

IEEE P2600 Hardcopy Device and System Security Comments

Cl Main SC 3.1.20 P 6 L 8 # 35
Sukert, Alan Xerox

Comment Type G Comment Status X

The document is still inconsistent in capitalizing the term 'E-mail'. For example, on page 6, line 8 it is capitalized while on page 26, line 11 it is not capitalized. I believe the convention we agreed on was that it would not be capitalized, but either way we should be consistent here.

SuggestedRemedy

Make sure E-mail is consistently capitalized or not capitalized within the document.

Proposed Response Response Status O

Cl Main SC 4.2.2.5 P 18 L 26 # 10
Sukert, Alan Xerox

Comment Type E Comment Status X

For consistency with the terminology defined in subclause 3.1.53, the term ""multifunction product"" should instead be ""multifunction device"".

SuggestedRemedy

See above suggestion

Proposed Response Response Status O

Cl Main SC 4.3.1 P 19 L 26 # 2
Thrasher, Jerry Lexmark

Comment Type T Comment Status X

There is a terminology collision with the ""Security Objectives"" discussed in 4.3.1 and those discussed in the Compliance Clause (Clause 10). I don't think the term Security Objective accurately describes what's in Clause 10 anyway.

SuggestedRemedy

Change the Clause 10 Security Objective terminology to something like Security Features or Security Capabilities.

Proposed Response Response Status O

Cl Main SC 4.3.1 P 19 L 31 # 38
Sukert, Alan Xerox

Comment Type T Comment Status X

The list of assets included in subclause 4.3.1 is inconsistent with the list of HCD assets in Clause 6. I'm not concerned about exact wording but whether the general categories of assets described in both places are consistent. See the comparison below:

Subclause 4.3.1	Clause 6
User documents	User Document data (probably the same)
Data associated with processing jobs	User Function Data (more than in 4.3.1)
Data associated with configuring & securing HCD	Management Data (data for configuring & accessing HCD)

SuggestedRemedy

Make the list of assets included in subclause 4.3.1 consistent with the list of HCD assets in Clause 6

Proposed Response Response Status O

Cl Main SC 4.3.2 P 20 L 24 # 11
Sukert, Alan Xerox

Comment Type E Comment Status X

For purposes of readability, suggest this line be changed from ""...storage, they are necessarily not encrypted..."" to ""...storage, they are not necessarily encrypted...""

SuggestedRemedy

See above suggestion

Proposed Response Response Status O

Cl Main SC 4.3.2 P 20 L 25 # 33
Sukert, Alan Xerox

Comment Type G Comment Status X

Standard practice on the use of acronyms in a document is that an acronym should always be defined the first time it is used in the document. The P2600 standard is inconsistent in doing this. For example, the acronym 'PSTN' which is first used in the main text outside of Clause 3 in page 20, line 25 is never defined in the main text outside of Clause 3. Contrast that with the acronym HCD that is defined the second time it is used in the text (page 16, line 3) and with the acronym MFD that is defined the first time it is used on page 16, line 15.

SuggestedRemedy

Be consistent on if and when acronyms are defined outside of Clause 3.

Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security Comments

CI Main SC 4.3.2 P 20 L 36 # 12
 Sukert, Alan Xerox
 Comment Type E Comment Status X
 The end of this sentence should be corrected from "...since these assets are consumable, they must be accessible to make it easy to replenishing them." to read "...since these assets are consumable, they must be accessible to make it easy to replenish them." to be grammatically correct.
 SuggestedRemedy
 See the above suggestion
 Proposed Response Response Status O

CI Main SC 4.4.3.2 P 21 L 45 # 13
 Sukert, Alan Xerox
 Comment Type E Comment Status X
 The word 'Threat' is incorrectly spelled as 'Theat' at the beginning of this line
 SuggestedRemedy
 Correct the spelling of 'threat'
 Proposed Response Response Status O

CI Main SC 5.1 P 23 L 13 # 34
 Sukert, Alan Xerox
 Comment Type G Comment Status X
 The term 'standard' when referring to the P2600 standard itself in the text is inconsistently capitalized. For example, in subclause 5.1, page 23, line 13 the word standard is capitalized, while in the same subclause, page 23, line 21 it is not capitalized.
 SuggestedRemedy
 be consistent throughout the main body as to whether 'standard' is or is not capitalized when referring to the P2600 standard itself.
 Proposed Response Response Status O

CI Main SC 5.1 P 23 L 19 # 14
 Sukert, Alan Xerox
 Comment Type E Comment Status X
 To be grammatically correct, this line should be revised to read "...closely matches the requirements of a particular manufacturer's target customers,..."
 SuggestedRemedy
 Update this line as indicated above
 Proposed Response Response Status O

CI Main SC 5.2.3 P 26 L 26 # 15
 Sukert, Alan Xerox
 Comment Type E Comment Status X
 The specific example being described here is for a Social Security Office, but the first sentence of this section here describes general Federal offices and doesn't even mention Social Security. If this sentence is designed to introduce the Social Security Office example it should reference the Social Security Office somewhere in that sentence.
 SuggestedRemedy
 Revise the sentence to read "Similar to the District Attorney's Office above, many Federal government offices and agencies like the Social Security Office must be open with easy access to all people."
 Proposed Response Response Status O

CI Main SC 5.3.1 P 29 L 6 # 16
 Sukert, Alan Xerox
 Comment Type E Comment Status X
 The term "high value assets" is used in this sentence to describe the Operational Environment A islands within an Operational Environment B example. I don't know if this phrase is a carry-over from the original Operational Environment A definition or if it was intended to be used here. Might want to think about using a different term here because we removed the definition of "high value asset" from Clause 3.
 SuggestedRemedy
 See suggestion above.
 Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security Comments

Cl Main SC 5.4.1 P 31 L 38 # 17
 Sukert, Alan Xerox

Comment Type E Comment Status X

I believe that grammatically this line should read "...accountability in the way one would in Operational Environments A or B." - no 'an' before Operational and adding 's' to Environment.

SuggestedRemedy

See suggestion above.

Proposed Response Response Status O

Cl Main SC 5.5.3 P 35 L 36 # 18
 Sukert, Alan Xerox

Comment Type E Comment Status X

This sentence should read "These offices are generally in small to medium office buildings with no substantial..." to be grammatically correct and to agree with the wording in the previous example on line 30.

SuggestedRemedy

See suggestion above

Proposed Response Response Status O

Cl Main SC 6.2.5.1 P 38 L 6 # 39
 Sukert, Alan Xerox

Comment Type T Comment Status X

The discussion of firmware in Clause 6 doesn't agree with the definition of the term "firmware" in 3.1.39. My concern is twofold - (1) the definition of firmware in 3.1.39 indicates that firmware is always embedded in the HCD, while in 6.2.5.1 it states that firmware is "often embedded" in the device (i.e., the HCD) and (2) 6.2.5.1 defines firmware as software while 3.1.39 defines firmware as computer instructions and data; we don't define the term software in Clause 3, but a search of definitions for software all commonly define software in terms of just instructions only.

I also noted a couple of grammatical errors in this subclause.

SuggestedRemedy

Revise 6.2.5.1 to read "Firmware is persistent instructions and data in the HCD that provides basic functions of the HCD, is developed by the manufacturer, is embedded in the device and is infrequently updated."

Proposed Response Response Status O

Cl Main SC 6.2.5.2 P 38 L 9 # 40
 Sukert, Alan Xerox

Comment Type T Comment Status X

The discussion of applet in 6.2.5.2 is inconsistent with the definition of applet in 3.1.6. My main concern is that in 3.1.6 an applet is defined as a program that is designed to be executed from another application while in 6.2.5.2 an applet is described as "any HCD application software". The definition in 3.1.6 is more restrictive than the description in 6.2.5.2.

Also, the term "Applet" is misspelled in the beginning of this line.

SuggestedRemedy

Revise 6.2.5.2 to read "Applets are HCD application software designed to be executed from another application that provide..."

Proposed Response Response Status O

Cl Main SC 7.2 P 41 L 26 # 36
 Sukert, Alan Xerox

Comment Type G Comment Status X

In Table 3 and elsewhere in Clause 7, the phrase "denial of service" is written as 'denial-of-service' while it is written as 'denial of service' in the rest of the document.

SuggestedRemedy

Make the phrase "denial of service" consistent in Clause 7 with how that phrase is written in the rest of the main body.

Proposed Response Response Status O

Cl Main SC 7.3.2.4 P 58 L 3 # 19
 Sukert, Alan Xerox

Comment Type E Comment Status X

In Table 40 in the full description for T.TSF.CRED.GUESS, in the last line "...obtain the data through local..." should be "...obtain the data through local..." (space missing after 'data').

SuggestedRemedy

Fix the error as indicated above

Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security Comments

Cl Main SC All P 69 L 1 # 3
Thrasher, Jerry Lexmark

Comment Type T Comment Status X

Clause 8 is titled Threat Mitigation Techniques, however in the individual threat mitigation discussions, each threat has ""Recommended Mitigation Techniques for HCD Manufacturers and IT Professionals. There is also a recommendation (The following techniques should.....)for each of the listed mitigation technique. Given the fact there is now a Compliance clause we should remove the recommendation language from Clause 8 and simply provide this clause as a list of possible mitigation techniques.

SuggestedRemedy

Change the 4th level headings from ""Recommended Mitigation Techniques for..."" to ""Mitigation Techniques for..."" and change each instance of ""The following techniques should be utilized by....."" to ""The following techniques may be utilized by.....:"

Proposed Response Response Status O

Cl Main SC 8.1 P 69 L 15 # 20
Sukert, Alan Xerox

Comment Type E Comment Status X

In this line, you probably should say ""For example, a network in a typical SOHO-like environment..."" rather than ""For example, a network in a typical SOHO environment..."" to be consistent with how this is phrased in line 19 and to be consistent with how it is phrased in subclause 5.2.1, page 24, line 8.

SuggestedRemedy

Make the phraseology consistent

Proposed Response Response Status O

Cl Main SC 8.1.2.2 P 70 L 21 # 21
Sukert, Alan Xerox

Comment Type E Comment Status X

Should probably use the phrase ""...to be an HCD but a web server or other critical..."" to be consistent with the phraseology used in subclause 8.1.1.2, page 69, line 28.

SuggestedRemedy

See the solution above

Proposed Response Response Status O

Cl Main SC 8.1.2.4 P 71 L 3 # 22
Sukert, Alan Xerox

Comment Type E Comment Status X

To be correct grammatically, this sentence should read ""...and effective anti-virus software is installed and operational"" (the is was missing).

SuggestedRemedy

See the suggestion above

Proposed Response Response Status O

Cl Main SC 8.1.4.2 P 71 L 39 # 23
Sukert, Alan Xerox

Comment Type E Comment Status X

To be correct grammatically, this sentence should read ""...that result in the failure of a device's hardware or..."" instead of ""...that result in the failure of devices hardware or...""

SuggestedRemedy

See suggestion above

Proposed Response Response Status O

Cl Main SC 8.1.12.1 P 77 L 24 # 24
Sukert, Alan Xerox

Comment Type E Comment Status X

'Providing' is misspelled as 'Privinging'.

SuggestedRemedy

Correct the spelling error.

Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security Comments

Cl Main SC 8.2.2.3 P 79 L 38 # 37
 Sukert, Alan Xerox

Comment Type G Comment Status X

To be consistent with how the term is defined in subclause 3.1.82, "white-list" should be "white list" in Clause 8.

Note that a similar comment applies to use "black list" instead of "black-list" - see subclause 8.6.1.3, page 104, line 27 for example.

SuggestedRemedy

See above suggestion

Proposed Response Response Status O

Cl Main SC 8.2.2.4 P 80 L 5 # 25
 Sukert, Alan Xerox

Comment Type E Comment Status X

There is a missing space between 'interface' and the 'parenthesis' - i.e., should read "...network interface (e.g., Wi-Fi..."

SuggestedRemedy

Add the missing space.

Proposed Response Response Status O

Cl Main SC 8.2.2.4 P 80 L 12 # 26
 Sukert, Alan Xerox

Comment Type E Comment Status X

Strictly for consistency with the grammatical structure of the other 6 techniques listed in this subclause, I would suggest revising technique e) to read --

e) Performing regular auditing of the print data collected by the print tracking or auditing system against the device's internal meters to ensure...

Note: This comment would also apply to subclause 8.2.4.4, page 82, line 2

SuggestedRemedy

See above suggestion

Proposed Response Response Status O

Cl Main SC 8.3.2.3 P 83 L 26 # 27
 Sukert, Alan Xerox

Comment Type E Comment Status X

The reference to 100base-FX Ethernet here does not include the reference to the associated IEEE Standard (IEEE Std. 802.3-2005, clause 26). However, the corresponding reference to 100base-FX Ethernet in subclause 8.4.2.3, page 95, line 25 does include the reference to the IEEE Standard. The two references to 100base-FX Ethernet should be consistent in whether or not the associated IEEE Standard is referenced.

SuggestedRemedy

Make the two references to 100base-FX Ethernet consistent in whether or not the associated IEEE Standard is referenced

Proposed Response Response Status O

Cl Main SC 8.3.3.2 P 84 L 2 # 28
 Sukert, Alan Xerox

Comment Type E Comment Status X

This first sentence just does not read correctly and I'm not sure what was meant to be said here - I think a verb or something is missing.

SuggestedRemedy

Rewrite this sentence to be clear.

Proposed Response Response Status O

Cl Main SC 8.3.5.2 P 85 L 17 # 29
 Sukert, Alan Xerox

Comment Type E Comment Status X

Per the convention we set up at an earlier meeting, users' document data should be capitalized.

SuggestedRemedy

I think the sentence should read "...able to access a user's User Document Data or other..."

Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security Comments

Cl Main SC 8.3.6.3 P 86 L 18 # 41
 Sukert, Alan Xerox

Comment Type T Comment Status X

Techniques b) & c) both discuss holding document data on a hard disk. The issue is that not all MFDs have hard disks (some MFDs have only volatile memory); yet the T.UD.PHY.OUTPUT threat would apply to MFDs that don't have hard disks just as much as it would apply to MFDs that do have a hard disk.

SuggestedRemedy

Replace the term ""hard disk"" in techniques b) & c) with the term ""memory"" or something similar so it would apply to all HCDs whether or not they have a hard disk drive.

Proposed Response Response Status O

Cl Main SC 8.3.7.2 P 87 L 5 # 30
 Sukert, Alan Xerox

Comment Type E Comment Status X

For consistency with terminology used elsewhere in the main body, I would suggest that the term ""multifunction unit"" be replaced by ""multifunction device"".

SuggestedRemedy

See above suggestion

Proposed Response Response Status O

Cl Main SC 8.3.11.1 P 90 L 34 # 31
 Sukert, Alan Xerox

Comment Type E Comment Status X

There is a missing space -- ""...can be expensive..."" should be ""can be expensive..."".

SuggestedRemedy

See above suggestion

Proposed Response Response Status O

Cl Main SC 8.3.11.3 P 91 L 27 # 32
 Sukert, Alan Xerox

Comment Type E Comment Status X

Since we do define the terms 'volatile memory' and non-volatile memory' in Clause 3, I would suggest that this technique use those terms rather than 'persistent' and 'non-persistent' storage

SuggestedRemedy

Revise technique k) to read ""...does not include on-volatile storage, or utilizing volatile storage media, such as ...""

Proposed Response Response Status O

Cl Main SC 8.4.6.2 P 98 L 26 # 42
 Sukert, Alan Xerox

Comment Type T Comment Status X

Since clause 8 is guidance and not requirements, the 'shall' here should be replaced by 'should'.

SuggestedRemedy

Revise to read ""The HCD should require proper authentication...""

Proposed Response Response Status O

Cl Main SC 8.4.11.2 P 101 L 38 # 43
 Sukert, Alan Xerox

Comment Type T Comment Status X

This sentence uses the terms 'atomicity' and 'synchronization'. 'Atomicity' is defined in Clause 3 but 'synchronization' is not defined in Clause 3 - I think it should be (I checked Google and there are 26 separate definitions of 'synchronization'; I'm not sure which one we are using here).

SuggestedRemedy

Include a definition for 'synchronization' or 'synchronize' in Clause 3. A suggested definition from

Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security Comments

Cl Main SC 8.5.2 P 103 L 23 # 44
Sukert, Alan Xerox

Comment Type T Comment Status X

The definition of T.TSF.SW.UPDATE in subclause 8.5.2.1, line 25 indicates this threat addresses both firmware and software updates. However, the remainder of the discussion of this threat in subclauses 8.5.2.2, 8.5.2.3 & 8.5.2.4 mentions firmware only and doesn't address software at all.

SuggestedRemedy

Either change the definition of this threat to cover firmware only or add discussion of software updates to subclauses 8.5.2.1, 8.5.2.2, 8.5.2.3 & 8.5.2.4.

Proposed Response Response Status O

Cl Main SC 9.6.2.2.5 P 126 L 29 # 4
Thrasher, Jerry Lexmark

Comment Type T Comment Status X

This introductory paragraph has a couple of problems. The first sentence mentions magnetic stripe technology and its drawbacks but magnetic stripe technology is not mentioned anywhere else in the authentication sections of Clause 9. The paragraph also states that smartcards allow security checks directly between the card and the device (HCD) without involving an authentication server, and this somehow differentiates it from the mag-stripe card. The reason given in the paragraph is neither true or the best way to implement authentication on an HCD. Managing identity at each and every HCD is not the preferred mechanism for implementing smartcards in environments where smartcards are used.

SuggestedRemedy

Remove the paragraph or reword it to discuss the embedded processor allowing for both remote challenge response protocol for authentication verification at a central server or locally at the HCD.

Proposed Response Response Status O

Cl Main SC 9.6.2.2.5 P 129 L 11 # 5
Thrasher, Jerry Lexmark

Comment Type T Comment Status X

This sentence is already obsolete, the move has already happened in environments where smartcard technology is prevalent. The smartcard section in general needs to be rewritten.

SuggestedRemedy

Remove the obsolete sentence and rewrite section 9.6.2.2.5.

Proposed Response Response Status O

Cl Main SC 9.6.2.2.6 P 129 L 39 # 6
Thrasher, Jerry Lexmark

Comment Type T Comment Status X

This paragraph doesn't belong, as written, in this standard.

SuggestedRemedy

Rewrite paragraph.

Proposed Response Response Status O

Cl Main SC 10.1.1.2 P 137 L 22 # 58
Sukert, Alan Xerox

Comment Type E Comment Status X

It is not clear why ""applet"" is placed in quotes here (and also in 10.1.2.2, 10.1.3.2 & 10.1.4.2) when it is not placed in quotes in the rest of the main body.

SuggestedRemedy

Remove the quotes around applets in 10.1.1.2, 10.1.2.2, 10.1.3.2 & 10.1.4.2

Proposed Response Response Status O

Cl Main SC 10.1.1.2 P 137 L 26 # 1
Thrasher, Jerry Lexmark

Comment Type E Comment Status X

This technique was copied incorrectly from 8.2.4.

SuggestedRemedy

Correct the sentence to match that of 10.1.2.2

Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security Comments

Cl Main SC 10.1.1.6 P 138 L 14 # 7
 Thrasher, Jerry Lexmark

Comment Type T Comment Status X

Don't think we should require the monitoring of accounting events, but recommended it from a compliance clause perspective.

SuggestedRemedy

Change the sentence to shall ...security-related events and should...accounting events.

Proposed Response Response Status O

Cl Main SC 10.1.1.6 P 138 L 16 # 53
 Sukert, Alan Xerox

Comment Type E Comment Status X

There is a grammatical error in this line (a 'the' is missing) that should be corrected - see suggestion below.

This comment also applies to subclauses 10.1.2.6 and 10.1.3.6

SuggestedRemedy

Revise line to read ""The HCD shall monitor and record accounting events and security-related events, and shall have the capability...""

Proposed Response Response Status O

Cl Main SC 10.1.1.8 P 138 L 34 # 8
 Thrasher, Jerry Lexmark

Comment Type T Comment Status X

This mitigation doesn't have anything to do with the Assurance of genuine HCD. This is also a problem in 10.1.2.8.

SuggestedRemedy

Should be ""Ensuring that only administrators have the ability to install or uninstall applets"" and possibly add firmware and software to that list in the mitigation technique.

Proposed Response Response Status O

Cl Main SC 10.1.1.9 P 138 L 38 # 54
 Sukert, Alan Xerox

Comment Type E Comment Status X

This line doesn't read correctly and should be revised for clarify - see suggestion below.

This comment also applies to subclause 10.1.2.9.

SuggestedRemedy

Revise this line to read something like ""The HCD shall restrict the use of the fax modem to transmission or reception of fax communications so the fax modem cannot be used to bridge...""

Proposed Response Response Status O

Cl Main SC 10.1.2.1 P 139 L 5 # 9
 Thrasher, Jerry Lexmark

Comment Type T Comment Status X

Don't think we should require user identification to use the HCD. This seems to require that

SuggestedRemedy

?

Proposed Response Response Status O

Cl Main SC 10.2.1.1 P 143 L 26 # 57
 Sukert, Alan Xerox

Comment Type T Comment Status X

In the Protection Profile for Operational Environment A (as well as the Protection Profiles for the other three Operational Environments) there is an assumption A.ADMIN - Administrator trust and competence that includes the assumption that system admins are trustworthy and will not use their position for malicious purposes. Given that especially in Operational Environments A and B attacks from insiders are more likely than ones from external sources this specific assumption should be included in any security objectives for IT professionals at least in Operational Environments A & B and possibly for Operational Environment C. The best place to add this additional assumption is in 10.2.x.1

SuggestedRemedy

Revise 10.2.1.1 and 10.2.2.1 to read ""...in order to make effective use of the HCD security functions for non-malicious purposes."" Consider whether 10.2.3.1 should be similarly revised.

Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security Comments

Cl **Main** SC **10.2.1.1** P **143** L **26** # **55**
Sukert, Alan Xerox

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

This subclause uses the terms 'auditor' and 'normal user', neither of which are defined in Clause 3.

SuggestedRemedy

Either use terms in this subclause that are defined in Clause 3 or provide definitions in Clause 3 for 'auditor' and 'normal user'. If the later option is decided, I would suggest using the definitions for auditor (A User who reviews and maintains the audit trail recorded by the TOE) and normal user (A User who accesses the HCD for normal use (e.g., copy, print, fax and scan) using the Operator Panel or Network or Local Interfaces.) that are in the current Protection Profiles.

Proposed Response Response Status

Cl **Main** SC **10.2.1.4** P **144** L **11** # **56**
Sukert, Alan Xerox

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

There is a minor grammatical error on this line that should be corrected - an extra 'the' is included.

SuggestedRemedy

Revise this line to read ""...are not compromised or replaced with malicious ones.""

Proposed Response Response Status