

IEEE P2600 Hardcopy Device and System Security comments

Cl All P SC .5.1, 13.5.1.1, 13.5.1.2 P8, 122 L 5 # 8
 Chen, Nancy Oki Data

Comment Type T Comment Status D

The definition of User is not consistent with what's in CC and U.EXTENTITY is never well defined. We have "Users" defined that has four types of users: originator, delegate, administrator, and ExtEntity. This means Users consists of human users and ExtEntity. Then ExtEntity is defined as an external ""User"" with which the TOE exchange data. So ExtEntity is an external human user or an ExtEntity with which the TOE exchange data. Therefore ExtEntity is never defined. However, U.EXTENTIY is only used in SMI TOE to mean an "external IT entity" or a remote human users outside the HCD.

SuggestedRemedy

- Fix the definition of Users to be consistent with CC part2 as follows:
- (1) Fix the Users object model diagram to derive into three child objects: LocalHumanUser, RemoteHumanUser, and ExternalITEntity. Originator, Delegate, and Administrator all derive from both LocalHumanUser and RemoteHumanUser.
 - (2) Change the definition of U.EXTENTITY in Table 1 to ""An external IT entity or a remote human user with which the TOE exchanges data.""
 - (3) Change ""A User"" in the definitions of U.ORIGINATOR, U.DELEGATE, U.ADMINSTRATOR to ""A local or remote human User"".
 - (4) Add one more user type definition U.ExtITEntity which is an external IT entity.
 - (4) Change ""User"" in the Access Control SFP table of every TOE to ""human User"".

Proposed Response Response Status W

PROPOSED ACCEPT IN PRINCIPLE.

The name of U.EXTENTITY will be changed to not collide with CC defined term EXTERNAL ENTITY.

Cl All P SC 0 P i L 6 # 44
 Smithson, Brian Ricoh

Comment Type E Comment Status D

We should try to use the exact same document for both the IEEE Std. and the standalone published PP. To do so, we will need to add some CC-specific content to the cover page.

SuggestedRemedy

Add the following information to the cover sheet, before the copyright statement:

Certification ID: [insert when issued]
 Version: 1.0
 Date: [insert when final]
 Author: Hardcopy Device and System Security Working Group
 Sponsor: IEEE Computer Society, Information Assurance Committee
 Common Criteria Scheme: [insert when decided]
 Common Criteria Testing Lab: [insert when decided]
 Common Criteria Conformance: Common Criteria Version 3.1, Release 2, parts 2 and 3 conformant
 Assurance level: EAL 3 augmented (by ALC_FLR.1) [change for each PP]

Proposed Response Response Status W

PROPOSED ACCEPT.

Cl All P SC 0 P iv L 9 # 45
 Smithson, Brian Ricoh

Comment Type E Comment Status D

More information to make the IEEE Std and PP formats uniform.

SuggestedRemedy

For more information
 Further information, including the status and updates of this protection profile can be found on the internet at: [insert URL].

Comments or questions regarding this document should be directed to: [whom?]. The comments should include the title of the document, the page, the section number, and paragraph number, detailed comment and recommendations.

Proposed Response Response Status W

PROPOSED ACCEPT.

IEEE P2600 Hardcopy Device and System Security comments

Cl **All P** SC 1 P 1 L 15 # 46
 Smithson, Brian Ricoh

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

More information is to make the IEEE Std and PP formats uniform.

SuggestedRemedy

1.3 Application notes

Application notes are provided where they may contribute to the understanding of the reader. These notes, while not part of the formal statement of this Family of Protection Profiles, are included as an acknowledgment of the diverse uses of this document and are intended to provide guidance to readers. Additional guidance may be found in [PP guide reference].

1.4 Notational conventions

[describes any special notational conventions]

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **All P** SC 1.2 P 1 L 12 # 51
 Smithson, Brian Ricoh

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

missing words in first sentence of Purpose

SuggestedRemedy

"The purpose of this standard is to define a Protection Profile for Hardcopy Devices in Operational..."

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

Make match the PAR. If there is an error in the PAR, do a modified PAR.

Cl **All P** SC 10.1.1 P 76 L 4 # 89
 Sukert, Alan Xerox

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

In PP-A. for consistency with the remainder of Clause 10 the term 'Fax TOE' on this line and on line 30 (same page) should be capitalized as 'FAX TOE'.

The same comment applies to PP-B (subclause 10.1.1, page 75, lines 4 and 30), PP-C (subclause 10.1.1, page 61, lines 4 and 22) and PP-D (subclause 10.1.1, page 49, lines 4 and 23)

SuggestedRemedy

Make capitalization of the term 'FAX TOE' consistent in Clause 10 in all four PP documents.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **All P** SC 10.1.1 P 76 L 10 # 88
 Sukert, Alan Xerox

Comment Type **G** Comment Status **D**

The capitalization of the term 'fax' in the discussion of the FAX TOE in PP-A is inconsistent in Clause 10. For example, subclause 10.1.1, page 76, line 10 denotes it as 'fax' while line 12 on the same page denotes it as 'Fax' and subclause 10.1.2, page 78, line 2 denotes it as 'FAX'.

The same comment applies to PP-B (see subclause 10.1.1, page 75, line 7 vs. subclause 10.1.1, page 75, line 12 vs. subclause 10.1.2, page 77, line 2); PP-C (see subclause 10.1.1, page 61, line 7 vs. subclause 10.1.1, page 61, line 10 vs. subclause 10.1.2, page 62, line 11); and PP-D (see subclause 10.1.1, page 49, line 7 vs. subclause 10.1.1, page 49, line 10 vs. subclause 10.1.2, page 50, line 11).

SuggestedRemedy

Be consistent on how the term 'fax' is capitalized with each of the four PP documents.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

IEEE P2600 Hardcopy Device and System Security comments

CI All P SC 11.1.1 P 97 L 7 # 41
 Smithson, Brian Ricoh
 Comment Type E Comment Status D
 list item A refers to "a Document", should be "User Document Data"
 SuggestedRemedy
 replace "a Document" with ""User Document Data".
 In PP-B: page 96, line 7
 In PP-C: page 77, line 7
 In PP-D: page 62, line 7
 Proposed Response Response Status W
 PROPOSED ACCEPT.

CI All P SC 11.5.7 P 113 L 5 # 54
 Smithson, Brian Ricoh
 Comment Type T Comment Status D
 App note after FMT_SMR.1 in DSR TOE refers to "DSR User", it is not a defined term.
 SuggestedRemedy
 Remove "and DSR User" from the app note after FMT_SMR.1
 In PP-B: P.112 L.5
 In PP-C: P.89 L.13
 It is fixed in PP-D.
 Proposed Response Response Status W
 PROPOSED ACCEPT.

CI All P SC 13.2.1 P 138 L 1 # 47
 Smithson, Brian Ricoh
 Comment Type T Comment Status D
 should D.PROT(+OTHERTOE).TRANSIT and D.CONF(+OTHERTOE).TRANSIT be listed as User Data in the SMI TOE? Would it make a difference in the handling of the threats (objectives and SFRs)? Would it make more confusion than it is worth?
 SuggestedRemedy
 not sure
 Proposed Response Response Status W
 PROPOSED REJECT.
 This comment was WITHDRAWN by the commenter.

CI All P SC 13.2.4 P 140 L 6 # 48
 Smithson, Brian Ricoh
 Comment Type T Comment Status D
 SMI assumptions should include A.USER.TRAINING (to correspond with P.USER.AUTHORIZATION)
 SuggestedRemedy
 Add A.USER.TRAINING, and OE.USER.TRAINED (on P.142 L.4)
 For PP-B: P.139 L.6 and P.141 L.1
 For PP-C: P.113 L.1 and P.114 L.10
 For PP-D: it is 12.2.4, P.78 L.1 and P.79 L.10
 Proposed Response Response Status W
 PROPOSED ACCEPT.

CI All P SC 13.5.11 P 160 L 21 # 50
 Smithson, Brian Ricoh
 Comment Type T Comment Status D
 PP app note for FTA_SSL.3.1 should say that FTA_SSL.3.1 fulfills O.USER.AUTHORIZED (in addition to ADMIN)
 SuggestedRemedy
 Add O.USER.AUTHORIZED to the app note.
 PP-B: P.153 L.10
 PP-C: P.125 L.1
 PP-D: P.87 L.22
 Proposed Response Response Status W
 PROPOSED ACCEPT.

IEEE P2600 Hardcopy Device and System Security comments

Cl All P SC 13.6 P 155 L 14 # 39
 Smithson, Brian Ricoh

Comment Type T Comment Status D

In table 116, FMT_MSA.1 and FMT_MSA.3 are specified for O.CONF.REST.NO_DIS, O.CONF.REST.NO_ALT, and O.PROT.REST.NO_ALT. They are not shown in table 117. Table 117 is correct.

SuggestedRemedy

Remove FMT_MSA.1 and FMT_MSA.3 for those objectives in table 116.

In PP-B: table 114, page 154, line 5
 In PP-C, table 104, page 126, line 1
 In PP-D, it is 12.6, table 76, page 89, line 1

Proposed Response Response Status W

PROPOSED ACCEPT.

Cl All P SC 13.6 P 156 L 1 # 49
 Smithson, Brian Ricoh

Comment Type T Comment Status D

Description of data in transit says "protection of stored...data...while in transit"; should not say "stored".

SuggestedRemedy

Remove "stored" from all data-in-transit objectives in table 117.

PP-B: P.154 L.6 etc.
 PP-C: P.126 L.1 etc.
 PP-D: P.89 L.1 etc.

Proposed Response Response Status W

PROPOSED ACCEPT.

Cl All P SC 4 P 3 L 8 # 72
 Sukert, Alan Xerox

Comment Type G Comment Status D

PP-A is inconsistent in capitalization of the terms 'Protection Profile'. It capitalized in line 4 on page 3 but not capitalized in line 8.

A similar comment applies to capitalization of the term 'Security Target' in PP-A. For example, it is capitalized in the Introduction, page iii but not capitalized in subclause 4, page 3, line 8.

The same two comments apply to the identical subclauses, pages and lines in PP-B, PP-C & PP-D.

SuggestedRemedy

Be consistent in all four PP documents on capitalization of the terms 'Protection Profile' and 'Security Target'.

Proposed Response Response Status W

PROPOSED ACCEPT.

Capitalize both everywhere

Cl All P SC 5.2 P 6 L 39 # 56
 Smithson, Brian Ricoh

Comment Type E Comment Status D

Change references to IEEE Std. P2600 to IEEE Std. 2600.

SuggestedRemedy

Change references to IEEE Std. P2600 to IEEE Std. 2600.

There are many subclause/page/line numbers to which this applies, see the numbers above for first example in PP-A.

Proposed Response Response Status W

PROPOSED REJECT.

We should call it P2600 until it is approved. BTW, the IEEE editors will fix it anyway.

IEEE P2600 Hardcopy Device and System Security comments

Cl All P SC 5.4 P 7 L 28 # 76
 Sukert, Alan Xerox

Comment Type G Comment Status D

The term 'Subject' when used in the context of entities are inconsistently capitalized. For example, PP-A subclause 5.4, page 7, line 28 capitalizes the term subject but subclause 7.1.1, page 15, line 8 does not capitalize that term.

A similar comment applies to PP-B -- e.g., subclause 5.4, page 7, line 27 vs. subclause 7.1.1, page 15, line 9

A similar comment applies to PP-B -- e.g., subclause 5.4, page 7, line 27 vs. subclause 7.1.1, page 14, line 8

A similar comment applies to PP-B -- e.g., subclause 5.4, page 6, line 25 vs. subclause 7.1.1, page 13, line 7

SuggestedRemedy

Make sure the capitalization of the term 'subject' when used as an entity is consistent in all four PPs.

Proposed Response Response Status W
 PROPOSED ACCEPT.

Cl All P SC 5.4 P 7 L 30 # 73
 Sukert, Alan Xerox

Comment Type T Comment Status D

You've added the new entity TOE owner. I didn't see 'TOE owner' in the TOE model shown in Figures 1-6 for any of the four PPs. I would think that 'TOE Owner' should show up at least in Figure 1 for the general TOE model in each of the four PPs.

You also describe the new entity 'Channels' in subclause 5.5.5 in each of the four PPs but it isn't shown in the corresponding Figure 1 in any of the four PPs. I would think that 'Channels' should also show up at least in Figure 1 for the general TOE model in each of the four PPs.

SuggestedRemedy

Update Figure 1 in each of the four PPs per the above comment.

Proposed Response Response Status W
 PROPOSED ACCEPT IN PRINCIPLE.

REJECTING comment against TOE owner

ACCEPTING adding Channels to figure 1 in all four PPs. In addition, in all TOE Admin Models, use INTERFACE instead of CHANNEL.

Cl All P SC 5.4 P 8 L 1 # 77
 Sukert, Alan Xerox

Comment Type T Comment Status D

I noted a couple of inconsistencies between Figure 1 and subclause 5.5.1 in PP-A. Specifically:

1. Figure 1 includes a 'Normal User' but this is not listed as one of the User entities in subclause 5.5.1.
2. Figure 1 shows the specific User entity 'Administrator' but doesn't show any of the other three User entities. Figure 1 should either show all of the four User entities or none of them; it shouldn't show just one of the four.

Also, I believe that the term 'Operations' in PP-A Figure 1 should be capitalized since it is referring to that part of the TOE model.

The same two comments apply to the other three PPs as follows:
 PP-B -- Figure 1, subclause 5.4, page 8, line 1 vs. subclause 5.5.1, page 8, line 4

PP-C -- Figure 1, subclause 5.4, page 8, line 1 vs. subclause 5.5.1, page 8, line 4

PP-D -- Figure 1, subclause 5.4, page 7, line 1 vs. subclause 5.5.1, page 7, line 4

SuggestedRemedy

In all four PPs --

- Update Figure 1 to resolve the inconsistencies noted in the comment above.
- Capitalize 'Operations' in Figure 1

Proposed Response Response Status W
 PROPOSED ACCEPT.

Cl All P SC 5.4 P 8 L 2 # 52
 Smithson, Brian Ricoh

Comment Type T Comment Status D

"Administrator" and "Normal User" should not be defined in this figure. ("Normal User" isn't even a defined term in the PP)

SuggestedRemedy

Remove "Administrator" and "Normal User" boxes and arrows.

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 # 91
 Sukert, Alan Xerox

Comment Type T Comment Status D

The definition of the following terms in Clause 5 of each PP do not agree with their corresponding definitions in P2600 main body Clauses 2 & 5:
 -- User (subclause 5.5.1, page 8, line 5)
 -- User Document Data (subclause 5.5.3, page 10, line 1)
 -- User Function Data (subclause 5.5.3, page 10, line 3)
 -- Confidential Data (subclause 5.5.3, page 10, line 8)
 -- Protected Data (subclause 5.5.3, page 10, line 11)

SuggestedRemedy

Update the definitions of the above terms in each of the four PPs to agree with the definition in the proposed updated Annex A (see Comment #224) that has definitions consistent with the P2600 main body.

Proposed Response Response Status W
 PROPOSED ACCEPT.

Cl All P SC 5.5.2 P 9 L 9 # 75
 Sukert, Alan Xerox

Comment Type G Comment Status D

In PP-A Table 2, it indicates that DSR stands for "Document Store/Retrieve". However, the subclause 11 discussion of the DSR TOE PP refers to DSR as meaning "Document Storage and Retrieval". A similar comment also applies to Figure 3 in PP-A subclause 5.5.2, page 9, line 7.

For PP-B, the same comment applies to Table 2 in subclause 5.5.2, page 9, line 9 and Figure 3 in subclause 5.5.2, page 9, line 7 vs. subclause 11.

For PP-C, the same comment applies to Table 2 in subclause 5.5.2, page 9, line 9 and Figure 3 in subclause 5.5.2, page 9, line 7 vs. subclause 11.

For PP-D, the same comment applies to Table 2 in subclause 5.5.2, page 8, line 9 and Figure 3 in subclause 5.5.2, page 8, line 7 vs. subclause 10.

SuggestedRemedy

Make sure the Table 2 definition of 'DSR', Figure 3 and the Clause 11 definition of 'DSR' are all consistent in all four PPs.

Proposed Response Response Status W
 PROPOSED ACCEPT.

Use "Document Storage and Retrieval"

Cl All P SC 5.5.3 P 9 L 15 # 90
 Sukert, Alan Xerox

Comment Type T Comment Status D

The PPs all use the term 'TOE Security Function' in defining the acronym TSF. However, CC Version 3.1, Revision 2 now defines TSF as 'TOE Security Functionality'. The PPs should be updated to reflect the new CC definition of TSF.

SuggestedRemedy

Modify 'TOE Security Function' to be 'TOE Security Functionality' where it occurs in all the PPs.

Proposed Response Response Status W
 PROPOSED ACCEPT.

Cl All P SC 5.5.3 P 11 L 1 # 79
 Sukert, Alan Xerox

Comment Type G Comment Status D

In PP-A, Table 3 in subclause 5.5.3, page 11 uses "output document handler" in the discussion of D.DOC.OUTPUT to refer to the destination of hardcopy document output. However, PP-A subclause 5.5.5, page 12, line 37 denotes this mechanism as the 'output hardcopy handler' and PP-A subclause 7.1.1, page 15, line 11 denotes this mechanism as a 'document handler'. All three subclauses in PP-A should refer to this mechanism in the same way.

The same comment applies to the remaining PPs as follows:

- PP-B: subclause 5.5.3, page 1, line 1 vs. subclause 5.5.5, page 12, line 31 vs. subclause 7.1.1, page 15, line 11
- PP-C: subclause 5.5.5, page 12, line 16 vs. subclause 7.1.1, page 14, line 11
- PP-D: subclause 5.5.5, page 10, line 32 vs. subclause 7.1.1, page 13, line 9

SuggestedRemedy

Make the reference to the output handler mechanism in a consistent manner throughout all four PPs.

Proposed Response Response Status W
 PROPOSED ACCEPT IN PRINCIPLE.

Use "Hardcopy Output Handler" as that is what it is called in P2600.

IEEE P2600 Hardcopy Device and System Security comments

Cl All P SC 5.5.3 P 12 L 9 # 78
 Sukert, Alan Xerox

Comment Type E Comment Status D

In PP-A there is a typographical error on this line -- "...distinguish the the assets..." should be "...distinguish the assets..."

The same comment applies to:

- PP-B, subclause 5.5.3, page 12, line 3
- PP-C, subclause 5.5.3, page 11, line 8
- PP-D, subclause 5.5.3, page 10, line 4

SuggestedRemedy

Correct the typographical error noted above.

Proposed Response Response Status W

PROPOSED ACCEPT.

Cl All P SC 7.1.1. P 15 L 10 # 80
 Sukert, Alan Xerox

Comment Type T Comment Status D

The discussion of the PRT model in PP-A subclause 7 mentions an asset entity called 'Output Document'. This entity isn't mentioned or discussed in PP-A subclause 5.5.3.

The same comment applies to the other three PPs as follows:

- PP-B: See subclause 7.1.1, page 15, line 11 vs. subclause 5.5.3, page 9, line 10
- PP-C: See subclause 7.1.1, page 14, line 11 vs. subclause 5.5.3, page 9, line 10
- PP-D: See subclause 7.1.1, page 13, line 9 vs. subclause 5.5.3, page 8, line 10

SuggestedRemedy

In each of the four PPs, either define 'Output Document' in subclause 5.5.3 or use in subclause 7.1.1 one of the objects described in subclause 5.5.3 .

Proposed Response Response Status W

PROPOSED ACCEPT IN PRINCIPLE.

Use "User Document Data"

Cl All P SC 7.1.2 P 16 L 9 # 81
 Sukert, Alan Xerox

Comment Type G Comment Status D

The convention that seems to be used in the PPs is that any use of one of the entities defined in subclause 5.5 in the Family of PPs is capitalized. However, this convention is not being followed consistently throughout each of the four PP documents. For example, 'user' is not capitalized on PP-A subclause 7.1.2, page 16, line 9 but 'User' is clearly one of the entities described in subclause 5.5.1, page 8, line 4. There are numerous other examples throughout all PP-A subclauses of inconsistent capitalization that can be cited.

The same is true in each of the other three PPs. A similar example to the one noted above in PP-A can be found in PP-B (see subclause 7.1.2, page 16, line 9 vs. subclause 5.5.1, page 8, line 4), PP-C (see subclause 7.6, page 28, line 2 vs. subclause 5.5.1, page 8, line 4) and PP-D (see subclause 7.6, page 23, line 3 vs. subclause 5.5.1, page 7, line 4),

SuggestedRemedy

Make sure that whatever convention is being used for capitalization of entities is consistently used throughout all four PPs.

Proposed Response Response Status W

PROPOSED ACCEPT.

Will be capitalized

IEEE P2600 Hardcopy Device and System Security comments

Cl All P SC 7.2.4 P 19 L 6 # 84
 Sukert, Alan Xerox

Comment Type E Comment Status D

In PP-A the wording of the definition of the A.ADMIN.TRAINING assumption in Table 10 has a grammatical error. It currently states "...operate the TOE in accordance those policies and procedures."; it should say "...operate the TOE in accordance with those policies and procedures." This same comment applies to subclause 8.2.4, page 40, line 5 (Table 26); subclause 9.2.4, page 60, line 5 (Table 42); subclause 10.2.4, page 80, line 11 (Table 58); subclause 11.2.4, page 101, line 6 (Table 74); subclause 12.2.4, page 121, line 5 (Table 90) and subclause 13.2.4, page 140, line 6 (Table 106).

The same comment applies to the following subclauses in the other three PPs:

--PP-B: subclause 7.2.4, page 19, line 5 (Table 10); subclause 8.2.4, page 40, line 1 (Table 26); subclause 9.2.4, page 59, line 5 (Table 42); subclause 10.2.4, page 79, line 6 (Table 58); subclause 11.2.4, page 100, line 6 (Table 74); subclause 12.2.4, page 120, line 5 (Table 90) and subclause 13.2.4, page 139, line 6 (Table 104)

--PP-C: subclause 7.2.4, page 17, line 5 (Table 8); subclause 8.2.4, page 33, line 6 (Table 22); subclause 9.2.4, page 49, line 5 (Table 36); subclause 10.2.4, page 64, line 14 (Table 50); subclause 11.2.4, page 80, line 13 (Table 64); subclause 12.2.4, page 96, line 1 (Table 80) and subclause 13.2.4, page 113, line 1 (Table 94)

--PP-D: subclause 7.2.4, page 16, line 1 (Table 8); subclause 8.2.4, page 28, line 6 (Table 20); subclause 9.2.4, page 40, line 1 (Table 32); subclause 10.2.4, page 52, line 13 (Table 44); subclause 11.2.4, page 65, line 6 (Table 56) and subclause 12.2.4, page 78, line 1 (Table 68)

SuggestedRemedy

Make the suggested change to the definition of the A.AMIN.TRAINING assumption in all the subclauses indicated for the four PPs in the comment above.

Proposed Response Response Status W
 PROPOSED ACCEPT.

Cl All P SC 7.3.4 P 20 L 8 # 85
 Sukert, Alan Xerox

Comment Type E Comment Status D

In PP-A the wording of the definition of the OE.ADMIN.TRAINED security objective in Table 12 has a grammatical error. It currently states "...operate the TOE in accordance those policies and procedures."; it should say "...operate the TOE in accordance with those policies and procedures." This same comment applies to PP-A in subclause 8.3.4, page 41, line 6 (Table 28), subclause 9.3.4, page 60, line 5 (Table 54), subclause 10.3.4, page 81, line 8 (Table 60); subclause 11.3.4, page 102, line 8 (Table 76); subclause 12.3.3.1, page 122, line 8 (Table 92) and subclause 13.3.3.1, page 142, line 4 (Table 109).

The same comment applies to the following subclauses in the other three PPs:

--PP-B: subclause 7.3.4, page 20, line 6 (Table 12); subclause 8.3.4, page 41, line 4 (Table 28); subclause 9.3.4, page 60, line 6 (Table 44); subclause 10.3.4, page 80, line 8 (Table 60); subclause 11.3.4, page 101, line 8 (Table 76); subclause 12.3.3.1, page 121, line 8 (Table 92) and subclause 13.3.3.1, page 141, line 6 (Table 107)

--PP-C: subclause 7.3.4, page 18, line 1 (Table 10); subclause 8.3.4, page 34, line 8 (Table 24); subclause 9.3.4, page 50, line 1 (Table 38); subclause 10.3.4, page 65, line 9 (Table 52); subclause 11.3.4, page 81, line 9 (Table 66); subclause 12.3.3.1, page 97, line 1 (Table 82) and subclause 13.3.3.1, page 114, line 10 (Table 97)

--PP-D: subclause 7.3.4, page 17, line 1 (Table 10); subclause 8.3.4, page 29, line 6 (Table 22); subclause 9.3.4, page 41, line 1 (Table 34); subclause 10.3.4, page 53, line 8 (Table 46); subclause 11.3.4, page 66, line 6 (Table 58) and subclause 12.3.3.1, page 79, line 10 (Table 71)

SuggestedRemedy

Make the suggested change to the definition of the A.AMIN.TRAINING assumption in all the subclauses indicated in the comment above for all four PPs.

Proposed Response Response Status W
 PROPOSED ACCEPT.

IEEE P2600 Hardcopy Device and System Security comments

Cl All P SC 7.3.4, 8.3.4, ... P 20 L 8 # 40
 Smithson, Brian Ricoh

Comment Type T Comment Status D

P.USER.AUTHORIZATION and P.ADMIN.AUTHORIZATION require that the TOE Owner grant permission to Users and Administrators to use and manage the TOE. There should be non-IT operational environment objectives to support those policies.

SuggestedRemedy

Add OEs in each PP in each environment (A, B, C, D) to correspond to P.USER.AUTH and P.ADMIN.AUTH:

OE.USER.AUTHORIZED - The TOE Owner shall grant permission to Users to be authorized to use the TOE according to the security policies and procedures of their organization.

OE.ADMIN.AUTHORIZED - The TOE Owner shall grant permission to Administrators to be authorized to manage the TOE according to the security policies and procedures of their organization.

There are many subclause/page/line numbers to which this applies, see the numbers above for first example in PP-A.

Proposed Response Response Status W

PROPOSED ACCEPT IN PRINCIPLE.

Also add it to the threat objectives table.

Cl All P SC 7.5.2, 8.5.2, ... P 23 L 20 # 37
 Smithson, Brian Ricoh

Comment Type T Comment Status D

PP application note after FAU_GEN.1 says "FAU_GEN.1 performs audit recommendations for [list of SFRs]" but the list of SFRs includes SFRs that are in neither the Requirements or Recommendations tables.

SuggestedRemedy

Limit the list of SFRs to only those SFRs that appear in the Requirements table, and also list the SFRs in the Recommendations table as ""optionally"". This applies to all TOEs in PP-A, PP-B, and PP-C.

There are many subclause/page/line numbers to which this applies, see the numbers above for first example in PP-A.

Proposed Response Response Status W

PROPOSED ACCEPT.

Cl All P SC 7.5.5 P 26 L 3 # 87
 Sukert, Alan Xerox

Comment Type E Comment Status D

There is a typographical error in the PP Application Note in PP-A -- 'FDP_AC C.1' should be 'FDP_ACC.1'.

This same comment applies to PP-A in the following subclauses:

- subclause 8.5.5, page 46, line 21
- subclause 8.5.6, page 47, line 29
- subclause 9.5.5, page 66, line 21
- subclause 9.5.6, page 67, line 27
- subclause 10.5.5, page 87, line 9
- subclause 11.5.5, page 108, line 9
- subclause 12.5.6, page 129, line 11 and
- subclause 13.5.6, page 150, line 3

This same comment also applies to PP-B in the following subclauses:

- subclause 7.5.5, page 25, line 24
- subclause 8.5.5, page 46, line 11
- subclause 8.5.6, page 47, line 14
- subclause 9.5.5, page 65, line 21
- subclause 9.5.6, page 66, line 27
- subclause 10.5.5, page 86, line 9
- subclause 11.5.5, page 107, line 9
- subclause 12.5.6, page 128, line 11 and
- subclause 13.5.6, page 148, line 17

This same comment applies to PP-A in the following subclauses:

- subclause 8.5.5, page 46, line 21
- subclause 8.5.6, page 47, line 29
- subclause 9.5.5, page 66, line 21
- subclause 9.5.6, page 67, line 27
- subclause 10.5.5, page 87, line 9
- subclause 11.5.5, page 108, line 9
- subclause 12.5.6, page 129, line 11 and
- subclause 13.5.6, page 150, line 3

This same comment also applies to PP-C in the following subclauses:

- subclause 8.5.6, page 39, line 13
- subclause 9.5.6, page 55, line 27
- subclause 12.5.6, page 102, line 15 and
- subclause 13.5.6, page 121, line 14

This same comment also applies to PP-D in the following subclauses:

- subclause 8.5.6, page 31, line 3
- subclause 9.5.6, page 43, line 1 and
- subclause 12.5.6, page 83, line 14

IEEE P2600 Hardcopy Device and System Security comments

Cl All P SC 8.5.6 P 48 L 12 # 86
Sukert, Alan Xerox

Comment Type G Comment Status D

PP-A is inconsistent in how the term 'TSF mediated' is denoted in the document. For example, in PP-A subclause 8.5.6, page 48, line 12 it is denoted as 'TSF mediated' but in PP-A subclause 8.5.6, page 49, line 4 this term is denoted as 'TSF-mediated'.

The same comment applies to PP-B (see subclause 8.5.6, page 48, line 4 vs. subclause 8.5.6, page 48, line 19), PP-C (see subclause 8.5.6, page 39, line 24 vs. subclause 8.5.6, page 40, line 13) and PP-D see subclause 8.5.6, page 31, line 14 vs. subclause 8.5.6, page 32, line 3).

SuggestedRemedy

Consistently refer to the term 'TSF mediated' within all four PP documents.

Proposed Response Response Status W

PROPOSED ACCEPT.

Use "TSF-mediated"

Cl All P SC 8.5.7, 9.5.7, 13.5.7 P 51 L 12 # 42
Smithson, Brian Ricoh

Comment Type T Comment Status D

For FMT_SMF.1, 2nd app note says "'FMT_MSA.1 performs management ...'", should refer instead to FMT_SMF.1.

SuggestedRemedy

In 2nd app note of FMT_SMF.1, change "'FMT_MSA.1 performs'" to "'FMT_SMF.1 performs'".

There are many subclause/page/line numbers to which this applies, see the numbers above for first example in PP-A.

Proposed Response Response Status W

PROPOSED ACCEPT.

Cl All P SC 8.6 P 54 L 1 # 53
Smithson, Brian Ricoh

Comment Type E Comment Status D

There is an extraneous trailing comma from O.CONF.REST.NO_DIS in table 35 (or equiv)

SuggestedRemedy

Remove trailing comma from O.CONF.REST.NO_DIS

In PP-B: P.54 L.6

In PP-C P.44 L.1

It is fixed in PP-D

Proposed Response Response Status W

PROPOSED ACCEPT.

Cl All P SC Annex A P 160 L 34 # 74
Sukert, Alan Xerox

Comment Type T Comment Status D

The definition of 'object' in PP-A, Annex A is slightly different that the one earlier in the document in PP-A subclause 5.5.3, page 9, line 11 as follows:

subclause 5.5.3, page 9, line 11 -- "Objects are passive entities in the TOE that contain or receive information and upon which Subjects perform Operations"

Annex A, page 160, line 34 -- "Object: An entity within the TSF scope of control that contains or receives information and upon which subjects perform operations".

The same comment applies to PP-B in subclause 5.5.3, page 9, line 11 vs. Annex A, page 158, line 34; PP-C in subclause 5.5.3, page 9, line 11 vs. Annex A, page 130, line 34 and PP-D in subclause 5.5.3, page 8, line 11 vs. Annex A, page 93, line 34

SuggestedRemedy

Make the definitions of object in subclause 5.5.3, page 9, line 11 and Annex A, page 160, line 34 consistent. Note that comment #224 proposes a complete update to Annex A for all four PPs that resolves this comment.

Proposed Response Response Status W

PROPOSED ACCEPT IN PRINCIPLE.

Use exactly the CC Part 1 definition.

IEEE P2600 Hardcopy Device and System Security comments

CI **All P** SC **Annex A** P **161** L **13** # **82**
 Sukert, Alan Xerox

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

The definition of TOE owner in Annex A is not consistent with the corresponding definition in PP-A subclause 5.4, page 7, line 30.

Subclause 5.4, page 7, line 30 -- TOE Owner describes person or organizational entity which is responsible for protecting TOE assets and establishing related security policies. Note that there is a typo in the subclause 5.4 definition - 'protecting' is misspelled.

Annex A -- TOE Owner: person or group with overall responsibility for TOE assets and related security policies.

Note that the same comments applies to the other three PPs as follows:
 -- PP-B: See subclause 5.4, page 7, line 29 vs. Annex A, page 159, line 13
 -- PP-C: See subclause 5.4, page 7, line 29 vs. Annex A, page 131, line 13
 -- PP-D: See subclause 5.4, page 6, line 27 vs. Annex A, page 94, line 13

SuggestedRemedy

In all four PPs, make the definition of TOE Owner consistent between subclause 5.4 and Annex A. Also correct the misspelling as necessary in the subclause 5.4 definition.

Note that the proposed updated Annex A to address Comment #124 will also help address this comment.

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

Use:

TOE Owner is a person or organizational entity responsible for protecting TOE assets and establishing related security policies.

CI **Annex** SC P **154** L **33** # **102**
 Volkoff, Brian HP

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

Recommendations and table are not consistent (and do not reference) with current recommendations/publications by NIST and the US DoD.

SuggestedRemedy

Include references to NIST and DoD publications.

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

This comment was WITHDRAWN by the commenter.

This comment was for P2600 and will be routed to sponsor ballot.

CI **PP-A** SC **11.1.1** P **97** L **17** # **2**
 aubry, carmen oce

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

Only the "Originator may be able to retrieve, modify, and store his own TSF Protected Data or TSF Confidential Data (e.g. user profile information, user password)."

How about the delegate, how is he supposed to create/modify/store it's credentials, for instance?

SuggestedRemedy

The Delegate may be able to retrieve, modify, and store his own TSF Protected Data or TSF Confidential Data (e.g. user profile information, user password).

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

Add a bullet "g" using suggested text.

IEEE P2600 Hardcopy Device and System Security comments

CI **PP-A** SC 12.2.1 P 119 L 24 # 58
 Smithson, Brian Ricoh

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

In tables 84 and 86, D.DOC.REST is referenced. I would be more consistent with the other TOEs if these were changed to the subclasses D.DOC.JOB, D.DOC.OUTPUT, and D.DOC.RETRIEVE. This would also be more accurate in table 86, because there is no "see also" TOE for D.DOC.JOB disclosure/alteration. Threats and objectives in the NVS TOE would also need to be changed. However, this would make it possible to remove the hierarchical structure of assets in Table 3 and Figure 4, and the confusing PP APP NOTE #2 after Table 3 could be removed. Instead, an app note could be inserted that said that the P2600 D.DOC.REST is composed of the P2600.1 .JOB, .RETRIEVE, and .OUTPUT.

SuggestedRemedy

Separate D.DOC.REST into its three subclasses in NVS TOE. Also separate the related threats and objectives. Remove the hierarchy of those assets in Table 3 and Figure 4 (and remove D.DOC.REST from Table 3 entirely). Remove the 2nd PP app note after Table 3, and insert a new one that equates P2600's D.DOC.REST with the PP's D.DOC.JOB|OUTPUT|RETRIEVE.

Applies also to PP-B, same page/line number.

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

In figure 4, draw dotted line box around .JOB, .OUTPUT and .RETRIEVE to equate them with D.DOC.REST in P2600

CI **PP-A** SC 12.2.2 P 120 L 6 # 57
 Smithson, Brian Ricoh

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

Assets not considered in NVS should also include D.DOC and D.FUNC

SuggestedRemedy

Add rows to table for D.DOC and D.FUNC, with rationale that NVS does not have any User Data, see also N/A.

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

Fully qualify D.DOC and D.FUNC.

CI **PP-A** SC 12.3.1 P 121 L 26 # 3
 aubry, carmen oce

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

(Table 91 Security objectives for the NVS TOE) The PP is asking for "The TOE shall protect deleted User Document Data on behalf of the Subject of another TOE in a nonvolatile storage medium that has been removed from TOE from unauthorized salvage."

Does this requirement cover the entire "non volatile storage" or only the spool?
 I'm interpreting it like the entire "non volatile storage" and that it is up to the manufacturer to employ the architecture that guarantees it (not using swap file or preventing some data to arrival in the swap file or overwriting the swap at boot... whatever he chooses).

SuggestedRemedy

We should specify somewhere (the guide to the PPs might be a good place) what was our intention:

- 1) do we want to ask the entire NVS be considered or
 - 2) do we want to allow the manufacturer to decide if he wants to overwrite only the spool.
- I'm not sure that with the current formulation, the CC evaluation labs and the CC schemes will have the same interpretation.

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

Create an App note that more accurately describes the intention but doesn't mandate spool and/or swap. For example an assumption could be in the ST that sophistication of the attacker is insufficient to recover data from the swap file. (Volunteer to write the note = Peter/Ron)

CI **PP-A** SC 13.5.5 P 148 L 23 # 59
 Smithson, Brian Ricoh

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

PP app note for FDP_IFC.1.1 refers to old objectives O.COMMS.NO_PROXY and O.COMMS.NO_BRIDGE

SuggestedRemedy

Replace O.COMMS.NO_PROXY and O.COMMS.NO_BRIDGE with O.SMI.MEDIATED.

Also applies to PP-B: P.147 L.11

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

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-A** SC **13.5.5** P **148** L **23** # **60**
 Smithson, Brian Ricoh

Comment Type **T** Comment Status **D**
 App note for FDP_IFC.1 should say O.DOC(+OTHERTOE)..., O.FUNC(+OTHERTOE)..., O.PROT(+OTHERTOE)..., and O.CONF(+OTHEROE)... Same for FTP_TRP.1.

SuggestedRemedy
 Replace O.DOC with O.DOC(+OTHERTOE), and O.FUNC with O.FUNC(+OTHERTOE). Add O.PROT(+OTHERTOE) and add O.CONF(+OTHERTOE) to the app note. Also need to make these changes to app note for FTP_TRP.1 and to Table 116 and 117.

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

Cl **PP-A** SC **13.5.7** P **152** L **15** # **61**
 Smithson, Brian Ricoh

Comment Type **T** Comment Status **D**
 App note should also say that FMT_MSA.3 is a dependency of FDP_IFF.1

SuggestedRemedy
 add to app note of FMT_MSA.3 ""and FDP_IFF.1""
 Also applies to PP-B P.151 L.1

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

Cl **PP-A** SC **7.1.1** P **15** L **23** # **1**
 aubry, carmen oce

Comment Type **T** Comment Status **D**
 Only the "Originator may be able to retrieve, modify, and store his own TSF Protected Data or TSF Confidential Data (e.g. user profile information, user password)."

How about the delegate, how is he supposed to create/modify/store it's credentials, for instance?

SuggestedRemedy
 The Delegate should be able to to retrieve, modify, and store his own TSF Protected Data or TSF Confidential Data (e.g. user profile information, user password).

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

See resolution for comment #2

Cl **PP-A** SC **7.1.2** P **16** L **9** # **4**
 aubry, carmen oce

Comment Type **T** Comment Status **D**
 "All users are identified and authenticated, and are authorized before being granted permission to perform PRT functions."

The PP asks the Printer to require (or perform) user authentication before receiving any print job. A large number of customers in enterprise environments are using print servers (the end-user is not directly printing to the printer). In this case, the print server requires (or performs) user authentication and not the printer.

What interpretation should be given (for the quoted requirement) when a print server is located between the end-user and the printer?
 1)It is mandatory that the printer requires (or performs) END-USER authentication OR
 2)The printer requires (or performs) user authentication but in this case the "user" may be the "print server"

SuggestedRemedy
 I think that the second case should be allowed in order to facilitate PP acceptance in enterprise environments. Document somewhere (PP guide, for instance) P2600 group recommendation.

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

No change. If the print server is outside the TOE it is not the subject of this PP.

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-A** SC **7.2.3** P **19** L **1** # **97**
 Sukert, Alan Xerox

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

In the PP-A Table 9 definition for P.AUDIT.LOGGING, the policy says that the audit log should be reviewed by authorized personnel. The policy is not sufficient as stated to meet the O.AUDIT.LOGGED objective of preventing unauthorized disclosure of the audit log. The policy must state that only authorized personnel can review the audit log; otherwise you can't guarantee that there is no unauthorized disclosure because the policy doesn't explicitly forbid non-authorized personnel from reviewing the audit log.

A similar comment applies to:
 -- PP-A: subclause 8.2.3, page 39, line 11; subclause 9.2.3, page 59, line 10; subclause 10.2.3, page 80, line 6; subclause 11.2.3, page 101, line 1 and subclause 12.2.3, page 120, line 13.

-- PP-B: subclause 7.2.3, page 18, line 11; subclause 8.2.3, page 39, line 11; subclause 9.2.3, page 58, line 10; subclause 10.2.3, page 79, line 1; subclause 11.2.3, page 100, line 1 and subclause 12.2.3, page 119, line 13.

-- PP-C: subclause 7.2.3, page 16, line 15; subclause 8.2.3, page 33, line 1; subclause 9.2.3, page 48, line 15; subclause 10.2.3, page 64, line 9; subclause 11.2.3, page 80, line 8 and subclause 12.2.3, page 95, line 10.

SuggestedRemedy

Revise P.AUDIT.LOGGING to read "...by the TOE, and will be reviewed only by authorized personnel." in all the subclauses indicated in the comment above for PP-A, PP-B and PP-C.

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

This comment was WITHDRAWN by the commenter.

Cl **PP-A** SC **7.5.1.1** P **22** L **1** # **98**
 Sukert, Alan Xerox

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

For PP-A, in Table 14 on page 22, the access control rule for D.DOC.OUTPUT says that a document may be released to an output handler if granted permission to do so by the originator. I can think of scenarios where an Administrator might also grant permission for release of a document to an output handler - for example, if the Administrator sets a time limit for a delayed print job to be held by the device and then a user submits a delayed print job but doesn't release the job before the time limit is exceeded, the device will automatically release the print job which in essence means the administrator (by setting the time limit) authorized release of that job and not the originator. There probably are other scenarios like this.

Note that this same comment applies to PP-B, subclause 7.5.1.1, page 21, line 9.

SuggestedRemedy

In PP-A and PP-B, revise the access control rule for D.DOC.OUTPUT in subclause 7.5.1.1 to read "...if granted permission to do so by U.ORIGINATOR or U.ADMINISTRATOR."

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

Cl **PP-A** SC **7.5.4** P **26** L **26** # **95**
 Sukert, Alan Xerox

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

There is a typographical error in the PP Application Note -- 'FDP_AC F.1' should be 'FDP_ACF.1'.

This same comment applies to PP-A in the following subclauses:

- subclause 8.5.5, page 47, line 18
- subclause 9.5.5, page 67, line 16
- subclause 10.5.5, page 88, line 3 and
- subclause 11.5.5, page 109, line 3

This same comment also applies to PP-B in the following subclauses:

- subclause 7.5.5, page 26, line 22
- subclause 8.5.5, page 47, line 3
- subclause 9.5.5, page 66, line 16
- subclause 10.5.5, page 87, line 3 and
- subclause 11.5.5, page 108, line 3.

SuggestedRemedy

Correct the typographical error indicated above in the indicated subclauses for PP-A and PP-B.

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

IEEE P2600 Hardcopy Device and System Security comments

CI **PP-A** SC **7.5.5** P **26** L **3** # **101**
 Sukert, Alan Xerox

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

There is a typographical error in the PP Application Note in PP-A -- 'FDP_AC C.1' should be 'FDP_ACC.1'.

This same comment applies to PP-A in the following subclauses:

- subclause 8.5.5, page 46, line 21
- subclause 8.5.6, page 47, line 29
- subclause 9.5.5, page 66, line 21
- subclause 9.5.6, page 67, line 27
- subclause 10.5.5, page 87, line 9
- subclause 11.5.5, page 108, line 9
- subclause 12.5.6, page 129, line 11 and
- subclause 13.5.6, page 150, line 3

This same comment also applies to PP-B in the following subclauses:

- subclause 7.5.5, page 25, line 24
- subclause 8.5.5, page 46, line 11
- subclause 8.5.6, page 47, line 14
- subclause 9.5.5, page 65, line 21
- subclause 9.5.6, page 66, line 27
- subclause 10.5.5, page 86, line 9
- subclause 11.5.5, page 107, line 9
- subclause 12.5.6, page 128, line 11 and
- subclause 13.5.6, page 148, line 17

This same comment applies to PP-A in the following subclauses:

- subclause 8.5.5, page 46, line 21
- subclause 8.5.6, page 47, line 29
- subclause 9.5.5, page 66, line 21
- subclause 9.5.6, page 67, line 27
- subclause 10.5.5, page 87, line 9
- subclause 11.5.5, page 108, line 9
- subclause 12.5.6, page 129, line 11 and
- subclause 13.5.6, page 150, line 3

This same comment also applies to PP-C in the following subclauses:

- subclause 8.5.6, page 39, line 13
- subclause 9.5.6, page 55, line 27
- subclause 12.5.6, page 102, line 15 and
- subclause 13.5.6, page 121, line 14

This same comment also applies to PP-D in the following subclauses:

- subclause 8.5.6, page 31, line 3
- subclause 9.5.6, page 43, line 1 and
- subclause 12.5.6, page 83, line 14

SuggestedRemedy

Correct the typographical error indicated above in the indicated subclauses in all four PPs.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Duplicate of #87.

CI **PP-A** SC **7.6** P **34** L **1** # **100**
 Sukert, Alan Xerox

Comment Type **G** Comment Status **D**

In PP-A to be consistent with capitalization used throughout the rest of the document in the Description of the O.USER.AUTHORIZED & O.ADMIN.AUTHORIZED security objectives both 'user' and/or 'administrators' should be captialized in the following subclauses: subclause 7.6, page 34, line 1 (Table 19); subclause 8.6, page 54, line 1 (Table 35); subclause 9.6, page 74, line 1 (Table 51); subclause 10.6, page 95, line 1 (Table 67); subclause 11.6, page 116, line 1 (Table 83); subclause 12.6, page 135, line 1 (Table 99) and subclause 13.6, page 157, line 1 (Table 117)

The same comment applies to the other three PPs as follows:

PP-B: subclause 7.6, page 34, line 1 (Table 19); subclause 8.6, page 54, line 1 (Table 35); subclause 9.6, page 74, line 1 (Table 51); subclause 10.6, page 94, line 1 (Table 67); subclause 11.6, page 115, line 1 (Table 83); subclause 12.6, page 134, line 1 (Table 99) and subclause 13.6, page 156 line 1 (Table 115)

PP-C: subclause 7.6, page 28, line 1 (Table 17); subclause 8.6, page 45, line 1 (Table 31); subclause 9.6, page 60, line 1 (Table 45); subclause 10.6, page 76, line 1 (Table 59); subclause 11.6, page 92, line 1 (Table 73); subclause 12.6, page 108, line 1 (Table 89) and subclause 13.6, page 127 line 1 (Table 105)

PP-D: subclause 7.6, page 23, line 3 (Table 15); subclause 8.6, page 27, line 2 (Table 27); subclause 9.6, page 47, line 2 (Table 39); subclause 10.6, page 60, line 2 (Table 51); subclause 11.6, page 73, line 1 (Table 63); and subclause 12.6, page 90, line 1 (Table 77)

SuggestedRemedy

Make the capitalization of user and administrators in the above subclauses for each of the four PPs consistent with the remainder of each PP document.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Shall be capitalized

IEEE P2600 Hardcopy Device and System Security comments

CI **PP-A** SC **8.1.1** P **36** L **27** # **99**
 Sukert, Alan Xerox

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

In PP-A, the change made to subclause 7.1.1, page 15, line 26 to add 'during' to the sentence needs to be made to this line also, as well as to subclause 9.1.1, page 56, line 24; subclause 10.1.1, page 76, line 37; subclause 11.1.1, page 97, line 28; subclause 12.1.1, page 118, line 21 and subclause 13.1.1, page 136, line 18.

SuggestedRemedy

Either (1) add the change from subclause 7.1.1, page 15, line 26 to subclause 8.1.1, page 26, line 27; subclause 9.1.1, page 56, line 24; subclause 10.1.1, page 76, line 37; subclause 11.1.1, page 97, line 28; subclause 12.1.1, page 118, line 21 and subclause 13.1.1, page 136, line 18 or (2) remove this change made to subclause 7.1.1, page 15, line 26.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

CI **PP-A** SC **8.2.1** P **38** L **25** # **96**
 Sukert, Alan Xerox

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

In Table 22, I believe that the reference to the 'DSR TOE' in the rationale for the D.DOC.OUTPUT asset not being applicable to the SCN TOE should be to the 'SCN TOE'.

SuggestedRemedy

Replace 'DSR TOE' with 'SCN TOE'.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

CI **PP-A** SC **Annex A** P **160** L **1** # **93**
 Sukert, Alan Xerox

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

PP-A Annex A does not include the definition of the Channel entity, although Channel is defined in subclause 5.5.5, page 12, line 23.

A similar comment applies to the other three PPs as follows:

- PP-B: subclause 5.5.5, page 12, line 16 vs. Annex A, page 158, line 1
- PP-C: subclause 5.5.5, page 12, line 1 vs. Annex A, page 130, line 1
- PP-D: subclause 5.5.5, page 10, line 17 vs. Annex A, page 93, line 1

SuggestedRemedy

Include the following definition in Annex A in all four PPs:

Channel: The mechanisms through which data can be transferred into and out of the TOE.

Note that the updated Annex A proposed to address Comment #224 also addresses this comment.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Fixed in Annex A

CI **PP-A** SC **Annex A** P **160** L **1** # **92**
 Sukert, Alan Xerox

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

PP-A Annex A does not include the definition of the Operation entity, although Operation is defined in subclause 5.5.4, page 12, line 16.

A similar comment applies to the other three PPs as follows:

- PP-B: subclause 5.5.4, page 12, line 9 vs. Annex A, page 158, line 1
- PP-C: subclause 5.5.4, page 11, line 14 vs. Annex A, page 130, line 1
- PP-D: subclause 5.5.4, page 10, line 10 vs. Annex A, page 93, line 1

SuggestedRemedy

Include the following definition in Annex A in all four PPs: Operation: A specific type of action performed by a Subject on an Object.

Note that the updated Annex A proposed to address Comment #224 also addresses this comment.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Fixed in Annex A

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-A** SC **Annex A** P **160** L **1** # **94**
 Sukert, Alan Xerox

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

The current Annex A Glossary included in each of the four PPs is incomplete and inadequate for the following reasons:

1. Several terms such as User Document Data have definitions that do not agree with their corresponding definitions in P2600 Clause 2.
2. Several CC-related terms such as TOE are not included in Annex A.
3. Definitions for several terms used in the PPs, such as User Data, are not included in Annex A.
4. The definitions in Annex A of several terms, such as object and subject, do not agree with the corresponding definitions in the main text of the PPs.

Annex A needs to be updated to address all the terms that fall into each of these four categories.

SuggestedRemedy

Rather than address each problem individually, substitute the proposed Annex A (which is attached to the E-mail with these comments) that addresses the above issues for the Annex A currently in each of the PPs.

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

See version 31b for a modified version of Annex A.

Cl **PP-B** SC P **136** L **3** # **5**
 aubry, carmen oce

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

The following "major security feature" does not correspond to an asset (in Table 100 - TSF Data assets of the SMI):

"b) The SMI TOE can protect the User Data and TSF Data of the Subject of another TOE from disclosure or alteration when such Assets are exchanged with external entities over shared communications media."

SuggestedRemedy

This feature should be removed.

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

Only remove User Data and leave TSF Data

Cl **PP-B** SC **13.5.5** P **147** L **11** # **62**
 Smithson, Brian Ricoh

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

App note for FDP_IFC.1 should also include O.PROT(+OTHERTOE)..., and O.CONF(+OTHERTOE)... Same for FTP_TRP.1.

SuggestedRemedy

Add O.PROT(+OTHERTOE) and add O.CONF(+OTHERTOE) to the app note. Also need to make these changes to app note for FTP_TRP.1 and to Table 116 and 117.

Also applies to PP-C P.120 L.11, and PP-D (12.5.5) P.82 L.11

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

Cl **PP-C** SC **10.1.1** P **61** L **27** # **21**
 Chen, Nancy Oki Data

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

This sentence does not read right.

SuggestedRemedy

Change to "Additional TSF data (e.g. audit logs) may be created or updated during the performance of administrative tasks."

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

Same as comment #99

Cl **PP-C** SC **10.5.1.1** P **66** L **10** # **22**
 Chen, Nancy Oki Data

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

Only Administrator has access to Protected Data and Confidential Data in Environment C.

SuggestedRemedy

Remove access to assets for Originator from Table 54.

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

IEEE P2600 Hardcopy Device and System Security comments

CI **PP-C** SC 10.5.7 P 73 L 4 # 23
 Chen, Nancy Oki Data
 Comment Type **E** Comment Status **D**
 Wrong SFR cited in Application Note.
 SuggestedRemedy
 Change FMT_MSA.1 to FMT_SMF.1
 Proposed Response Response Status **W**
 PROPOSED ACCEPT.
 Same as comment #42

CI **PP-C** SC 11.5.1.1 P 82 L 10 # 24
 Chen, Nancy Oki Data
 Comment Type **T** Comment Status **D**
 Only Administrator has access to Protected Data and Confidential Data in Environment C.
 SuggestedRemedy
 Remove access to assets for Originator from Table 68.
 Proposed Response Response Status **W**
 PROPOSED ACCEPT.
 See comment #22

CI **PP-C** SC 11.5.6 P 86 L 25 # 25
 Chen, Nancy Oki Data
 Comment Type **T** Comment Status **D**
 O.USER.AUTHORIZED is not an objective in Environment C.
 SuggestedRemedy
 Remove O.USER.AUTHORIZED from the Application Note.
 Proposed Response Response Status **W**
 PROPOSED ACCEPT.

CI **PP-C** SC 11.5.6 P 86 L 25 # 68
 Smithson, Brian Ricoh
 Comment Type **T** Comment Status **D**
 PP app note after FIA_AFL.1 should not include O.USER.AUTHORIZED
 SuggestedRemedy
 Remove ""O.USER.AUTHORIZED and "" from the app note.
 Proposed Response Response Status **W**
 PROPOSED ACCEPT.
 Same as #25

CI **PP-C** SC 11.5.7 P 88 L 19 # 69
 Smithson, Brian Ricoh
 Comment Type **T** Comment Status **D**
 2nd app note after FMT_MTD.1 does not apply to this environment
 SuggestedRemedy
 Remove 2nd app note ("In typical applications...") from FMT_MTD.1.
 Proposed Response Response Status **W**
 PROPOSED ACCEPT.

CI **PP-C** SC 11.5.7 P 88 L 20 # 26
 Chen, Nancy Oki Data
 Comment Type **T** Comment Status **D**
 Only Administrator has access to Protected Data and Confidential Data in Environment C.
 SuggestedRemedy
 Remove the sentence: U.ORIGINATOR can modify some TSF Data when such data was created for that user (for example, a user's own password).
 Proposed Response Response Status **W**
 PROPOSED ACCEPT.

IEEE P2600 Hardcopy Device and System Security comments

CI **PP-C** SC 11.5.7 P 89 L 7 # 27
 Chen, Nancy Oki Data
 Comment Type **E** Comment Status **D**
 Wrong SFR cited in Application Note.
 SuggestedRemedy
 Change FMT_MSA.1 to FMT_SMF.1
 Proposed Response Response Status **W**
 PROPOSED ACCEPT.
 Same as #42

CI **PP-C** SC 12.5.7 P 104 L 23 # 30
 Chen, Nancy Oki Data
 Comment Type **E** Comment Status **D**
 Wrong SFR cited in Application Note.
 SuggestedRemedy
 Change FMT_MSA.1 in the Application Note to FMT_SMF.1
 Proposed Response Response Status **W**
 PROPOSED ACCEPT.
 Same as #42

CI **PP-C** SC 12.5.2 P 100 L 9 # 28
 Chen, Nancy Oki Data
 Comment Type **E** Comment Status **D**
 FDP_ACC.1 is not required in Environment C.
 SuggestedRemedy
 Delete FDP_ACC.1 from the Application Note.
 Proposed Response Response Status **W**
 PROPOSED ACCEPT IN PRINCIPLE.
 Remove FDP_ACF.1 here and everywhere in C.
 If FDP_ACC.1 shows up in C, it should be removed as well.

CI **PP-C** SC 13.1.1 P 109 L 17 # 31
 Chen, Nancy Oki Data
 Comment Type **E** Comment Status **D**
 This sentence does not read right.
 SuggestedRemedy
 Change to ""Additional TSF data (e.g. audit logs) may be created or updated during the performance of administrative tasks.""
 Proposed Response Response Status **W**
 PROPOSED ACCEPT.
 Same as #99

CI **PP-C** SC 12.5.6 P 102 L 15 # 29
 Chen, Nancy Oki Data
 Comment Type **E** Comment Status **D**
 Wrong SFR cited in Application Note.
 SuggestedRemedy
 Change FDP_ACC.1 in the Application Note to FIA_AFL.1
 Proposed Response Response Status **W**
 PROPOSED ACCEPT.

CI **PP-C** SC 13.1.2 P 110 L 1 # 32
 Chen, Nancy Oki Data
 Comment Type **T** Comment Status **D**
 Only Administrator is identified and authenticated in Environment C.
 SuggestedRemedy
 Change ""All users"" to Administrator. Change ""SMI functions"" to ""SMI management functions"".
 Proposed Response Response Status **W**
 PROPOSED ACCEPT.

IEEE P2600 Hardcopy Device and System Security comments

CI **PP-C** SC **13.1.2** P **110** L **710** # **33**
 Chen, Nancy Oki Data
 Comment Type **T** Comment Status **D**
 Only Administrator is identified, authenticated and authorized to access TSF data in Environment C.
 SuggestedRemedy
 Delete "originating user and" from the sentence.
 Proposed Response Response Status **W**
 PROPOSED ACCEPT.

CI **PP-C** SC **13.5.1.1** P **116** L **7** # **36**
 Chen, Nancy Oki Data
 Comment Type **T** Comment Status **D**
 In a typical environment C only administrator is required to be identified, authenticated, and authorized. However it's important to identify and authenticate external IT entities should exchange of Protected Data or Confidential Data is required between MFD and an external IT entity. Public facing businesses that subject to government regulations or require higher level of security against U.EXTENTIVITY should use HCDs compliant to PP for environment A or B.
 SuggestedRemedy
 (1) Change U.EXTENTIVITY in SMI Access Control SFP Table to U.ExtITEntity.
 (2) Replace each U.EXTENTIVITY in the Information Flow Control SFP with ""U.ExtITEntity and Remote Administrator"" under the new definition of Users.
 Proposed Response Response Status **W**
 PROPOSED ACCEPT IN PRINCIPLE.

We have changed a number of definitions in the changes to Annex A (V31a) provided by Alan Sukert. Please verify that these changes address your concern. V31b is the version that will be inserted in all four PPs.

CI **PP-C** SC **13.5.6** P **121** L **14** # **34**
 Chen, Nancy Oki Data
 Comment Type **E** Comment Status **D**
 Wrong SFR cited in Application Note.
 SuggestedRemedy
 Change FDP_ACC.1 in the Application Note to FIA_AFL.1
 Proposed Response Response Status **W**
 PROPOSED ACCEPT.

CI **PP-C** SC **13.5.7** P **122** L **19** # **71**
 Smithson, Brian Ricoh
 Comment Type **T** Comment Status **D**
 FMT_MSA.1 and FMT_MSA.3 should not have been removed from the SMI TOE. FMT_MSA.3 is a dependency of FDP_IFF.1, and FMT_MSA.1 is a dependency of FMT_MSA.3.
 SuggestedRemedy
 Add FMT_MSA.1 and FMT_MSA.3 into the SMI TOE. Add FMT_MSA.1 to the app note for FMT_SMF.1. Add FMT_MSA.1 and FMT_MSA.3 to the app note for FMT_SMR.1. Add FMT_MSA.1 and FMT_MSA.3 to appropriate places in SMI completeness and sufficiency tables. See P2600.4-31a for example.
 Proposed Response Response Status **W**
 PROPOSED ACCEPT.

CI **PP-C** SC **13.5.7** P **123** L **14** # **35**
 Chen, Nancy Oki Data
 Comment Type **E** Comment Status **D**
 Wrong SFR cited in Application Note.
 SuggestedRemedy
 Change FMT_MSA.1 in the Application Note to FMT_SMF.1, Delete FDP_ACF.1
 Proposed Response Response Status **W**
 PROPOSED ACCEPT.

CI **PP-C** SC **5.5.1** P **8** L **5** # **65**
 Smithson, Brian Ricoh
 Comment Type **T** Comment Status **D**
 Originator and Delegate are not used in this environment.
 SuggestedRemedy
 Replace text with "There may be three types of Users: Anonymous User, Administrator, and External Entity."
 Change figure 2: replace Originator and Delegate with Anonymous User.
 Change Table 1 accordingly.
 Change all references to Originator and/or Delegate accordingly throughout the FoPP. See P2600.4-31a for example.
 Proposed Response Response Status **W**
 PROPOSED ACCEPT IN PRINCIPLE.
 Remove Originator and Delegate but don't add Anonymous User as an entity. References to an anonymous user should not be capitalized.

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-C** SC **5.5.3** P **11** L **4** # **63**
 Smithson, Brian Ricoh
 Comment Type **T** Comment Status **D**
 Second PP app note after Asset table does not apply to PP-C.
 SuggestedRemedy
 Remove second PP app note.
 Proposed Response Response Status **W**
 PROPOSED ACCEPT.

Cl **PP-C** SC **7.1.1** P **14** L **13** # **64**
 Smithson, Brian Ricoh
 Comment Type **T** Comment Status **D**
 User Function Data should not be referenced in this TOE for env C.
 SuggestedRemedy
 Remove ""User Function Data (e.g. print status) and "" from line 13.
 Proposed Response Response Status **W**
 PROPOSED ACCEPT.

Cl **PP-C** SC **7.5.1.1** P **19** L **5** # **9**
 Chen, Nancy Oki Data
 Comment Type **T** Comment Status **D**
 Only Administrator has access to Protected Data and Confidential Data in Environment C.
 SuggestedRemedy
 Remove access for Originator from Table 12.
 Proposed Response Response Status **W**
 PROPOSED ACCEPT.

Cl **PP-C** SC **7.5.2** P **20** L **18** # **10**
 Chen, Nancy Oki Data
 Comment Type **E** Comment Status **D**
 FDP class, FMT_MSA are not required in Environment C.
 SuggestedRemedy
 Remove FDP_ACF.1, FMT_MSA.1, FMT_MSA.3 from the PP Application Note.
 Proposed Response Response Status **W**
 PROPOSED ACCEPT IN PRINCIPLE.
 FMT_MSA.1 is require for the SMI TOE.

Cl **PP-C** SC **7.5.2** P **20** L **19** # **70**
 Smithson, Brian Ricoh
 Comment Type **T** Comment Status **D**
 Multiple app notes still refer to FMT_MSA.1 and FMT_MSA.3, which are not present except in SMI TOE
 SuggestedRemedy
 Remove all references to FMT_MSA.1 and FMT_MSA.3 in all TOEs except in the SMI TOE.
 There are many subclause/page/line numbers to which this applies, see the numbers above for first example in PP-A.
 Proposed Response Response Status **W**
 PROPOSED ACCEPT.

Cl **PP-C** SC **8.1.1** P **30** L **21** # **11**
 Chen, Nancy Oki Data
 Comment Type **E** Comment Status **D**
 This sentence does not read right.
 SuggestedRemedy
 Change to ""Additional TSF data (e.g. audit logs) may be created or updated during the performance of administrative tasks.""
 Proposed Response Response Status **W**
 PROPOSED ACCEPT.

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-C** SC **8.5.1.1** P **35** L **9** # **12**
 Chen, Nancy Oki Data
 Comment Type **T** Comment Status **D**
 Only Administrator has access to Protected Data and Confidential Data in Environment C.
 SuggestedRemedy
 Remove access for Originator from Table 26.
 Proposed Response Response Status **W**
 PROPOSED ACCEPT.

Cl **PP-C** SC **8.5.2** P **39** L **13** # **14**
 Chen, Nancy Oki Data
 Comment Type **E** Comment Status **D**
 Wrong SFR cited in Application Note.
 SuggestedRemedy
 Change FDP_ACC.1 in the Application Note to FIA_AFL.1
 Proposed Response Response Status **W**
 PROPOSED ACCEPT.

Cl **PP-C** SC **8.5.11** P **43** L **7** # **15**
 Chen, Nancy Oki Data
 Comment Type **E** Comment Status **D**
 O.USER.AUTHORIZED is not an objective in Environment C.
 SuggestedRemedy
 Remove O.USER.AUTHORIZED from the Application Note.
 Proposed Response Response Status **W**
 PROPOSED ACCEPT.

Cl **PP-C** SC **8.5.7** P **41** L **22** # **66**
 Smithson, Brian Ricoh
 Comment Type **E** Comment Status **D**
 Extra linebreak between 22-23
 SuggestedRemedy
 Remove linebreak between ""dependency of"" and ""FMT_MTD.1"".
 Proposed Response Response Status **W**
 PROPOSED ACCEPT.

Cl **PP-C** SC **8.5.2** P **37** L **4** # **13**
 Chen, Nancy Oki Data
 Comment Type **E** Comment Status **D**
 FMT_MSA is not required in Environment C.
 SuggestedRemedy
 Remove FMT_MSA.1, FMT_MSA.3 from the PP Application Note.
 Proposed Response Response Status **W**
 PROPOSED ACCEPT IN PRINCIPLE.
 FMT_MSA.1 is required in SMI

Cl **PP-C** SC **8.6** P **43** L **15** # **16**
 Chen, Nancy Oki Data
 Comment Type **E** Comment Status **D**
 FDP_ACC.1 and FDP_ACF.1, FMT_MSA.1 and FMT_MSA.3 are not required in Environment C.
 SuggestedRemedy
 Remove FDP_ACF.1, FDP_ACC.1, FMT_MSA.1, FMT_MSA.2 from Table 30 & Table 31.
 Proposed Response Response Status **W**
 PROPOSED ACCEPT.

Note: Fix the table formatting in all profiles where the column heading, "SFR", has wandered down into the first row.

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-C** SC **8.6** P **43** L **16** # **67**
 Smithson, Brian Ricoh

Comment Type **T** Comment Status **D**
 O.USER.AUTHORIZED and O.FUNC.REST.NO_ALT should not be in tables 30 and 31.

SuggestedRemedy
 Remove O.USER.AUTHORIZED and O.FUNC.REST.NO_ALT columns from table 30.
 Remove FDP_ACC and FDP_ACF rows from table 30. Remove O.USER.AUTHORIZED
 spanned rows from table 31. Remove O.USER.AUTHORIZED from table 31 (leave
 O.ADMIN.AUTHORIZED) and remove the words "users and" from that row.

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

Cl **PP-C** SC **9.1.1** P **46** L **18** # **17**
 Chen, Nancy Oki Data

Comment Type **E** Comment Status **D**
 This sentence does not read right.

SuggestedRemedy
 Change to "Additional TSF data (e.g. audit logs) may be created or updated during the
 performance of administrative tasks."

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

Cl **PP-C** SC **9.5.1.1** P **51** L **5** # **18**
 Chen, Nancy Oki Data

Comment Type **E** Comment Status **D**
 Only Administrator has access to Protected Data and Confidential Data in Environment C.

SuggestedRemedy
 Remove access to assets for Originator from Table 40.

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

Cl **PP-C** SC **9.5.6** P **55** L **11** # **19**
 Chen, Nancy Oki Data

Comment Type **E** Comment Status **D**
 Wrong SFR cited in Application Note.

SuggestedRemedy
 Change FDP_ACC.1 in the Application Note to FIA_AFL.1

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

Cl **PP-C** SC **9.5.7** P **57** L **12** # **20**
 Chen, Nancy Oki Data

Comment Type **E** Comment Status **D**
 Wrong SFR cited in Application Note.

SuggestedRemedy
 Change FMT_MSA.1 to FMT_SMF.1

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

Cl **PP-D** SC **7.5.11** P **22** L **17** # **7**
 aubry, carmen oce

Comment Type **T** Comment Status **D**
 Do we need FTA_SSL.3 in SoHo environments?
 FTA_SSL.3 TSF-initiated termination
 The TSF shall terminate an interactive session after a [assignment: time interval of user
 inactivity].

SuggestedRemedy
 Think at the impact on the use of Digest Authentication.

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

Committee member will investigate this issue for consideration with the next version of the
 document.

IEEE P2600 Hardcopy Device and System Security comments

CI **PP-D** SC 7.5.6 P 18 L 17 # 6
aubry, carmen oce

Comment Type T Comment Status D

Do we need FIA_AFL.1 and FIA_SOS.1 in SoHo environments?

FIA_AFL.1.1 The TSF shall detect when [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]] unsuccessful authentication attempts occur related to [assignment: list of authentication events].

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [assignment: a defined quality metric].

SuggestedRemedy

Think at the impact on the use of Digest Authentication.

Proposed Response Response Status W

PROPOSED REJECT.

Committee member will investigate this issue for consideration with the next version of the document.