

IEEE P2600 Hardcopy Device and System Security comments

Cl 00 SC 1.1 P 5 L 7 # 28
 Smithson, Brian Ricoh Americas Corpo
 Comment Type E Comment Status X
 Should we add dates to the titles for 2600.2/3/4? (i.e. "2600.2tm-2010"?)
 SuggestedRemedy
 Consider/discuss whether we should add dates. If so, add on this page and elsewhere.
 Proposed Response Response Status O

Cl 00 SC 1.1 P 5 L 7 # 26
 Smithson, Brian Ricoh Americas Corpo
 Comment Type E Comment Status X
 The titles for 2600.2/3/4 changed (.1 is the same as always). Titles are now (example of 2600.2): "IEEE Standard Protection Profile for Hardcopy Devices in IEEE Std. 2600-2008 Operational Environment B".
 SuggestedRemedy
 Change on this page and elsewhere that the full titles appear.
 Proposed Response Response Status O

Cl 00 SC 1.4 P 7 L 8 # 27
 Smithson, Brian Ricoh Americas Corpo
 Comment Type E Comment Status X
 Missing "TM" on 2600.2/3/4.
 SuggestedRemedy
 Add a trademark symbol, same as on 2600.1.
 Proposed Response Response Status O

Cl 00 SC 2.2 P 8 L 35 # 29
 Smithson, Brian Ricoh Americas Corpo
 Comment Type E Comment Status X
 I don't think "validated" is the correct word. How something is validated is mandated by the CEM. I think you mean "satisfied" (as in: you satisfy a requirement).
 SuggestedRemedy
 Change line and next line to "...does not mandate how the requirement for user identification is to be satisfied; as a result, user identification can be implemented completely within the TOE or can be..."
 Proposed Response Response Status O

Cl 00 SC 4.2.1.1 P 15 L 18 # 30
 Smithson, Brian Ricoh Americas Corpo
 Comment Type E Comment Status X
 we do apply functional requirements under certain conditions (security functional requirements, at least) by way of the packages
 SuggestedRemedy
 Maybe more clear to say "...the Common Criteria does not allow elements such as threats, policies, assumptions, or objectives, to be applied..."
 Proposed Response Response Status O

Cl 00 SC 4.2.1.1 P 15 L 33 # 36
 Smithson, Brian Ricoh Americas Corpo
 Comment Type T Comment Status X
 the common PP is not always combined with a package. env C and D have only one package (SML) and it is not always required
 SuggestedRemedy
 Safer to say "...but in practice, it will usually be combined with at least one SFR package."
 Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security comments

Cl 00 SC 5.2 P 24 L 23 # 31
Smithson, Brian Ricoh Americas Corpo

Comment Type E Comment Status X

It seems like the heading for this section is a little strange. The section is about choosing which OpEnv to certify against for a given product and its intended usage.

SuggestedRemedy

Change to something like ""5.2 Choosing the appropriate Operational Environment to certify a product""

Proposed Response Response Status O

Cl 00 SC 6.2 P 36 L 33 # 39
Smithson, Brian Ricoh Americas Corpo

Comment Type T Comment Status X

security requirements rationale is not required in OpEnv D because PP-D is a LAL PP. It can be included at the ST author's discretion (if they have also included objectives)

SuggestedRemedy

Make a note about that under list item 6.

Proposed Response Response Status O

Cl 00 SC 6.2 P 36 L 12 # 37
Smithson, Brian Ricoh Americas Corpo

Comment Type T Comment Status X

The SPD is not required for OpEnv D, because PP-D is a low assurance level PP. It can be included at the ST author's discretion.

SuggestedRemedy

Make a note under list item 3.

Proposed Response Response Status O

Cl 00 SC 6.3.1.3 P 39 L 16 # 32
Smithson, Brian Ricoh Americas Corpo

Comment Type E Comment Status X

strange page break, also on 6.6.1 page 45 line 9

SuggestedRemedy

fix it...

Proposed Response Response Status O

Cl 00 SC 6.2 P 36 L 17 # 38
Smithson, Brian Ricoh Americas Corpo

Comment Type T Comment Status X

In OpEnv D, not all of the objectives are required and a rationale table is not required, because PP-D is a low assurance level PP. The ST author can include this information at his/her discretion. The rational table can be included only if the author has also included an SPD so that objectives map to something.

SuggestedRemedy

Make a note under list item 4 that the following are not required, but may be included, in OpEnv D: security objectives for the TOE, and relation between objectives and SPD.

Proposed Response Response Status O

Cl 00 SC 6.6.2 P 50 L 40 # 33
Smithson, Brian Ricoh Americas Corpo

Comment Type E Comment Status X

Is the destination fax machine really trusted? Is it really similar to the printed document case? The receiving fax machine is outside of the TOE environment.

SuggestedRemedy

Reconsider this paragraph.

Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security comments

Cl 00 SC 6.6.9 P 55 L 11 # 34
 Smithson, Brian Ricoh Americas Corpo

Comment Type E Comment Status X

Shouldn't this advice be placed in the errata section where the problem is identified? It seems strange to put it here with a reference to errata and to have a pointer back here from the errata.

SuggestedRemedy

Move this content to 13.1 item 3.

Proposed Response Response Status O

Cl 00 SC 6.8.3 P 57 L 40 # 35
 Smithson, Brian Ricoh Americas Corpo

Comment Type E Comment Status X

Packages can refer to SAR or SFR, so maybe it is better to head this as SAR Packages and not just Packages

SuggestedRemedy

Change to something like "2. SAR Packages and EAL conformance"

Proposed Response Response Status O

Cl 00 SC 6.8.3 P 58 L 1 # 40
 Smithson, Brian Ricoh Americas Corpo

Comment Type T Comment Status X

"Low assurance level" isn't actually related to EALs, it is related to PP conformance.

SuggestedRemedy

Remove "Low assurance level" from table 8, and make a note about it under "3. PP Conformance".

Proposed Response Response Status O

Cl 00 SC TOC P 3 L 11 # 25
 Smithson, Brian Ricoh Americas Corpo

Comment Type E Comment Status X

For some reason, GUIDELINES is boldfaced in the TOC for clauses 6 and 7, maybe it got tagged boldface in the header but the boldface is invisible in the header because headers are already boldfaced (if that makes any sense at all...)

SuggestedRemedy

Good luck fixing!

Proposed Response Response Status O

Cl Globa SC 1.1 P 5 L 7 # 42
 Thrasher, Jerry Lexmark International

Comment Type E Comment Status X

Since .2 .3 and .4 have completed Sponsor Ballot we may need to add 2009 to the date for the titles....they likely will be approved this year.

SuggestedRemedy

Proposed Response Response Status O

Cl Globa SC 4.2.2.2 P 17 L 20 # 43
 Thrasher, Jerry Lexmark International

Comment Type E Comment Status X

The sentence is confusing ...suggest

SuggestedRemedy

The action of a User association all or part of that User's security attributes to an activated Subject that then acts on behalf of the User to perform an Operation is denoted by the Common Criteria as "binding:....."

Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security comments

Cl **Globa** SC **6.9.4** P **75** L **30** # **44**
 Thrasher, Jerry Lexmark International
 Comment Type **E** Comment Status **X**
 The spacing of the text box to the line of text before it is messed up....possibly a Word'ism...may have to delete the lines before the box and retype to fix.
 SuggestedRemedy
 Proposed Response Response Status **O**

Cl **Guide** SC **13** P **99** L **13** # **24**
 Farrell, Lee Canon
 Comment Type **E** Comment Status **X**
 This paragraph seems to be in a smaller font. Was that intentional?
 [I understand that the source document uses a smaller font, but does that really matter?]
 SuggestedRemedy
 Proposed Response Response Status **O**

Cl **Globa** SC **TOC** P **3** L **11** # **41**
 Thrasher, Jerry Lexmark International
 Comment Type **E** Comment Status **X**
 The word Guidelines is in bold for the heading in Clause 6
 SuggestedRemedy
 fix
 Proposed Response Response Status **O**

Cl **Guide** SC **4.2.5.1** P **22** L **40** # **3**
 Farrell, Lee Canon
 Comment Type **E** Comment Status **X**
 Change ""Items a and b) "" to ""Items a) and b) ""
 SuggestedRemedy
 Proposed Response Response Status **O**

Cl **Guide** SC **13** P **98** L **2** # **23**
 Farrell, Lee Canon
 Comment Type **E** Comment Status **X**
 Both paragraph formats should be full justification, to be consistent.
 SuggestedRemedy
 Proposed Response Response Status **O**

Cl **Guide** SC **5.3** P **26** L **4** # **4**
 Farrell, Lee Canon
 Comment Type **E** Comment Status **X**
 Change ""problem"" to ""problems""
 SuggestedRemedy
 Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security comments

Cl Guide SC 6.2 P 35 L 26 # 5
Farrell, Lee Canon

Comment Type E Comment Status X
Lines 26-31: either use ""a"" or ""a."" or even ""a)."" (least favorite) consistently throughout the document. (See pg. 36 lines 21-23, pg 39 lines 13-14 and much of Clause 6.9 [and elsewhere?])

SuggestedRemedy

Proposed Response Response Status O

Cl Guide SC 6.3.1.2 P 38 L 23 # 6
Farrell, Lee Canon

Comment Type E Comment Status X
Change ""probably because"" to ""e.g.,""

SuggestedRemedy

Proposed Response Response Status O

Cl Guide SC 6.3.1.3 P 39 L 16 # 7
Farrell, Lee Canon

Comment Type E Comment Status X
Why is there a page break after line 16?

SuggestedRemedy

Proposed Response Response Status O

Cl Guide SC 6.4 P 40 L 27 # 8
Farrell, Lee Canon

Comment Type E Comment Status X
The footnote callout for ""TSF Data"" is wrong. Footnote 32 is called out on page 39 line 16. Should it be Footnote #33 instead?

SuggestedRemedy

Proposed Response Response Status O

Cl Guide SC 6.5 P 42 L 5 # 9
Farrell, Lee Canon

Comment Type E Comment Status X
Change ""reexamine at"" to ""reexamine"".

SuggestedRemedy

Proposed Response Response Status O

Cl Guide SC 6.5.1 P 43 L 8 # 10
Farrell, Lee Canon

Comment Type E Comment Status X
Include the word ""Clause"" in the reference ""see 7 Item 5.a)"". [Previously agreed to use ""ClauseÆ"" when referencing 1st level paragraphs, but not insert ""Clause"" when referencing 2nd level paragraphs or higher.]

SuggestedRemedy

Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security comments

Cl Guide SC 6.6.1 P 45 L 9 # 11
 Farrell, Lee Canon
 Comment Type E Comment Status X
 Why is there a page break after line 9?
 SuggestedRemedy
 Proposed Response Response Status O

Cl Guide SC 6.9.7 P 77 L 33 # 15
 Farrell, Lee Canon
 Comment Type E Comment Status X
 Paragraph format should be full justification, to be consistent.
 SuggestedRemedy
 Proposed Response Response Status O

Cl Guide SC 6.6.1.1 P 48 L 28 # 12
 Farrell, Lee Canon
 Comment Type E Comment Status X
 I think the footnote callout number is incorrect.
 SuggestedRemedy
 Proposed Response Response Status O

Cl Guide SC 7.6 P 87 L 13 # 16
 Farrell, Lee Canon
 Comment Type E Comment Status X
 Paragraph format should be full justification, to be consistent.
 SuggestedRemedy
 Proposed Response Response Status O

Cl Guide SC 6.9 P 62 L 42 # 13
 Farrell, Lee Canon
 Comment Type E Comment Status X
 I think the range ""7 - 6.9.10"" is incorrect. Maybe ""6.1 - 6.9.10ö?
 SuggestedRemedy
 Proposed Response Response Status O

Cl Guide SC 8.1 P 88 L 31 # 17
 Farrell, Lee Canon
 Comment Type E Comment Status X
 Both paragraph formats should be full justification, to be consistent.
 SuggestedRemedy
 Proposed Response Response Status O

Cl Guide SC 6.9.2 P 70 L 12 # 14
 Farrell, Lee Canon
 Comment Type E Comment Status X
 [See text in footnote #50] Remove ""here"".
 SuggestedRemedy
 Proposed Response Response Status O

Cl Guide SC 8.1 P 89 L 2 # 18
 Farrell, Lee Canon
 Comment Type E Comment Status X
 Paragraph format should be full justification, to be consistent.
 SuggestedRemedy
 Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security comments

Cl Guide SC 8.1 P 89 L 35 # 19
 Farrell, Lee Canon
 Comment Type E Comment Status X
 Paragraph format should be full justification, to be consistent.
 SuggestedRemedy
 Proposed Response Response Status O

Cl Guide SC TOC P 3 L 11 # 1
 Farrell, Lee Canon
 Comment Type E Comment Status X
 Why is ""GUIDELINES"" in bold font?
 SuggestedRemedy
 Proposed Response Response Status O

Cl Guide SC 8.1 P 90 L 3 # 20
 Farrell, Lee Canon
 Comment Type E Comment Status X
 Paragraph format should be full justification, to be consistent.
 SuggestedRemedy
 Proposed Response Response Status O

Cl Guide SC TOC P 4 L 13 # 2
 Farrell, Lee Canon
 Comment Type E Comment Status X
 Why is ""GUIDELINES"" in bold font?
 SuggestedRemedy
 Proposed Response Response Status O

Cl Guide SC 8.3 P 91 L 6 # 21
 Farrell, Lee Canon
 Comment Type E Comment Status X
 Lines 6-9 and 11-28 are missing Question numbers and paragraph indentation, as in
 Clauses 8.1 and 8.2.
 SuggestedRemedy
 Proposed Response Response Status O

Cl PP Gu SC 6.6.1.1 P 47 L 27 # 49
 Sukert, Alan Xerox
 Comment Type T Comment Status X
 The sentence starting on line 27 is not correct as stated - what it should say is that if fewer
 audit events than those specified in the applicable Audit Data Requirement table are
 specified in the ST, the ST can't claim conformance to the applicable PP.
 SuggestedRemedy
 Revise this sentence to read something like ""The ST should not select the ""minimum""
 level of audit data generation and list fewer audit events than those specified in the Audit
 Data Requirement table in the applicable PP from the IEEE Std 2600 Series of Protection
 Profiles, and still claim conformance to that PP.""
 Proposed Response Response Status O

Cl Guide SC 9 P 92 L 2 # 22
 Farrell, Lee Canon
 Comment Type E Comment Status X
 All paragraph formats in this Clause should be full justification, to be consistent.
 SuggestedRemedy
 Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP Gu** SC **6.6.1.2** P **47** L **32** # **46**
 Sukert, Alan Xerox

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

The text ""for a Basic level of audit detail,"" is bolded and shouldn't be.

Note there is also an extraneous quotation mark after functionality on this line that should be removed.

SuggestedRemedy

Unbold the indicated text.

Remove the extraneous quotation mark on this line.

Proposed Response Response Status **O**

Cl **PP Gu** SC **6.7** P **55** L **14** # **45**
 Sukert, Alan Xerox

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

This is a restatement of Comment #105 from the Sep 09 Meeting:

I don't think that the AC SFP can be modified like this without violating demonstrable conformance. Remember, a vendor can provide the ability to let admins or users grant extended permissions to other users, admins can change the default permissions, and admins can even disable security entirely, but the product (as certified) must still be capable of being locked down as specified in the PP.

SuggestedRemedy

Remove lines 14-22 (including table 7).

It is OK to mention that vendors can provide features that relax the permissions, but the product must be certified in a configuration where the AC SFPs are strictly enforced.

It is also good to mention that if a product lets Administrators view/delete/whatever any document they want, then those rules can be added to the SFP. This would not violate conformance because the standard SFP rules apply only to Normal Users; Administrators are not specified one way or the other.

Smithson to talk to Helmut K. to sort out this issue.

Proposed Response Response Status **O**

Cl **PP Gu** SC **6.9** P **62** L **6** # **48**
 Sukert, Alan Xerox

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

The references to '7 on both line 6 and line 10 on page 62 should be to ""Clause 7'.

SuggestedRemedy

Change the indicated reference on lines 6 and 10 to 'Clause 7'.

Proposed Response Response Status **O**

Cl **PP Gu** SC **6.9.10** P **81** L **3** # **50**
 Sukert, Alan Xerox

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

In updating the indicated text to address Comment #101 from the Sep meeting, the author feels that appropriate examples of how flow control SFRs can be used when forwarding of unmediated transmission is never allowed or is allowed would be appropriate here.

SuggestedRemedy

Add after line 5 appropriate examples of how flow control SFRs can be used when forwarding of unmediated transmission is never allowed or is allowed.

Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security comments

CI **PP Gu** SC **6.9.2** P **64** L # **47**
Sukert, Alan Xerox

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

In updating the additional guidance for PP Application Note 10 to resolve previous comments, I noticed that the PP Application Note as stated in IEEE Std 2600.1, Clause 10.1, page 19 may not agree with the direction in CC Part 2, Appendix C.3, page 185.

CC Part 2, Appendix C.3 indicates that auditable events are hierarchical, meaning for example that if the Basic audit level is chosen all auditable events for both the Basic and Minimal levels must be collected. PP Application Note 10 states that in the event of a conflict between the CC IEEE Std 2600.1 Table 15, the ""greater of those requirements"" must be specified in the ST. Unless the ""greater of those requirements"" includes the lower audit level requirement the requirements of CC Part 2 Appendix C.3 would not be met.

SuggestedRemedy

Review the guidance for PP Application Note 10 as a group to make sure it doesn't negate what is in CC Part 2, Appendix C.3.

Review the text of PP Application Note 10 to make sure it also doesn't negate what is in CC Part 2, Appendix C.3. Include the proper revision to this PP Application Note in PP Guide Clause 13 (Errata) if necessary.

Proposed Response Response Status **O**