

IEEE P2600 Hardcopy Device and System Security comments

Cl All P SC P L # 2
 Chen, Nancy Oki Data

Comment Type T Comment Status D

There should be two types of "+delegate" attribute defined - one is the "+delegate" of Owner / Originator, the other one is that of Administrator. The delegate of Owner/Originator can only read/modify/delete the assets created by the Owner/Originator. The delegate of an Administrator can read/modify/delete all user's assets. These two different type of delegates must be distinguished.

SuggestedRemedy

- (1) Create two different notations and define two different "+delegates" attributes - one for Owner, one for Administrator.
- (2) Change the "+delegates" attributes accordingly in all Access Control SFP rules for PRT, SCN, CPY, FAX, DSR, NVS TOES.

Proposed Response Response Status W

PROPOSED ACCEPT IN PRINCIPLE.

Implement as per P2600.1-35-proto plus changes discussed during the meeting to

- 1) Make it clear that an administrator can also delegate
- 2) The definition of DELEGATES in the glossary can include both cases
- 3) Consistently use "who submitted the job" rather than that plus "who submitted user document data."

Cl All P SC 13,5,6 P 150 L 15 # 6
 Smithson, Brian Ricoh

Comment Type T Comment Status D

is FIA_UAU.7_really_ a principal SFR for fulfilling O.*.AUTHORIZED?

SuggestedRemedy

consider at meeting and change if needed

Proposed Response Response Status W

PROPOSED ACCEPT.

Make it a supporting SFR

Cl All P SC 13.5.6 P 150 L 15 # 5
 Smithson, Brian Ricoh

Comment Type T Comment Status D

FIA_UAU.7 app note in SMI: should say that it also fulfills O.USER.AUTHORIZED

SuggestedRemedy

add the appropriate text

Proposed Response Response Status W

PROPOSED ACCEPT.

Cl All P SC 13.5.7 P 151 L 17 # 4
 Smithson, Brian Ricoh

Comment Type T Comment Status D

there is no FDP_ACF.1 in SMI

SuggestedRemedy

remove refs to FDP_ACF.1 (app notes in MSA.1 and MSA.3, check elsewhere)

Proposed Response Response Status W

PROPOSED ACCEPT.

Cl All P SC 13.6 P 159 L 1 # 8
 Smithson, Brian Ricoh

Comment Type T Comment Status D

Sufficiency table rows for O.USER.AUTHORIZED and O.ADMIN.AUTHORIZED should be combined in the SMI TOE (as in other TOEs). Note that the entry for O.USER.AUTHORIZED is incorrect.

SuggestedRemedy

Combine O.USER.AUTHORIZED and O.ADMIN.AUTHORIZED, using data in O.ADMIN.AUTHORIZED.

Proposed Response Response Status W

PROPOSED ACCEPT.

IEEE P2600 Hardcopy Device and System Security comments

Cl All P SC 5.5.1 P 8 L 5 # 10
 Smithson, Brian Ricoh

Comment Type T Comment Status D

""Delegate"" is overused as both a User class and as an attribute. It should really be an attribute. ""Originator"" is then too specific -- an authorized non-administrative user could actually be a recipient (of FAX or DSR output, or even PRT output that was submitted by another). Therefore, the name should be changed to simply distinguish it from Administrator.

SuggestedRemedy

Proposal: Change U.ORIGINATOR (and similar references) to U.NORMAL. Remove U.DELEGATE and refer instead to U.NORMAL(+Delegate). Change model diagrams, tables, and all references, as needed. Change definition of Delegate to refer to attribute. Remove definition of Originator and create a new one for Normal user. Also consider changing policies and objectives that refer to ".USER." to ".NORMAL.", or perhaps just combine the ".USER." and ".ADMIN." policies and objectives into a single policy/objective for all applicable users (but this may have an effect on the approved std 2600).

Proposed Response Response Status W

PROPOSED ACCEPT IN PRINCIPLE.

Same as comment #2

Also change definition of +Remote in table 2 to say "user has bound to the TOE through a SHARED MEDIA INTERFACE."

Cl All P SC 7.5.11 P 19 L 9 # 11
 Smithson, Brian Ricoh

Comment Type T Comment Status D

PP-C and PP-D SFPs for D.FUNC.REST: rule is missing in PRT and DSR, and it should allow create, read, modify, delete for U.USER for PRT/SCN/CPY/FAX/DSR

SuggestedRemedy

add that rule, see PP-A for example.

Proposed Response Response Status W

PROPOSED ACCEPT IN PRINCIPLE.

PP-C

D.FUNC.REST is not protected in PP-C and so there should be no references to it anywhere:

Figure 4 (object diagram): remove User Function Data / Rest from the tree

SCN TOE: remove D.FUNC.REST from table 29 (SFP)

FAX TOE: remove D.FUNC.REST from table 43 (SFP)

DSR TOE: remove D.FUNC.REST from table 57 (SFP)

However, D.DOC.TRANSIT and D.FUNC.TRANSIT must be defined because they should be used in the SMI information flow control SFP. But they aren't.

See PP-D for how these changes would be implemented:

Figure 4 (object diagram): add User Document Data / Transit

Table 4 (object definitions): add D.DOC.TRANSIT and D.FUNC.TRANSIT

Figure 18 (SMI TOE model): add User Data +OtherTOE / Transit (this one is not in PP-D, see below)

New table, insert before Table 93: User Data assets of the SMI TOE

Table 103 (SMI Information Flow Control SFP): add both D.DOC.TRANSIT and D.FUNC.TRANSIT to the first two rows

Also noticed: Figure 5 (operations) should be updated, like in the other PPs.

PP-D

IEEE P2600 Hardcopy Device and System Security comments

Has one problem:

Figure 17 (SMI TOE model): add User Data +OtherTOE / Transit

Cl **All P** SC **7.5.7** P **28** L **27** # **9**
 Smithson, Brian Ricoh
 Comment Type **T** Comment Status **D**
 FMT_MSA.1.1(b) and (d) seem to imply a requirement that an originator must be able to modify the Delegate attribute, but not all implementations may have that function and it is not required that they do.
 SuggestedRemedy
 changed to ""selection: originator, nobody""
 Proposed Response Response Status **W**
 PROPOSED ACCEPT IN PRINCIPLE.
 Put all three (administrator, originator and nobody) in one selection statement.

Cl **All P** SC **7.6** P **33** L **20** # **7**
 Smithson, Brian Ricoh
 Comment Type **T** Comment Status **D**
 FAU_SAR.2 is a principal SFR but is marked in this Completeness table (and others) as supporting.
 SuggestedRemedy
 Change it to indicate that it is principal.
 Proposed Response Response Status **W**
 PROPOSED ACCEPT.

Cl **PP-A** SC **13.5.12** P **154** L **2** # **3**
 Shigeru, Ueda Canon

Comment Type **T** Comment Status **D**
 P2600.1-SMI requests to establish trusted pass between TSF and remote IT products such as PC or various type of servers in order for User data and/or TSF data not to be disclosed nor altered. FTP_TRP is assigned for it. FTP_TRP is the SFR which defines the requirements to establish and maintain trusted communication to or from users and the TSF. From implementation point of view, I believe many vendors will use IPsec for this requirement because it is one of the most appropriate protocol for this purpose. However, IPsec does not establish trusted pass between TSF and remote users but establish TSF and Remote IT products because there is no mechanism in IPsec to identify remote users. So I think IPsec does not fit to FTP TRP.1. It is the problem from implementation point of view. On the other hand, FTP_ITC.1 is the SFP which defines requirements for the creation of a trusted channel between the TSF and other trusted IT products. That means that FTP_ITC.1 fits well to IPsec. Also FTP_ITC.1 does not have any dependencies to other SFRs.

SuggestedRemedy
 Change FTP_TRP.1 to FTP_ITC.1

Proposed Response Response Status **W**
 PROPOSED REJECT.

It is not necessary to identify the remote user on the other end of the IPsec pipe using IPsec. It is sufficient that you can identify the IT MACHINE on the other end of the IPsec pipe. Once the path between the HCD and the other piece of IT equipment has been established and secured, the USER can be authenticated over that trusted path.

In addition, according to CC V3.1, FTP_ITC.1 is specified for security critical operations while FTP_TRP.1 is for other security relevant interactions.

Cl **PP-A** SC **13.5.5** P **149** L **17** # **21**
 Sukert, Alan Xerox

Comment Type **E** Comment Status **D**
 The APP Note says that PP APPLICATION NOTE FDP_IFF.1 is one of the dependencies of FDP_IFC.1. In fact it is the only dependency of FDP_IFC.1, so it would be more correct if this APP Note said that FDP_IFF.1 is the dependency of FDP_IFC.1.

SuggestedRemedy
 Consider updating the indicated App Note as indicated above.

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

Use "a dependency"

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-A** SC **13.5.7** P **151** L **2** # **20**
 Sukert, Alan Xerox

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

It is not clear for the SMI TOE why FMT_MSA.1 was not broken down into separate FMT_MSA.1(a) & (b) SFRs covering management of the security attributes for the D.PROT.REST and D.CONF.REST objects individually and for the SMI Access Control SFP as was done for the five previous TOEs in this PP.

SuggestedRemedy

Treat FMT_MSA.1 in the SMI TOE the same way this SFR is treated in the other five TOEs in PP-A.

Proposed Response Response Status **W**

PROPOSED REJECT.

It is not broken down into separate ones because for those two objects there are no attributes associated with them.

Cl **PP-A** SC **5.5.3** P **10** L **14** # **12**
 Sukert, Alan Xerox

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

Figure 4 still uses the term 'delegates' in defining the attributes of assets. It appears that in the rest of the document 'delegates' was changed to 'delegates'; this same change should be made in Figure 4 also.

SuggestedRemedy

Change 'delegates' to 'delegates' in Figure 4.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **PP-A** SC **5.5.3** P **10** L **14** # **1**
 Chen, Nancy Oki Data

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

The ""+delegates"" attribute of Asset in Figure 4 should be consistent with its definition in Table 5.

SuggestedRemedy

Change ""+delegates"" to ""delegates""

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Same as comment #12 (Sukert).

Cl **PP-A** SC **5.5.3** P **12** L **14** # **14**
 Sukert, Alan Xerox

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

Table 6 uses the acronym SNMP. However, this acronym is not defined in Annex B.

SuggestedRemedy

Include the definition of SNMP in Annex B.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Spell out on first use.

Cl **PP-A** SC **7.1.1** P **15** L **21** # **17**
 Sukert, Alan Xerox

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

The discussion of PRT TOE model in this subclause mentions that the Administrator has the ability to retrieve, modify and store TSF protected and confidential data. There are two issues that I note:

1. In subclause 5.5.4 the operations defined for objects are read, create, modify and delete. I can relate retrieve to the "read" operation and modify to the "modify" operation, but neither the "create" nor "delete" operations relate to the concept of storing data. Either some note that relates store to the allowable operations is needed or a "store" operation for objects is needed.
2. In the PRT Access Control SFP in subclause 7.5.1.1 (Table 17) it indicates that for TSF protected data the Administrator can "create", "modify" and "delete" while for TSF confidential data the Administrator can do all four operations; this seems inconsistent with subclause 7.1.1 where the Administrator appears to be able to do all operations for both TSF confidential and TSF protected data.

The same comment applies to each of the other six TOEs that are included in PP-A.

SuggestedRemedy

Resolve the apparent inconsistencies among the various subclauses in each TOE as to what operations an administrator can perform on TSF protected and confidential data.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

PART 1: In the TOE models such as 7.1.1., change them to the same operations as defined in 5.5.4.

PART 2: 7.5.1.1. is correct as is.

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-A** SC **7.5.2** P **24** L **1** # **15**
 Sukert, Alan Xerox

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

The PP APP Note here says that FAU_GEN.1 is a principal SFR that directly fulfills O.USER.AUTHORIZED and O.ADMIN.AUTHORIZED. However, this is not shown in Table 21 on page 33 (there is no 'P' for FAU_GEN.1 for either of these two objectives).

A similar comment applies to subclause 8.5.2, page 45, line 9 vs. Table 37; subclause 9.5.2, page 65, line 9 vs. Table 53; subclause 10.5.2, page 85, line 22 vs. Table 69; subclause 11.5.2, page 107, line 1 vs. Table 85; subclause 12.5.2, page 126, line 10 vs. Table 101 (note that only O.USER.AUTHORIZED is mentioned in 12.5.2) and subclause 13.5.2, page 146, line 4 vs. Table 119.

SuggestedRemedy

Make the indicated App Notes and corresponding tables consistent in terms of what objectives FAU_GEN.1 fulfills.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

The app note should say it fulfills O.AUDIT.LOGGED and not O.*.AUTHORIZED.

Cl **PP-A** SC **7.5.2** P **24** L **26** # **16**
 Sukert, Alan Xerox

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

The APP Note says that FAU_SAR.1 is one of the dependencies of FAU_SAR.2. In fact it is the only dependency of FAU_SAR.2, so it would be more correct if this APP Note said that FAU_SAR.1 is the dependency of FAU_SAR.2.

This same comment applies to subclause 8.5.2, page 46, line 11; subclause 9.5.2, page 66, line 11; subclause 10.5.2, page 86, line 24; subclause 11.5.2, page 107, line 26; subclause 12.5.2, page 127, line 11 and subclause 13.5.2, page 147, line 11.

SuggestedRemedy

Consider updating the indicated App Notes as indicated above.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Use "a dependency"

Cl **PP-A** SC **7.5.5** P **26** L **29** # **18**
 Sukert, Alan Xerox

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

The APP Note says that FDP_ACF.1 is one of the dependencies of FDP_ACC.1. In fact it is the only dependency of FDP_ACC.1, so it would be more correct if this APP Note said that FDP_ACF.1 is the dependency of FDP_ACC.1.

This same comment applies to subclause 8.5.5, page 48, line 10; subclause 9.5.5, page 68, line 10; subclause 10.5.5, page 88, line 29 and subclause 11.5.5, page 109, line 28.

SuggestedRemedy

Consider updating the indicated App Notes as indicated above.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Use "a dependency"

Cl **PP-A** SC **7.5.7** P **28** L **25** # **19**
 Sukert, Alan Xerox

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

In the decription of the SFRs iterations of FMT_MSA.1 (in the case of the PRT TOE they are MT_MSA.1 (a) - FMT_MSA.1 (f), for example) the identical two AppNotes appear for each SFR:

PP APPLICATION NOTE FMT_MSA.1 is one of the dependencies of FMT_MSA.3
 PP APPLICATION NOTE FMT_MSA.1 performs management functions that are recommended for FDP_ACF.1

If the two notes are identical for each SFR then they should appear only one time; otherwise the two AppNotes associated with each of these six SFRs whould be modified to address that particular SFR as in the following for FMT_MSA.1 (a):
 PP APPLICATION NOTE FMT_MSA.1(a) is one of the dependencies of FMT_MSA.3
 PP APPLICATION NOTE FMT_MSA.1(a) performs management functions that are recommended for FDP_ACF.1.

The same comment applies to subclause 8.5.7, page 49, line 29; subclause 9.5.7, page 69, line 29; subclause 10.5.7, page 90, line 12 and subclause 11.5.7, page 111, line 9.

SuggestedRemedy

Determine how to handle the identical two APPNotes for the multiple iterations of SFR FMT_MSA.1 in the various TOEs in PP-A.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Repeat the App Note but indicate the iteration letter.

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-A** SC **7.5.7** P **29** L **1** # **22**
 Sukert, Alan Xerox

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

The APP Note says that FMT_MSA.1 is one of the dependencies of FMT_MSA.3. In fact it is the only dependency of FMT_MSA.3, so it would be more correct if this APP Note said that FMT_MSA.1 is the dependency of FMT_MSA.3.

This same comment applies to subclause 8.5.7, page 50, line 4; subclause 9.5.7, page 70, line 4; subclause 10.5.7, page 90, line 25 and subclause 11.5.7, page 114, line 4 and subclause 13.5.7, page 151, line 16.

Note: This comment should be addressed in connection with the comment on the multiple duplicate App Notes for subclause 7.5.7.

SuggestedRemedy

Consider updating the indicated App Notes as indicated above.

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

Use "a dependency"

Cl **PP-A** SC **7.5.9** P **32** L **20** # **23**
 Sukert, Alan Xerox

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

The APP Note says FPT_STM.1 is one of the dependencies of FAU_GEN.1. In fact it is the only dependency of FAU_GEN.1, so it would be more correct if this APP Note said that FPT_STM.1 is the dependency of FAU_GEN.1.

This same comment applies to subclause 8.5.9, page 53, line 6; subclause 9.5.9, page 73, line 6; subclause 10.5.9, page 94, line 16; subclause 11.5.9, page 115, line 16; subclause 12.5.9, page 132, line 15 and subclause 13.5.9, page 153, line 8.

SuggestedRemedy

Consider updating the indicated App Notes as indicated above.

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

Use "a dependency"

Cl **PP-A** SC **Keywords** P **ii** L **11** # **13**
 Sukert, Alan Xerox

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

Among the keywords listed for PP-A is "NIC". I noted that outside of the keyword list it is not used anywhere else in the document. Also, the acronym "NIC" is not defined in Annex B.

Note that this keyword also appears in subclause 4, page 5, line 3.

SuggestedRemedy

Either include NIC in Annex B or remove it from the list of keywords for PP-A.

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

Remove NIC.

Cl **PP-B** SC **13.5.5** P **146** L **34** # **34**
 Sukert, Alan Xerox

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

The APP Note says that PP APPLICATION NOTE FDP_IFF.1 is one of the dependencies of FDP_IFC.1. In fact it is the only dependency of FDP_IFC.1, so it would be more correct if this APP Note said that FDP_IFF.1 is the dependency of FDP_IFC.1.

SuggestedRemedy

Consider updating the indicated App Note as indicated above.

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

Use "a dependency"

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-B** SC **13.5.7** P **148** L **20** # **33**
 Sukert, Alan Xerox

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

It is not clear for the SMI TOE why FMT_MSA.1 was not broken down into separate FMT_MSA.1(a) & (b) SFRs covering management of the security attributes for the D.PROT.REST and D.CONF.REST objects individually and for the SMI Access Control SFP as was done for the five previous TOEs in this PP.

SuggestedRemedy

Treat FMT_MSA.1 in the SMI TOE the same way this SFR is treated in the other five TOEs in PP-B.

Proposed Response Response Status **W**

PROPOSED REJECT.

Same as #20

Cl **PP-B** SC **14** P **157** L **2** # **26**
 Sukert, Alan Xerox

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

Table 120 for the P2600.2 Security Assurance Requirements references some incorrect SARs for EAL2 as follows:

Class	Component Listed	Correct Component
ADV	ADV_FSP.3	ADV_FSP.2
ADV	ADV_TDS.2	ADV_TDS.1
ALC	ALC_CMC.3	ALC_CMC.2
ALC	ALC_CMS.3	ALC_CMS.2
ALC	ALC_DVS.1	Not in EAL2
ALC	ALC_LCD.1	Not in EAL2
ATE	ATE_COV.2	ATE_COV.1
ATE	ATE_DPT.1	Not in EAL2

SuggestedRemedy

Include the correct SARs for EAL3 in Table 120.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **PP-B** SC **5.5.3** P **10** L **12** # **25**
 Sukert, Alan Xerox

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

Figure 4 still uses the term 'delegates' in defining the attributes of assets. It appears that in the rest of the document 'delegates' was changed to 'delegates'; this same change should be made in Figure 4 also.

SuggestedRemedy

Change 'delegates' to 'delegates' in Figure 4.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Same as #12

Cl **PP-B** SC **5.5.3** P **12** L **14** # **27**
 Sukert, Alan Xerox

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

Table 6 uses the acronym SNMP. However, this acronym is not defined in Annex B.

SuggestedRemedy

Include the definition of SNMP in Annex B.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Same as #14

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-B** SC 7.1.1 P 15 L 21 # 30
 Sukert, Alan Xerox

Comment Type T Comment Status D

The discussion of PRT TOE model in this subclause mentions that the Administrator has the ability to retrieve, modify and store TSF protected and confidential data. There are two issues that I note:

1. In subclause 5.5.4 the operations defined for objects are read, create, modify and delete. I can relate retrieve to the ""read"" operation and modify to the ""modify"" operation, but neither the ""create"" nor ""delete"" operations relate to the concept of storing data. Either some note that relates store to the allowable operations is needed or a ""store"" operation for objects is needed.
2. In the PRT Access Control SFP in subclause 7.5.1.1 (Table 17) it indicates that for TSF protected data the Administrator can ""create"", ""modify"" and ""delete"" while for TSF confidential data the Administrator can do all four operations; this seems inconsistent with subclause 7.1.1 where the Administrator appears to be able to do all operations for both TSF confidential and TSF protected data.

The same comment applies to each of the other six TOEs that are included in PP-B.

SuggestedRemedy

Resolve the apparent inconsistencies among the various subclauses in each TOE as to what operations an administrator can perform on TSF protected and confidential data.

Proposed Response Response Status W
 PROPOSED ACCEPT IN PRINCIPLE.

Same as #17

Cl **PP-B** SC 7.5.2 P 23 L 22 # 28
 Sukert, Alan Xerox

Comment Type T Comment Status D

The PP APP Note here says that FAU_GEN.1 is a principal SFR that directly fulfills O.USER.AUTHORIZED and O.ADMIN.AUTHORIZED. However, this is not shown in Table 21 on page 33 (there is no 'P' for FAU_GEN.1 for either of these two objectives).

A similar comment applies to subclause 8.5.2, page 44, line 7 vs. Table 37; subclause 9.5.2, page 63, line 7 vs. Table 53; subclause 10.5.2, page 83, line 27 vs. Table 69; subclause 11.5.2, page 104, line 22 vs. Table 85; subclause 12.5.2, page 124, line 9 vs. Table 101 (note that only O.USER.AUTHORIZED is mentioned in 12.5.2) and subclause 13.5.2, page 144, line 2 vs. Table 118.

SuggestedRemedy

Make the indicated App Notes and corresponding tables consistent in terms of what objectives FAU_GEN.1 fulfills.

Proposed Response Response Status W
 PROPOSED ACCEPT.

Same as #15

Cl **PP-B** SC 7.5.2 P 24 L 17 # 29
 Sukert, Alan Xerox

Comment Type E Comment Status D

The APP Note says that FAU_SAR.1 is one of the dependencies of FAU_SAR.2. In fact it is the only dependency of FAU_SAR.2, so it would be more correct if this APP Note said that FAU_SAR.1 is the dependency of FAU_SAR.2.

This same comment applies to subclause 8.5.2, page 45, line 3; subclause 9.5.2, page 64, line 3; subclause 10.5.2, page 84, line 21; subclause 11.5.2, page 105, line 17; subclause 12.5.2, page 125, line 6 and subclause 13.5.2, page 144, line 26.

SuggestedRemedy

Consider updating the indicated App Notes as indicated above.

Proposed Response Response Status W
 PROPOSED ACCEPT.

Use "a dependency"

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-B** SC **7.5.5** P **24** L **17** # **31**
 Sukert, Alan Xerox

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

The APP Note says that FDP_ACF.1 is one of the dependencies of FDP_ACC.1. In fact it is the only dependency of FDP_ACC.1, so it would be more correct if this APP Note said that FDP_ACF.1 is the dependency of FDP_ACC.1.

This same comment applies to subclause 8.5.5, page 46, line 36; subclause 9.5.5, page 65, line 36; subclause 10.5.5, page 86, line 26 and subclause 11.5.5, page 107, line 17.

SuggestedRemedy

Consider updating the indicated App Notes as indicated above.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Use "a dependency"

Cl **PP-B** SC **7.5.7** P **28** L **2** # **32**
 Sukert, Alan Xerox

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

In the decription of the SFRs iterations of FMT_MSA.1 (in the case of the PRT TOE they are MT_MSA.1 (a) - FMT_MSA.1 (f), for example) the identical two AppNotes appear for each SFR:

PP APPLICATION NOTE FMT_MSA.1 is one of the dependencies of FMT_MSA.3
 PP APPLICATION NOTE FMT_MSA.1 performs management functions that are recommended for FDP_ACF.1

If the two notes are identical for each SFR then they should appear only one time; otherwise the two AppNotes associated with each of these six SFRs whould be modified to address that particular SFR as in the following for FMT_MSA.1 (a):

PP APPLICATION NOTE FMT_MSA.1(a) is one of the dependencies of FMT_MSA.3
 PP APPLICATION NOTE FMT_MSA.1(a) performs management functions that are recommended for FDP_ACF.1.

The same comment applies to subclause 8.5.7, page 48, line 20; subclause 9.5.7, page 67, line 20; subclause 10.5.7, page 88, line 7 and subclause 11.5.7, page 109, line 2.

SuggestedRemedy

Determine how to handle the identical two APPNotes for the multiple iterations of SFR FMT_MSA.1 in the various TOEs in PP-B.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Same as #19

Cl **PP-B** SC **7.5.7** P **28** L **15** # **35**
 Sukert, Alan Xerox

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

The APP Note says that FMT_MSA.1 is one of the dependencies of FMT_MSA.3. In fact it is the only dependency of FMT_MSA.3, so it would be more correct if this APP Note said that FMT_MSA.1 is the dependency of FMT_MSA.3.

This same comment applies to subclause 8.5.7, page 48, line 33; subclause 9.5.7, page 67, line 33; subclause 10.5.7, page 88, line 20; subclause 11.5.7, page 109, line 15 and subclause 13.5.7, page 148, line 34.

Note: This comment should be addressed in connection with the comment on the multiple duplicate App Notes for subclause 7.5.7.

SuggestedRemedy

Consider updating the indicated App Notes as indicated above.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Use "a dependency"

Cl **PP-B** SC **7.5.9** P **32** L **16** # **36**
 Sukert, Alan Xerox

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

The APP Note says FPT_STM.1 is one of the dependencies of FAU_GEN.1. In fact it is the only dependency of FAU_GEN.1, so it would be more correct if this APP Note said that FPT_STM.1 is the dependency of FAU_GEN.1.

This same comment applies to subclause 8.5.9, page 51, line 28; subclause 9.5.9, page 70, line 28; subclause 10.5.9, page 92, line 16; subclause 11.5.9, page 113, line 10; subclause 12.5.9, page 130, line 8 and subclause 13.5.9, page 150, line 23.

SuggestedRemedy

Consider updating the indicated App Notes as indicated above.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Use "a dependency"

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-B** SC **Keywords** P **ii** L **9** # **24**
 Sukert, Alan Xerox

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

Among the keywords listed for PP-B is 'NIC'. I noted that outside of the keyword list it is not used anywhere else in the document. Also, the acronym 'NIC' is not defined in Annex B.

Note that this keyword also appears in subclause 4, page 5, line 3.

SuggestedRemedy

Either include NIC in Annex B or remove it from the list of keywords for PP-B.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Same as #13

Cl **PP-C** SC **13.5.5** P **116** L **1** # **44**
 Sukert, Alan Xerox

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

The APP Note says that PP APPLICATION NOTE FDP_IFF.1 is one of the dependencies of FDP_IFC.1. In fact it is the only dependency of FDP_IFC.1, so it would be more correct if this APP Note said that FDP_IFF.1 is the dependency of FDP_IFC.1.

SuggestedRemedy

Consider updating the indicated App Note as indicated above.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Use "a dependency"

Cl **PP-C** SC **13.5.7** P **117** L **19** # **46**
 Sukert, Alan Xerox

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

It is not clear for the SMI TOE why FMT_MSA.1 was not broken down into separate FMT_MSA.1(a) & (b) SFRs covering management of the security attributes for the D.PROT.REST and D.CONF.REST objects individually and for the SMI Access Control SFP as was done for in PP-A and PP-B for the TOEs other than the SMI TOE.

SuggestedRemedy

Treat FMT_MSA.1 in the SMI TOE the same way this SFR is treated in PP-A and PP-B.

Proposed Response Response Status **W**

PROPOSED REJECT.

Same as #20

Cl **PP-C** SC **13.5.7** P **117** L **33** # **47**
 Sukert, Alan Xerox

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

The APP Note says that FMT_MSA.1 is one of the dependencies of FMT_MSA.3. In fact it is the only dependency of FMT_MSA.3, so it would be more correct if this APP Note said that FMT_MSA.1 is the dependency of FMT_MSA.3.

SuggestedRemedy

Consider updating the indicated App Note as indicated above.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Use "a dependency"

Cl **PP-C** SC **14** P **126** L **2** # **39**
 Sukert, Alan Xerox

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

Table 110 for the P2600.3 Security Assurance Requirements references some incorrect SARs for EAL2 as follows:

Class	Component Listed	Correct Component
ADV	ADV_FSP.3	ADV_FSP.2
ADV	ADV_TDS.2	ADV_TDS.1
ALC	ALC_CMC.3	ALC_CMC.2
ALC	ALC_CMS.3	ALC_CMS.2
ALC	ALC_DVS.1	Not in EAL2
ALC	ALC_LCD.1	Not in EAL2
ATE	ATE_COV.2	ATE_COV.1
ATE	ATE_DPT.1	Not in EAL2

SuggestedRemedy

Include the correct SARs for EAL3 in Table 110.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Same as #26

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-C** SC **5.5.3** P **10** L **13** # **38**
 Sukert, Alan Xerox

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

Table 4 lists D.DOC.DELETED as a asset for Operational Environment C. However, D.DOC.DELETED is not used in any of the 7 TOEs described in PP-C, so it's not clear why it is listed as an asset for PP-C.

SuggestedRemedy

Resolve whether or not D.DOC.DELETED is an asset in PP-C; if so make sure it is used in one of the TOEs within PP-C.

Proposed Response Response Status **W**

PROPOSED REJECT.

It is actually used in the NVS PP but with the +OTHERTOE attribute.

Cl **PP-C** SC **5.5.3** P **11** L **11** # **40**
 Sukert, Alan Xerox

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

Table 6 uses the acronym SNMP. However, this acronym is not defined in Annex B.

SuggestedRemedy

Include the definition of SNMP in Annex B.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Same as #14

Cl **PP-C** SC **7.1.1** P **14** L **18** # **43**
 Sukert, Alan Xerox

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

The discussion of PRT TOE model in this subclause mentions that the Administrator has the ability to retrieve, modify and store TSF protected and confidential data. There are two issues that I note:

1. In subclause 5.5.4 the operations defined for objects are read, create, modify and delete. I can relate retrieve to the ""read"" operation and modify to the ""modify"" operation, but neither the ""create"" nor ""delete"" operations relate to the concept of storing data. Either some note that relates store to the allowable operations is needed or a ""store"" operation for objects is needed.
2. In the PRT Access Control SFP in subclause 7.5.1.1 (Table 15) it indicates that for TSF protected data the Administrator can ""create"", ""modify"" and ""delete"" while for TSF confidential data the Administrator can do all four operations; this seems inconsistent with subclause 7.1.1 where the Administrator appears to be able to do all operations for both TSF confidential and TSF protected data.

The same comment applies to each of the other six TOEs that are included in PP-C.

SuggestedRemedy

Resolve the apparent inconsistencies among the various subclauses in each TOE as to what operations an administrator can perform on TSF protected and confidential data.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

Same as #17

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-C** SC **7.5.2** P **21** L **1** # **41**
 Sukert, Alan Xerox

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

The PP APP Note here says that FAU_GEN.1 is a principal SFR that directly fulfills O.ADMIN.AUTHORIZED. However, this is not shown in Table 19 on page 27 (there is no 'P' for FAU_GEN.1 for either of these two objectives).

A similar comment applies to subclause 8.5.2, page 35, line 1 vs. Table 33; subclause 9.5.2, page 51, line 1 vs. Table 47; subclause 10.5.2, page 66, line 3 vs. Table 61; subclause 11.5.2, page 81, line 1 vs. Table 75; subclause 12.5.2, page 96, line 1 vs. Table 91 and subclause 13.5.2, page 113, line 3 vs. Table 108.

SuggestedRemedy

Make the indicated App Notes and corresponding tables consistent in terms of what objectives FAU_GEN.1 fulfills.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Same as #15

Cl **PP-C** SC **7.5.2** P **21** L **25** # **42**
 Sukert, Alan Xerox

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

The APP Note says that FAU_SAR.1 is one of the dependencies of FAU_SAR.2. In fact it is the only dependency of FAU_SAR.2, so it would be more correct if this APP Note said that FAU_SAR.1 is the dependency of FAU_SAR.2.

This same comment applies to subclause 8.5.2, page 36, line 25; subclause 9.5.2, page 51, line 25; subclause 10.5.2, page 66, line 27; subclause 11.5.2, page 81, line 25; subclause 12.5.2, page 96, line 25 and subclause 13.5.2, page 114, line 1.

SuggestedRemedy

Consider updating the indicated App Notes as indicated above.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Use "a dependency"

Cl **PP-C** SC **7.5.9** P **25** L **27** # **45**
 Sukert, Alan Xerox

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

The APP Note says FPT_STM.1 is one of the dependencies of FAU_GEN.1. In fact it is the only dependency of FAU_GEN.1, so it would be more correct if this APP Note said that FPT_STM.1 is the dependency of FAU_GEN.1.

This same comment applies to subclause 8.5.9, page 40, line 22; subclause 9.5.9, page 55, line 22; subclause 10.5.9, page 70, line 22; subclause 11.5.9, page 85, line 22; subclause 12.5.9, page 100, line 27 and subclause 13.5.9, page 119, line 18.

SuggestedRemedy

Consider updating the indicated App Notes as indicated above.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Use "a dependency"

Cl **PP-C** SC **Keywords** P **ii** L **9** # **37**
 Sukert, Alan Xerox

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

Among the keywords listed for PP-C is 'NIC'. I noted that outside of the keyword list it is not used anywhere else in the document. Also, the acronym 'NIC' is not defined in Annex B.

Note that this keyword also appears in subclause 4, page 5, line 3.

SuggestedRemedy

Either include NIC in Annex B or remove it from the list of keywords for PP-C.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Same as #13

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-D** SC **12.5.5** P **73** L **1** # **52**
 Sukert, Alan Xerox

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

The APP Note says that PP APPLICATION NOTE FDP_IFF.1 is one of the dependencies of FDP_IFC.1. In fact it is the only dependency of FDP_IFC.1, so it would be more correct if this APP Note said that FDP_IFF.1 is the dependency of FDP_IFC.1.

SuggestedRemedy

Consider updating the indicated App Note as indicated above.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Use "a dependency"

Cl **PP-D** SC **12.5.7** P **74** L **8** # **53**
 Sukert, Alan Xerox

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

It is not clear for the SMI TOE why FMT_MSA.1 was not broken down into separate FMT_MSA.1(a) & (b) SFRs covering management of the security attributes for the D.PROT.REST and D.CONF.REST objects individually and for the SMI Access Control SFP as was done for in PP-A and PP-B for the TOEs other than the SMI TOE.

SuggestedRemedy

Treat FMT_MSA.1 in the SMI TOE the same way this SFR is treated in PP-A and PP-B.

Proposed Response Response Status **W**

PROPOSED REJECT.

Same as #20

Cl **PP-D** SC **12.5.7** P **74** L **22** # **54**
 Sukert, Alan Xerox

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

The APP Note says that FMT_MSA.1 is one of the dependencies of FMT_MSA.3. In fact it is the only dependency of FMT_MSA.3, so it would be more correct if this APP Note said that FMT_MSA.1 is the dependency of FMT_MSA.3.

SuggestedRemedy

Consider updating the indicated App Note as indicated above.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Use "a dependency"

Cl **PP-D** SC **5.5.3** P **10** L **10** # **50**
 Sukert, Alan Xerox

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

Table 6 uses the acronym SNMP. However, this acronym is not defined in Annex B.

SuggestedRemedy

Include the definition of SNMP in Annex B.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Same as #14

Cl **PP-D** SC **7.1.1** P **13** L **17** # **51**
 Sukert, Alan Xerox

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

The discussion of PRT TOE model in this subclause mentions that the Administrator has the ability to retrieve, modify and store TSF protected and confidential data. There are two issues that I note:

1. In subclause 5.5.4 the operations defined for objects are read, create, modify and delete. I can relate retrieve to the "read" operation and modify to the "modify" operation, but neither the "create" nor "delete" operations relate to the concept of storing data. Either some note that relates store to the allowable operations is needed or a "store" operation for objects is needed.
2. In the PRT Access Control SFP in subclause 7.5.1.1 (Table 15) it is indicated that for TSF protected data the Administrator can "create", "modify" and "delete" while for TSF confidential data the Administrator can do all four operations; this seems inconsistent with subclause 7.1.1 where the Administrator appears to be able to do all operations for both TSF confidential and TSF protected data.

The same comment applies to each of the other six TOEs that are included in PP-D.

SuggestedRemedy

Resolve the apparent inconsistencies among the various subclauses in each TOE as to what operations an administrator can perform on TSF protected and confidential data.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

Same as #17

IEEE P2600 Hardcopy Device and System Security comments

CI **PP-D** SC **8.5.1.1** P **28** L **6** # **48**
Sukert, Alan Xerox

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

It is not clear why the SCN Access Control SFP includes discussion of D.FUNC.REST when clause 8.2.1 does not list D.FUNCT.REST (or any User Document Data for that matter) as assets of the SCN TOE that need to be protected.

A similar comment applies to the CPY TOE (subclause 9.5.1.1, page 31, line 7) and FAX TOE (subclause 10.5.1.1, page 48, line 10)

SuggestedRemedy

Resolve the inconsistency when the list of assets to be protected and the associated access control SFP for the SCN, CPY and FAX TOEs as to including of D.FUNC.REST.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

See response to comment #11.

CI **PP-D** SC **Keywords** P **ii** L **9** # **49**
Sukert, Alan Xerox

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

Among the keywords listed for PP-D is 'NIC'. I noted that outside of the keyword list it is not used anywhere else in the document. Also, the acronym 'NIC' is not defined in Annex B.

Note that this keyword also appears in subclause 4, page 4, line 44.

SuggestedRemedy

Either include NIC in Annex B or remove it from the list of keywords for PP-D.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Same as #13