

IEEE P2600 Hardcopy Device and System Security comments

CI **All P** SC **7.5.2** P L # **1**
 Chen, Nancy Oki Data

Comment Type **T** Comment Status **X**

Audit level of ""none"" with Additional information of ""none"" for a specified audit event in the Audit Data Requirements table and Audit Data Recommendations table could be very misleading. For example, does this mean that For this event, nothing should be audited. This applies to the same tables in all TOEs of all PPs.

SuggestedRemedy

According to PDTR_15446 Audit level from ""none"" should be changed to ""not specified"" which means the audit level is not one of the levels (minimum, basic, or detailed) specified by Common Criteria.

Proposed Response Response Status **O**

CI **P2600** SC **5.5** P L # **2**
 Chen, Nancy Oki Data

Comment Type **T** Comment Status **X**

Definitions of new terms such as security attribute name and nomenclature in Access Control table and Information Flow Control table should be added in Entity Definitions.

SuggestedRemedy

Add these new terminologies into Section 5.5 Entity Definitions.

Proposed Response Response Status **O**

CI **PP-C** SC **1.1** P **1** L **5** # **6**
 Sukert, Alan Xerox

Comment Type **E** Comment Status **X**

There is a grammatical error in the beginning of line 5 - 'standard' should be plural to agree with the corresponding verb 'are' on line 7.

SuggestedRemedy

Revise the first sentence in clause 1.1 to read ""Standards for a Protection Profile for Hardcopy Devices...are required."" or ""A standard for a Protection Profile for Hardcopy Devices...is required."" in all four PPs.

Proposed Response Response Status **O**

CI **PP-C** SC **1.4.1** P **2** L **2** # **7**
 Sukert, Alan Xerox

Comment Type **E** Comment Status **X**

'wholy' is misspelled; it should be 'wholly'.

SuggestedRemedy

Revise the indicated lines to read ""...in that row wholly or partially...""

Proposed Response Response Status **O**

CI **PP-C** SC **1.4.1** P **2** L **7** # **8**
 Sukert, Alan Xerox

Comment Type **E** Comment Status **X**

'secodary' is misspelled; it should be 'secondary'.

SuggestedRemedy

Revise the indicated lines to read ""indicates that it performs a secondary fulfillment.""

Proposed Response Response Status **O**

CI **PP-C** SC **11.1.1** P **76** L **13** # **13**
 Sukert, Alan Xerox

Comment Type **E** Comment Status **X**

The PP Application Note on this line has a grammatical error - says ""provided by that or those TOEs..."" and thus doesn't read correctly.

SuggestedRemedy

Change the line indicated above to read ""...and will use the Channel(s) and interface(s) provided by those TOEs...""

Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-C** SC **12.1.1** P **91** L **19** # **34**
 Sukert, Alan Xerox

Comment Type **T** Comment Status **X**

There appears to be an inconsistency between Figure 17 for the TOE model and Table 74 in subclause 12.2.1, page 92, line 1.

Figure 17 shows that the NVS TOE processes User Document Data from the Other TOE that is both deleted and at rest. However, subclause 12.2.1, page 92, line only describes D.DOC(+OTHERTOE).DELETED (i.e., User Document Data from the Other TOE that has been deleted).

SuggestedRemedy

Resolve the inconsistency between Figure 17 for the TOE model and Table 74 in subclause 12.2.1, page 92, line 1

Proposed Response Response Status **O**

Cl **PP-C** SC **12.5.5** P **100** L **4** # **18**
 Sukert, Alan Xerox

Comment Type **E** Comment Status **X**

The objective O.DOC(+OTHERTOE).DELETED.NO_SAL is misspelled on this line.

SuggestedRemedy

Correct the spelling of objective O.DOC(+OTHERTOE).DELETED.NO_SAL.

Proposed Response Response Status **O**

Cl **PP-C** SC **13.1.1** P **107** L **7** # **19**
 Sukert, Alan Xerox

Comment Type **E** Comment Status **X**

Per the convention used in the PPs, 'remote user' should be capitalized because it describes an entity.

Same comment applies to subclause 13.1.2, page 108, line 5.

SuggestedRemedy

Capitalize 'remote user' on the lines indicated above.

Proposed Response Response Status **O**

Cl **PP-C** SC **13.1.1** P **107** L **12** # **20**
 Sukert, Alan Xerox

Comment Type **E** Comment Status **X**

This line refers to the 'Shared-medium TOE'; it should be the 'SMI TOE' to be consistent with the rest of Subclause 13.

SuggestedRemedy

Change 'Shared-medium TOE' to 'SMI TOE'.

Proposed Response Response Status **O**

Cl **PP-C** SC **13.1.2** P **108** L **13** # **21**
 Sukert, Alan Xerox

Comment Type **E** Comment Status **X**

Per convention used in all PPs 'shared media interfaces' on lines 13 and 14 should be 'shared-medium interfaces'.

SuggestedRemedy

Replace 'shared media interfaces' with 'shared-medium interfaces'

Proposed Response Response Status **O**

Cl **PP-C** SC **13.2.4** P **111** L **1** # **26**
 Sukert, Alan Xerox

Comment Type **T** Comment Status **X**

Because the SMI TOE, as indicated in subclause 13.1.1, deals with the essential processing elements required to control access to and communications over shared communications media it is not clear why the A.LOCATION.SECURITY assumption and associated objective OE.LOCATION.SECURED are needed for this TOE or even make sense for this TOE. Since we are dealing with a communication media what location of the TOE needs to be secured or monitored. This assumption/objective pair can be eliminated for this TOE without sacrificing any security of the SMI TOE.

SuggestedRemedy

Remove A.LOCATION.SECURITY and OE.LOCATION.SECURED from the applicable tables in the subclause indicated above.

Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-C** SC **13.5.7** P **121** L **2** # **36**
 Yami, Sameer Toshiba
 Comment Type **T** Comment Status **X**
 'FMT_MSA.1 Management of security attributes' is introduced over here. It was not present in P2600.3-31a_RFQ.pdf.
 Is this a new requirement or was it missed in earlier document?
 SuggestedRemedy
 Put in a clarification for this change.
 Proposed Response Response Status **O**

Cl **PP-C** SC **13.6** P **126** L **1** # **14**
 Sukert, Alan Xerox
 Comment Type **E** Comment Status **X**
 In Table 105 for the O.SMI.MEDIATED objective, in the purpose of FDP_IFC.1 'shared media interface' should be 'shared-medium interface' to be consistent with the rest of the document..
 SuggestedRemedy
 Change 'shared media interface' to 'shared-medium interface' in the Tables indicated above.
 Proposed Response Response Status **O**

Cl **PP-C** SC **13.5.7** P **121** L **18** # **35**
 Yami, Sameer Toshiba
 Comment Type **T** Comment Status **X**
 FMT_MSA.3 Static attribute initialisation, is introduced over here.
 This was not present in 'P2600.3-31a_RFQ.pdf' though references are made throughout the document.
 Does this introduce a new requirement which was not there, or is this was missed in the earlier version
 SuggestedRemedy
 Put in a clarification for this change.
 Proposed Response Response Status **O**

Cl **PP-C** SC **13.6** P **127** L **1** # **27**
 Sukert, Alan Xerox
 Comment Type **T** Comment Status **X**
 The SFRs listed in Table 105 that are mapped to the O.CONF.REST_NO_DIS, O.PROT.REST_NO_ALT and O.CONF.REST_NO_ALT objectives does not agree with the SFRs that are mapped to these objectives in Table 104. Table 105 indicates that only the SFRs FMT_MTD.1 and FMT_SMR.1 map to these objectives; Table 104 also includes SFRs FIA_UID.1 and FMT_SMF.1.
 SuggestedRemedy
 Resolve the inconsistency between the tables indicated above as to what SFRs map to the O.CONF.REST_NO_DIS, O.PROT.REST_NO_ALT and O.CONF.REST_NO_ALT objectives.
 Proposed Response Response Status **O**

Cl **PP-C** SC **13.6** P **126** L **1** # **15**
 Sukert, Alan Xerox
 Comment Type **E** Comment Status **X**
 The description for O.SMI.MEDIATED in Table 105 has a misspelling - 'communication s medium interfaces' should be 'communications medium interfaces'.
 SuggestedRemedy
 Correct the description for O.SMI.MEDIATED as indicated above.
 Proposed Response Response Status **O**

Cl **PP-C** SC **4** P **3** L **32** # **22**
 Sukert, Alan Xerox
 Comment Type **G** Comment Status **X**
 In general acronyms, even if they are included in the acronyms list, should be defined the first time they are used within the document. On page 3, line 32 the acronym 'HCD' and on line 33 the acronym 'MFP' are used but not defined.
 SuggestedRemedy
 Include the definition of the acronyms HCD and MFP in page 3, lines 32 and 33. Make sure the same is done for all other acronyms in this PP.
 Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-C** SC 4 P 3 L 46 # 9
 Sukert, Alan Xerox

Comment Type **E** Comment Status **X**

The sentence in line 46 is not grammatically correct.

SuggestedRemedy

Revise the indicated lines to read "...that perform a scanning function in which physical document input is converted to electronic document output."

Proposed Response Response Status **O**

Cl **PP-C** SC 5.2 P 6 L 42 # 10
 Sukert, Alan Xerox

Comment Type **E** Comment Status **X**

The reference to 'Clause 5' in page 6, line 42 should be to 'Clause 4'.

SuggestedRemedy

Revise the indicated lines to read "A complete description of those environments can be found in IEEE Std. P2600, Clause 4."

Proposed Response Response Status **O**

Cl **PP-C** SC 5.3 P 7 L 5 # 16
 Sukert, Alan Xerox

Comment Type **E** Comment Status **X**

This line states "In order to create a Common Criteria profile that can be used...". Technically what is being created is a Common Criteria Protection Profile.

SuggestedRemedy

Revise the indicated lines to read "In order to create a Common Criteria Protection Profile that can be used..."

Proposed Response Response Status **O**

Cl **PP-C** SC 7.1.1 P 14 L 7 # 32
 Sukert, Alan Xerox

Comment Type **T** Comment Status **X**

The PRT TOE Model in item a) refers to an "anonymous user". First of all per the convention used in the other PPs 'user' should be capitalized because it refers to an entity. More importantly, the category of "anonymous user" isn't defined as one of the types of Users described in subclause 5.5.1 on page 8.

Note that this comment also applies to line 11 on page 14; subclause 8.1.1, page 29, lines 7 and 12; subclause 9.1.1, page 45, lines 7 and 11; subclause 10.1.1, page 60, lines 8 and 18 and subclause 11.1.1, page 76, lines 7 and 8.

Also, user needs to be capitalized in subclause 7.5.1.1, page 19, line 5; subclause 8.5.1.1, page 34, line 9; subclause 9.5.1.1, page 50, line 5; subclause 10.5.1.1, page 65, line 10; subclause 11.5.1.1, page 81, line 9 and subclause 13.5.1.1, page 114, line 5.

SuggestedRemedy

Capitalize 'user' on the subclauses and lines listed above.

Either define 'Anonymous User' in the applicable subclauses listed above or use one of the User types defined in the subclause defining the User types for each TOE.

Proposed Response Response Status **O**

Cl **PP-C** SC 7.1.1 P 14 L 22 # 33
 Sukert, Alan Xerox

Comment Type **T** Comment Status **X**

This comment is related to Comment #269. The 'anonymous User' described in lines 7 and 14 is not shown in Figure 7 - PRT TOE Model.

Same comment applies to Figure 9 in subclause 8.1.1, page 29, line 25; Figure 11 in subclause 9.1.1, page 45, line 22; Figure 13 in subclause 10.1.1, page 61, line 3 and Figure 15 in subclause 11.1.1, page 77, line 1;.

SuggestedRemedy

Include 'Anonymous User' in the TOE Model figures for the PRT TOE (Figure 7), SCN TOE (Figure 9), CPY TOE (Figure 11), FAX TOE (Figure 13) and DSR TOE (Figure 15).

Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security comments

CI **PP-C** SC **7.3.4** P **18** L **1** # **23**
 Sukert, Alan Xerox

Comment Type **T** Comment Status **X**

The definitions for OE.USER.AUTHORIZED and OE.ADMIN.AUTHORIZED are awkward and do not read correctly. You don't want the TOE owner to grant permission for the user (or admin) to be authorized to use (or manage) the HCD; I think you want the TOE owner to authorize the user (or admin) to use (or manage) the HCD.

The same comment applies to subclause 8.3.4, page 33, line 6; subclause 9.3.4, page 49, line 5; subclause 10.3.4, page 64, line 9; subclause 11.3.4, page 80, line 4; subclause 12.3.3.1, page 95, line 1 and subclause 13.3.3.1, page 112, line 10.

SuggestedRemedy

Consider changing the definitions for OE.USER.AUTHORIZED and OE.ADMIN.AUTHORIZED to read something like ""The TOE Owner shall authorize Users to use the TOE..."" and ""The TOE Owner shall authorize Administrators to manage the TOE..."", respectively in all the subclauses cited above.

Proposed Response Response Status **O**

CI **PP-C** SC **7.3.4** P **18** L **1** # **11**
 Sukert, Alan Xerox

Comment Type **E** Comment Status **X**

In the first row of Table 10, the definition of OE.LOCATION.SECURED has a grammatical error. The same comment applies to subclause 8.3.4, page 33, line 6; subclause 9.3.4, page 49, line 5; subclause 10.3.4, page 64, line 9; subclause 11.3.4, page 80, line 4; subclause 12.3.3.1, page 95, line 1 and subclause 13.3.3.1, page 112, line 10.

SuggestedRemedy

Change the definition of OE.LOCATION.SECURED to read ""The TOE shall be placed in a secure or monitored area which limits the opportunity for unauthorized physical access to the TOE."" in the PPs and subclauses listed above.

Proposed Response Response Status **O**

CI **PP-C** SC **7.5.2** P **20** L **13** # **12**
 Sukert, Alan Xerox

Comment Type **E** Comment Status **X**

In Table 14, I believe the auditable event for FIA_AFL1 is incorrectly defined. You want to track when the limit is reached here, not something else.

This same comment applies to the following - subclause 8.5.2, Table 28, page 36, line 3; subclause 9.5.2, Table 42, page 51, line 13; subclause 10.5.2, Table 56, page 67, line 3; subclause 11.5.2, Table 70, page 82, line 18; subclause 12.5.2, Table 86, page 97, line 18 and subclause 13.5.2, Table 102, page 116, line 1.

SuggestedRemedy

The second auditable event in the tables listed above should read something like ""Attempts to reach authenticate failure limit"".

Proposed Response Response Status **O**

CI **PP-C** SC **7.5.6** P **23** L **12** # **24**
 Sukert, Alan Xerox

Comment Type **T** Comment Status **X**

The application note says that FIA_UAU.1 is a dependency of both FIA_AFL.1 and FIA_UAU.7; it is not a dependency of FIA_UAU.7.

The same comment applies to the following: subclause 8.5.6, page 39, line 15; subclause 9.5.6, page 54, line 16; subclause 10.5.6, page 70, line 15; subclause 11.5.6, page 85, line 26; subclause 12.5.6, page 101, line 8 and subclause 13.5.6, page 120, line 8.

SuggestedRemedy

Correct this application note to read ""FIA_UAU.1 is a dependency of FIA_AFL.1"" in the indicated subclauses.

Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-C** SC **7.5.6** P **24** L **8** # **25**
 Sukert, Alan Xerox

Comment Type **T** Comment Status **X**

The PP Application Note on this line lists FIA_UAU.1, FAU_GEN.2 and FMT_SMR.1 as being dependent on FIA_UID.1. Note that FAU_UID.1 is also a dependency of FIA_UAU.7.

The same comment applies to the following: subclause 8.5.6, page 40, line 8; subclause 9.5.6, page 55, line 8; subclause 10.5.6, page 71, line 8; subclause 11.5.6, page 86, line 14; subclause 12.5.6, page 101, line 22 and subclause 13.5.6, page 120, line 22.

SuggestedRemedy

Update the Application Note in the subclauses indicated above to read ""FIA_UID.1 is a dependency of FIA_UAU.1, FIA_UAU.7, FAU_GEN.2 and FMT_SMR.1.""

Proposed Response Response Status **O**

Cl **PP-C** SC **9.5.2** P **52** L **21** # **4**
 Sukert, Alan Xerox

Comment Type **E** Comment Status **X**

The PP Application Note on this line references FAU_STG.1; it should reference FAU_SAR.2 instead. This comment also applies to subclause 13.5.2, page 117, line 14

SuggestedRemedy

Revise this PP Application Note to read ""FAU_SAR.2 is a requirement which fulfills O.AUDIT.LOGGED"" in the subclauses listed above.

Proposed Response Response Status **O**

Cl **PP-C** SC **9.5.2** P **53** L **11** # **17**
 Sukert, Alan Xerox

Comment Type **E** Comment Status **X**

The objective O.AUDIT.LOGGED is misspelled on this line (missing 'D').

SuggestedRemedy

Correct the spelling of objective O.AUDIT.LOGGED on this line.

Proposed Response Response Status **O**

Cl **PP-C** SC **9.5.2** P **53** L **11** # **5**
 Sukert, Alan Xerox

Comment Type **E** Comment Status **X**

The PP Application Note on this line references FAU_STG.1; it should reference FAU_STG.4 instead. Also the security objective listed in this note is misspelled.

SuggestedRemedy

Revise this PP Application Note to read ""FAU_STG.4 is a requirement which fulfills O.AUDIT.LOGGED"" in the PPs and subclauses noted above.

Proposed Response Response Status **O**

Cl **PP-C** SC **Annex A** P **129** L **23** # **30**
 Sukert, Alan Xerox

Comment Type **T** Comment Status **X**

The definition for Compromise in Annex A does not match the corresponding definition of Compromise in P2600 standard, Rev D33a, subclause 2.2.16.

SuggestedRemedy

Make the definition of Compromise in Annex A match the corresponding definition in P2600 standard, Rev D33a, subclause 2.2.16.

Proposed Response Response Status **O**

Cl **PP-C** SC **Annex A** P **129** L **32** # **28**
 Sukert, Alan Xerox

Comment Type **T** Comment Status **X**

The definition for Hardcopy Device in Annex A does not match the corresponding definition of Hardcopy Device in P2600 standard, Rev D33a, subclause 2.1.1.

SuggestedRemedy

Make the definition of Hardcopy Device in Annex A match the corresponding definition in P2600 standard, Rev D33a, subclause 2.1.1.

Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security comments

CI **PP-C** SC **Annex A** P **130** L **26** #

Sukert, Alan Xerox

Comment Type **T** Comment Status **X**

The definition for Operational Environment in Annex A of each PP does not match the corresponding definition of Operational Environment in P2600 standard, Rev D33a, subclause 2.2.46.

SuggestedRemedy

Make the definition of Operational Environment in Annex A match the corresponding definition in P2600 standard, Rev D33a, subclause 2.2.46.

Proposed Response Response Status **O**

CI **PP-C** SC **Annex A** P **131** L **33** #

Sukert, Alan Xerox

Comment Type **T** Comment Status **X**

The definition for User Document Data in Annex A does not match the corresponding definition of User Document Data in P2600 standard, Rev D33a, subclause 2.2.59.

SuggestedRemedy

Make the definition of User Document Data in Annex A match the corresponding definition in P2600 standard, Rev D33a, subclause 2.2.59.

Proposed Response Response Status **O**

CI **PP-C** SC **Annex A** P **131** L **35** #

Sukert, Alan Xerox

Comment Type **T** Comment Status **X**

The definition for User Function Data in Annex A does not match the corresponding definition of User Function Data in P2600 standard, Rev D33a, subclause 2.2.60.

SuggestedRemedy

Make the definition of User Function Data in Annex A match the corresponding definition in P2600 standard, Rev D33a, subclause 2.2.60.

Proposed Response Response Status **O**