do not want to include (in NVS protection) devices that are designed for servicing but not for end-user removal. The current definition does not prohibit service personnel from removing devices.

Cl **PP-B** SC 17.1 P 46 L 14 # 41
 Smithson, Brian Ricoh

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

It was not the original intention of the NVS package to protect integrity of data; the driving customer requirement is only to protect confidentiality. However, the common PP has objectives for protecting integrity of user and TSF data.

SuggestedRemedy

- (1) In the common PP:
 - (a) Add an OSP P.OFFLINE.CONFIDENTIALITY "To preserve data confidentiality, the TOE will protect confidential data from unauthorized disclosure when the TOE is not operating".
 - (b) In the objectives rationale table, add P.OFFLINE.CONFIDENTIALITY and link it to OE.PHYSICAL.MANAGED.

- (2) In the NVS package:
 - (a) Remove "and integrity" from page 46 line 14.
 - (b) Change the name and designation of FTP_CIP_EXP.1 to FTP_CP.EXP.1 "Confidentiality of Stored Data".
 - (c) Remove "and integrity" from FTP_CIP_EXP.1.1.
 - (d) Remove FTP_CIP_EXP.1.2 and FTP_CIP_EXP.1.3.
 - (e) Remove app note on page 47 line 9.
 - (f) Remove the "NO_ALT" objectives from app note on page 47 line 12, and from tables 37 and 38.
 - (g) Remove "or alteration" from table 38.

Proposed Response Response Status **W**

PROPOSED REJECT.

This comment was WITHDRAWN by the commenter.

Cl **PP-B** SC 17.1 P 46 L 15 # 9
 Sukert, Alan Xerox

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

grammatical error: the line states "...preserved even in the case of an attacker that analyzes this the content...". Should be "...preserved even in the case of an attacker that analyzes the content...".

SuggestedRemedy

Correct the line as indicated above.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-B** SC 17.2 P 46 L 27 # 25

Sukert, Alan Xerox

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

Not clear for extended SFR FTP_CIP_EXP.1.3 why the requirement only applies to detecting errors validating just the integrity of user and TSF data; wouldn't you also want to detect errors validating that confidentiality of user and TSF data hasn't been compromised.

Same comment applies to subclause 17.3, page 47, line 8.

SuggestedRemedy

Revise FTP_CIP_EXP.1.3 to read ""The TSF shall perform [assignment: list of actions] when it detects an error when validating the confidentiality and integrity of user and TSF data.""

Proposed Response Response Status **W**

PROPOSED REJECT.

how do you detect that confidentiality has been compromised?

Cl **PP-B** SC 17.4 P 47 L 23 # 11

Sukert, Alan Xerox

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

Some extra ""Table 38"" lines got included that need to be removed.

SuggestedRemedy

Remove the extra ""Table 38"" lines.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

(In Change Bar version only)

Cl **PP-B** SC 18.1 P 48 L 13 # 28

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

Cl **PP-B** SC 18.5 P 50 L 16 # 3

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 being consistent with the security objectives, clarify the communication function to state which data are protected from disclosure, which are 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.

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-B** SC **18.5** P **50** L **17** # **31**
 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-B 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-B.

Cl **PP-B** SC **18.6** P **51** L **1** # **29**
 Sukert, Alan Xerox

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

The description for O.CHANNELS.MANAGED in Table 41 is not consistent with the corresponding description for O.CHANNELS.MANAGED in Table 19 (subclause 10.12, page 27, line 1). Table 41 states ""Authorization of Users and Administrators to use the TOE"" while Table 19 states ""Management of input-output channels"". The two should be consistent.

SuggestedRemedy

Make sure the description for O.CHANNELS.MANAGED is consistent between Table 19 and Table 41.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Table 19 is correct

Cl **PP-B** SC **Annex A** P **53** L **1** # **26**
 Sukert, Alan Xerox

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

If the NVS package is going to revolve around removable nonvolatile storage device, the definition of such a device that is included in subclause 17.1 needs to be added to Annex A.

SuggestedRemedy

Add the following definition to Annex A:

Removable nonvolatile storage: nonvolatile storage that is part of an evaluated TOE but is designed to be removed from the TOE by authorized personnel. See also Nonvolatile storage.

Note that this includes resolution of a previous comment about authorized personnel.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **PP-B** SC **Annex B** P **56** L **5** # **30**
 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 8), 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.