

IEEE P2600 Hardcopy Device and System Security comments

Cl Annex SC Annex G P 163 L 7 # 23
 Sukert, Alan Xerox
Comment Type T Comment Status X
 Since Common Criteria Version 3.1 has been officially issued, I think the current references B134 - B137 should be replaced by the corresponding references to the CCv3.1 documents.
SuggestedRemedy
 See above
Proposed Response Response Status O

Cl Main SC 1.3.8 P 3 L 11 # 28
 Sukert, Alan Xerox
Comment Type E Comment Status X
 For consistency with the text in Clause 9, subclause 9.1 (page 112, lines 5-7) I would suggest changing the sentence on this line to read ""Best practices are provided for manufacturers, IT administrators, and users of HCDs."
SuggestedRemedy
 See above
Proposed Response Response Status O

Cl Main SC 1.2 & 1.3.9 P 2-3 L # 40
 Sukert, Alan Xerox
Comment Type G Comment Status X
 I think we discussed this at the Sep meeting in Waterloo CN. I noted that ""Protection Profiles"" is capitalized in subclause 1.2, line 24 but isn't capitalized in subclause 1.3.9, lines 13 & 16
SuggestedRemedy
 Be consistent in capitalization of the words ""Protection Profile""
Proposed Response Response Status O

Cl Main SC 3 P 8 L 35 # 44
 Sukert, Alan Xerox
Comment Type T Comment Status X
 Based on the discussions we had at the Sep meeting plus some internal discussions I've had with the product Systems group at Xerox, I think it is important we add a definition of ""Production Systems"" to Clause 3 if we plan on including Production Systems in the standard. That way everyone will have a common and consistent understanding of what we are referring to when we speak about ""Production Systems"". I am enclosing the definition we came up with as a starting point for the discussion
SuggestedRemedy
 Suggested definition:
 production systems. A product or a set of products/modules that is used by an owner/operator to produce printed work that has been commissioned by others.
Proposed Response Response Status O

Cl Main SC 1.3.4 P 2 L 35 # 29
 Sukert, Alan Xerox
Comment Type E Comment Status X
 Since Clause 5 is titled ""Operational Environments"", this subclause title should be consistent with the title in Clause 5 as well as the text on lines 36-37
SuggestedRemedy
 Retitle subclause 1.3.4 as ""Operational environments""
Proposed Response Response Status O

Cl Main SC 4.1 P 15 L 15 # 30
 Sukert, Alan Xerox
Comment Type E Comment Status X
 This sentence uses the abbreviation 'MFP' to stand for multifunction device. Per the acronym definitions in Clause 3, 'MFD' is the acronym for multifunction device.
SuggestedRemedy
 Use the correct acronym for multifunction device - MFD.
Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security comments

Cl Main SC 4.2.1.1 P 16 L 6 # 31
 Sukert, Alan Xerox
Comment Type E **Comment Status** X
 The last sentence in this subclause has a small grammatical error - it states ""Examples of Original Document Handler components..."" ,components is a plural noun but ""an"" is the singular.
SuggestedRemedy
 Change sentence to read ""Examples of Original Document Handler components...""
Proposed Response **Response Status** O

Cl Main SC 4.3.2 P 19 L 43 # 34
 Sukert, Alan Xerox
Comment Type E **Comment Status** X
 The last sentence in this subclause encrypted in storage."" should be modified as follows: ""...an HCD can also be a target for accessing documents that would otherwise be encrypted in storage and transit."" (added the that to make sentence grammatically correct)
SuggestedRemedy
 Make sentence grammatically correct
Proposed Response **Response Status** O

Cl Main SC 4.2.2.6 P 17 L 31 # 32
 Sukert, Alan Xerox
Comment Type E **Comment Status** X
 The sentence on this line should read ""NOTE - Figure 1 shows the System Processor or Memory system..."" for consistency with Figure 1 and the rest of this subclause.
SuggestedRemedy
 See above
Proposed Response **Response Status** O

Cl Main SC 5.2.1 P 22 L 36 # 35
 Sukert, Alan Xerox
Comment Type E **Comment Status** X
 This is definitely a nit - there is a double period at the end of the last sentence in subclause 5.2.1.
SuggestedRemedy
 Remove the double-period.
Proposed Response **Response Status** O

Cl Main SC 4.2.3.3 P 18 L 12 # 33
 Sukert, Alan Xerox
Comment Type E **Comment Status** X
 I noted that the Copy Controller Interface discussed in this subclaus eis not shown in Figure 1 on page 16.
SuggestedRemedy
 Include the Copy Controller Interface in Figure 1.
Proposed Response **Response Status** O

Cl Main SC 5.2.3 P 25 L 22 # 45
 Sukert, Alan Xerox
Comment Type T **Comment Status** X
 The discussion of the DA's office has a reference to ""high value assets"". I think this may have been a carry-over from the original definition of Operational Environment A. Should rewrite the sentence to remove this reference - see below for suggested wording
SuggestedRemedy
 Revise sentence to read ""...since they meet the definition of assets in need of strong protection.""
Proposed Response **Response Status** O

IEEE P2600 Hardcopy Device and System Security comments

CI Main SC 5.3.1 P 26 L 9 # 46
Sukert, Alan Xerox

Comment Type T Comment Status X

The reference to Figure 1 in this line indicates that Figure 3 is an example of a "network architecture typical of Operational Environment B...". Yet Figure 3 on page 27 is titled "Centrally-Managed Operational Environment B Example". Unless a centrally-managed configuration is always typical of these types of environments, the title of Figure 3 should be consistent with the description of the figure in 5.3.1.

SuggestedRemedy

Make the title of Figure 4 on page 27 consistent with the description of the figure in 5.3.1.

Proposed Response Response Status O

CI Main SC 5.3.1 P 28 L 12 # 36
Sukert, Alan Xerox

Comment Type E Comment Status X

The last sentence in this subclause explains Figure 4 on the same page. It references Operational Environment D in that explanation for the part of Figure 4 that shows a Operational Environment A home office. There are two consistency issues:

1. You are discussing Operational Environment D here before it has been defined or discussed in Clause 4, which generally is not good practice.
2. Figure 4 doesn't show the Operational Environment D part of the home office configuration, so the reader probably wouldn't understand the description in the text.

SuggestedRemedy

Two possible approaches:

1. Delete the discussion entirely of Operational Environment D here and remove the home office part of Figure 4. Then after discussing Operational Environment D in 5.5 you can show Figure 4 modified to include the home office, which would then be understood in the proper context by the reader.
2. If you want to keep the discussion of Operational Environment D in 5.3.1, include a reference to 5.5 in the text on line 12 and make sure you add the appropriate Operational Environment D portion in Figure 4.

Proposed Response Response Status O

CI Main SC 5.5.1 P 32 L 27 # 37
Sukert, Alan Xerox

Comment Type E Comment Status X

I think by our convention that the reference to "802.11" on this line should be to "IEEE Std 802.11".

SuggestedRemedy

See above

Proposed Response Response Status O

CI Main SC 7.3.2.1 P 43 L 4 # 1
Sukert, Alan Xerox

Comment Type T Comment Status X

Table 7 references the acronyms UDP and IMCP. Neither one is included in the Acronyms and abbreviations table in subclause 3.2.

SuggestedRemedy

Add 'UDP' and 'ICMP' to 3.2.

Proposed Response Response Status O

CI Main SC 7.3.2.3 P 51 L 4 # 48
Sukert, Alan Xerox

Comment Type T Comment Status X

In Table 25 the short description of T.UD.ACC.NORMAL is "Accessing another's User Data using normal HCD interfaces", yet the full description only discusses User Document Data which per subclause 6.2.1 is a subset of User Data.

Note that same comment applies to Table 26, page 52, line 2

SuggestedRemedy

Two possible approaches:

1. Change the short description to read "Accessing another's User Document Data using normal HCD interfaces" or
2. Change the full description to something like "An attacker can access another's users data from..."

Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security comments

Cl Main SC 8.3.2.3 P 53 L 2 # 41
 Sukert, Alan Xerox
Comment Type G **Comment Status** X
 There are several instances in Clause 8 where the phrase ""user document data"" should be capitalized to be consistent with the convention we adopted previously.
SuggestedRemedy
 Capitalize the phrase 'User Document Data' wherever it occurs.
Proposed Response **Response Status** O

Cl Main SC 9.5.2.2 P 127 L 13 # 42
 Sukert, Alan Xerox
Comment Type G **Comment Status** X
 Subclause 9.5.2.2 in this line uses the phrase ""out of box""; subclause 9.5.2.3 on line 17 demotes this phrase as ""out-of-box"".
SuggestedRemedy
 Be consistent in how you denote this phrase
Proposed Response **Response Status** O

Cl Main SC 9.4.2 P 125 L 38 # 38
 Sukert, Alan Xerox
Comment Type E **Comment Status** X
 The abbreviation 'TLS' used on his line is not included in the list of acronyms and abbreviations in subclause 3.2.
SuggestedRemedy
 Add definition of 'TLS' in subclause 3.2
Proposed Response **Response Status** O

Cl Main SC 9.6.2.2.4 P 131 L 22 # 26
 Sukert, Alan Xerox
Comment Type E **Comment Status** X
 SNMP is used in this line but not defined in subclause 3.2.
SuggestedRemedy
 Define SNMP in subclause 3.2
Proposed Response **Response Status** O

Cl Main SC 9.4.2 P 126 L 6 # 39
 Sukert, Alan Xerox
Comment Type E **Comment Status** X
 The abbreviation 'S/MIME' used on his line is not included in the list of acronyms and abbreviations in subclause 3.2.
SuggestedRemedy
 Add the definition of 'S/MIME' in subclause 3.2
Proposed Response **Response Status** O

Cl Main SC 9.6.2.2.5 P 133 L 45 # 27
 Sukert, Alan Xerox
Comment Type T **Comment Status** X
 The acronym SC (meaning Smart Card) is used in conjunction with PC/SC specifications, but SC is not defined in subclause 3.2.
SuggestedRemedy
 Define SC in subclause 3.2
Proposed Response **Response Status** O

IEEE P2600 Hardcopy Device and System Security comments

Cl **Main** SC **9.6.3.1** P **136** L **4** # **43**
Sukert, Alan Xerox

Comment Type **G** Comment Status **X**

There are several acronyms used in this subclause that are not defined in sunclause 3.2 - HTTPS, CBC, APOP, ESMTP, LDAPS, RADIUS, TACAS, KDC, 3DES, DSS, DSA, SSH, IPv6.

Also AES on page 137, line 40 is not defined in subclause 3.2 as well as VISTR and HMG on page 138, Table 59

SuggestedRemedy

make sure all these acronyms are defined in subclause 3.2.

Proposed Response Response Status **O**