

IEEE P2600 Hardcopy Device and System Security comments

Cl **Globa** SC P L # 82
 Thrasher, Jerry Lexmark International I

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

h)Guarantees and legal reviews

Please review P2600 for any explicit or implicit guarantees made within the document, especially those that are safety-related. Avoid making guarantees if there is a possibility of unforeseen situations or circumstances altering an outcome. For example, words such as ""ensure,"" ""guarantee,"" etc., should be modified, if they are inaccurate. Substitutions might include ""maximize"" or ""minimize,"" e.g. ""to ensure safety"" might be changed to ""to maximize safety.""

SuggestedRemedy

Proposed Response Response Status **O**

Cl **Globa** SC P L # 81
 Thrasher, Jerry Lexmark International I

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

g)Lists

Some of the lists in the draft contain only one item.

Please consider organizing info so that each list contains at least two items.

SuggestedRemedy

Proposed Response Response Status **O**

Cl **Globa** SC P L # 80
 Thrasher, Jerry Lexmark International I

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

f) Reference to commercial equipment/products

""References to commercial equipment or products in a standard shall be generic and shall not include trademarks or other proprietary designations. Where a sole source exists for essential equipment or materials, it is permissible to supply the name of the trademark owner in a footnote. (See Clause 7 of the 2007 Style Manual)

?

SuggestedRemedy

Please consider any references made in the draft to commercial equipment/products, including Linux, Unix, etc. If it is required that these be named, please add following footnote:

This information is given for the convenience of users of this standard and does not constitute an endorsement by the IEEE of these products. Equivalent products may be used if they can be shown to lead to the same results.

Proposed Response Response Status **O**

Cl **Globa** SC P L # 79
 Thrasher, Jerry Lexmark International I

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

e) References to Web sites in normative body of the text

It is noted that there are many non-IEEE Web sites included in the body of the draft and that many of these point to established organizations. If these organizations are SDOs or government bodies, this is fine. If not (e.g., Mastercard), you will be asked to submit the relevant info to the IEEE so that the IEEE can host it on an IEEE Web site. The point is to ensure that the info is available, current, and relevant. When material is on non-IEEE Web sites, this is out of the hands of the IEEE to monitor.

?Please consider the various Web sites referred to in text and determine whether they are most appropriate as part of the normative body of the text or as entries in an informative bibliography?

SuggestedRemedy

Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security comments

Cl **Globa** SC P L # 78
 Thrasher, Jerry Lexmark International I

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

d) Definitions?construction of the definitions clause
 oAll terms defined in IEEE standards are incorporated into The Authoritative Dictionary [B7]. (See 10.5.2 of 2007 Style Manual)

? If the definitions included in the draft are intended to only be applicable to the draft (as stated in the preface to the definitions clause), please change the name of the clause from ""Definitions"" to ""Special terms."" Otherwise, please follow the guidelines for definitions outlined in the 2007 Style Manual (e.g., no self-references) and remove the sentence that introduces the definitions

SuggestedRemedy

Proposed Response Response Status

Cl **Globa** SC P L # 77
 Thrasher, Jerry Lexmark International I

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

c) Reproduced tables, figures, or text
 oWorking groups shall obtain permission to use any figure taken from another source, including from a manufacturer, preferably prior to using it in a draft standard.ö (See 16.1 of 2007 Style Manual) Sample copyright permission letters are found in Annex D of the 2007 Style Manual.

?

SuggestedRemedy

Please ensure that the necessary and appropriate permissions have been obtained for any reproduced tables, figures, or text. Even if they were used previously, the permissions might need to be updated.

Proposed Response Response Status

Cl **Globa** SC P L # 76
 Thrasher, Jerry Lexmark International I

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

b) Normative and informative clauses
 ""Normative text means information that is required to implement the standard and is therefore officially part of the standard. Informative text is provided for information only and is therefore not officially part of the standard. The draft standard shall contain normative text in the main clauses of the document, including footnotes to tables (see 15.5), and in normative annexes. Informative text shall be placed in notes (to text, tables, and figures), in footnotes within text, and in informative annexes. Interspersed normative and informative text is not allowed. As such, neither clauses nor subclauses shall be labeled as informative. Identification of normative or informative text shall be reviewed during the ballot of a document; therefore, it is important that the working group consult an IEEE Standards project editor early with any questions."" (See 10.1 of 2007 Style Manual)

?

SuggestedRemedy

Please remove the labels associated with the clauses found within the draft. Please rearrange material accordingly.

Proposed Response Response Status

Cl **Globa** SC P L # 75
 Thrasher, Jerry Lexmark International I

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

a) The title of the PAR should match the title of the draft.
 The title on the modified PAR is ""Standard for Information Technology: Hardcopy Device and System Security."" The title on the draft is ""Standard for Information Technology: Hardcopy System and Device Security."" Please change either the PAR or the draft so that the two match.

SuggestedRemedy

Proposed Response Response Status

IEEE P2600 Hardcopy Device and System Security comments

Cl **Globa** SC **3.1** P L # **83**
 Thrasher, Jerry Lexmark International I
 Comment Type **E** Comment Status **X**
 i)Document structure
 ?Should 3.1 be labeled something other than ""scope?"" The scope in Clause 1 is the scope of the project and unintended references to another scope might cause confusion.
 SuggestedRemedy
 Proposed Response Response Status **O**

Cl **Main** SC **3.4.3.4** P **21** L **12** # **56**
 Sukert, Alan Xerox
 Comment Type **E** Comment Status **X**
 The end of this line reads ""...Clauses 7, 8, and a)."" It is not clear what the 'and a)' is referring to here.
 SuggestedRemedy
 Delete the 'and a)'.
 Proposed Response Response Status **O**

Cl **Main** SC **1.3.9** P **7** L **22** # **27**
 Smithson, Brian Ricoh
 Comment Type **E** Comment Status **X**
 We should make it more clear in the document introduction that in order to claim compliance, you need to (a) pick an environment, and (b) fulfill the requirement of that environment in clause 9.
 SuggestedRemedy
 I think that a new introductory section (1.4 Compliance with this Standard) would sufficiently highlight the compliance requirements. It may be useful to have two subclauses, one for manufacturers and one for IT professionals. The content of each subclause would state the particular words that should be used for claiming compliance (noting that IEEE 2600 is a trademark, etc.) for the chosen environment and a brief statement and pointer to the appropriate subclause in clause 9 for the specific compliance requirements.
 Proposed Response Response Status **O**

Cl **Main** SC **4.2.4** P **26** L **37** # **67**
 Sukert, Alan Xerox
 Comment Type **G** Comment Status **X**
 On this line 'Denial of Service' is capitalized. The term is not capitalized other times it is used (e.g., page 23, Clause 4.2.2., line 14).
 SuggestedRemedy
 Be consistent in capitalization of the term 'denial of service' in the document.
 Proposed Response Response Status **O**

Cl **Main** SC **2.1.63** P **7** L **25** # **55**
 Sukert, Alan Xerox
 Comment Type **E** Comment Status **X**
 The acronym PP for Protection Profile is defined in Clause 2.1.63 but is not included in the list of acronyms and abbreviations defined in Clause 2.2.
 SuggestedRemedy
 Either define the acronym 'PP' in clause 2.2 or don't use the PP acronym in clause 2.1.63 and elsewhere in the document.
 Proposed Response Response Status **O**

Cl **Main** SC **4.3.4** P **31** L **37** # **71**
 Sukert, Alan Xerox
 Comment Type **T** Comment Status **X**
 I noted that for Operational Environment B, the listed security expectations in this subclause only cover protection of user documents from unauthorized disclosure, modification or access when the documents are stored in the HCD. This is inconsistent with subclause 9.1.2.5 that requires protection of protected and confidential data and software in transit for Operational Environment B.
 SuggestedRemedy
 Modify page 31, line 37 to read ""... while both stored and in transit.""
 Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security comments

Cl Main SC 4.4.3 P 33 L 26 # 72
 Sukert, Alan Xerox

Comment Type T Comment Status X

The list of security expectations for Operational Environment C in subclause 4.4.3 includes the following expectation -- "HCDs are expected to provide protections against the disclosure of residual user document information that may reside in the HCD after processing of that user document is completed." This is consistent with the Security Objective for Operational Environment C described in subclause 9.1.3.1.

I noted that the same security objective is listed for Operational Environments A and B in subclauses 9.1.1.3 and 9.1.2.3, respectively, but the corresponding security expectation is not included in either subclause 4.2.4 for Operational Environment A or in subclause 4.3.4 for Operational Environment B.

SuggestedRemedy

Include the security expectation "HCDs are expected to provide protections against the disclosure of residual user document information that may reside in the HCD after processing of that user document is completed." in subclauses 4.2.4 for Operational Environment A and 4.3.4 for Operational Environment B.

Proposed Response Response Status O

Cl Main SC 4.5.4 P 37 L 9 # 73
 Sukert, Alan Xerox

Comment Type T Comment Status X

The security expectation for Operational Environment D in lines 9-11 doesn't indicate whether this applies to information stored in the TOE, in transit or both. Since the security objectives for Operational Environment D in subclauses 9.1.4.1 and 9.1.4.2 cover protection of data both when it is stored and when it is in transit, it is suggested that line 11 be changed to read " ...for certain types of security related information) both stored and in transit.

SuggestedRemedy

See comment above

Proposed Response Response Status O

Cl Main SC 6.1.1 P 41 L 20 # 57
 Sukert, Alan Xerox

Comment Type E Comment Status X

Grammatically the wording 'Disclosure to...' should be 'disclosed to...' on line 20.

SuggestedRemedy

See comment above

Proposed Response Response Status O

Cl Main SC 6.2 P L # 6
 Chen, Nancy Oki Data

Comment Type E Comment Status X

Would like the Clause references be clickable links.

SuggestedRemedy

Change the Clause references to clickable links.

Proposed Response Response Status O

Cl Main SC 6.4.2 P 69 L 1 # 58
 Sukert, Alan Xerox

Comment Type E Comment Status X

1. Table 52 contains a row for threat T.FUNC.TEMP.ALT. However, this threat is not discussed anywhere else in Clause 6.

2. Table 53 indicates threat T.HCD.AVAIL.BYPASS is discussed in subclause 6.3.2.2. Actually it is discussed in subclause 6.3.2.1.

SuggestedRemedy

1. Delete the row for threat T.FUNC.TEMP.ALT in Table 52.

2. Change 6.3.2.2 to 6.3.2.1 in the row for threat T.HCD.AVAIL.BYPASS.

Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security comments

Cl Main SC 7.3.11.3 P L # 3
 aubry, carmen oce
 Comment Type E Comment Status X
 Solutions less efficient appear before the ones more effective in mitigating or even preventing the risk:
 d is less efficient than h
 SuggestedRemedy
 Change the order to reflect the efficiency.
 Proposed Response Response Status O

Cl Main SC 7.3.3.3 P L # 1
 aubry, carmen oce
 Comment Type E Comment Status X
 Less efficient solutions appear before the ones more effective in mitigating or even preventing the risk:
 b is on second position while more effective ones like f, g, h are by the end.
 SuggestedRemedy
 Change the order to reflect the effectiveness.
 Proposed Response Response Status O

Cl Main SC 7.3.15.2 P 96 L 19 # 59
 Sukert, Alan Xerox
 Comment Type E Comment Status X
 The sentence starting in line 19 has a couple of grammatical errors in it.
 SuggestedRemedy
 Revise the sentence to read ""If authenticated or poorly authenticated access methods are present in the HCD, an attacker can access...""
 Proposed Response Response Status O

Cl Main SC 7.6.3.3 P 109 L 30 # 15
 Chen, Nancy Oki Data
 Comment Type T Comment Status X
 white list, black list, MAC, phone are not protocol or port, they are address filters.
 SuggestedRemedy
 (1) Delete ""(e.g.,white list, black list of IP, MAC, phone etc.)""
 (2) Add an additional mitigation technique as b): ""Providing address or destination filters to block/permit connections from unknown/know hosts (e.g. white list, black list of IP, MAC, phone, etc.)
 Proposed Response Response Status O

Cl Main SC 7.3.2 P L # 4
 aubry, carmen oce
 Comment Type T Comment Status X
 T.DOC.CAMERA.DIS
 The description of this threat gives the impression that the camera is external to the HCD.
 a) to d) will reduce the risk of gaining access to internal of the HCD. This is not really a mitigation technique for this particular threat.
 SuggestedRemedy
 Only e) seems appropriate for this threat.
 Proposed Response Response Status O

Cl Main SC 7.6.3.3 P 109 L 34 # 13
 Chen, Nancy Oki Data
 Comment Type T Comment Status X
 Some embedded OS are not standard UNIX OS but may implement standard Unix services such as telnet.
 SuggestedRemedy
 Delete ""If a standard off-the-shelf operating system is used,"" from the mitigation technique (c).
 Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security comments

Cl Main SC 8.2.2.6.3 P 117 L 12 # 60
 Sukert, Alan Xerox
 Comment Type E Comment Status X
 Sentence has an extra 'focused' that should be removed.
 SuggestedRemedy
 Revise the sentence to read "...the focus of security code reviews or inspections could be on the..."
 Proposed Response Response Status O

Cl Main SC 8.4.2 P 125 L 4 # 62
 Sukert, Alan Xerox
 Comment Type E Comment Status X
 Since this subclause is about providing network data confidentiality, integrity and non-repudiation, to avoid confusion it is suggested that this sentence be revised to read "Mechanisms that can be used in an HCD environment to provide network data confidentiality, integrity and non-repudiation are:"
 SuggestedRemedy
 See comment above
 Proposed Response Response Status O

Cl Main SC 8.2.2.6.4.2.1 P 118 L 11 # 61
 Sukert, Alan Xerox
 Comment Type E Comment Status X
 Grammatical error in this sentence should be corrected. I also noted there are two extra periods at the end of this sentence that should be removed.
 SuggestedRemedy
 Revise the sentence to read "...ilities" and should be specified and measured to ensure the required level of security is achieved."
 Proposed Response Response Status O

Cl Main SC 8.7.3.1 P 137 L 43 # 70
 Sukert, Alan Xerox
 Comment Type T Comment Status X
 Table 53 needs to include the following Disk Overwriting techniques: DoD Directive 5200.28-M and AIR FORCE SYSTEM SECURITY INSTRUCTION 5020.
 SuggestedRemedy
 Add the following two rows to Table 53:

 U.S. Government 3 Pass 1: ASCII 050 (hex value 0x35) all bytes
 DoD 5200.28-M Pass 2: ASCII compliment of 5 (hex value 0xCA) all bytes
 Pass 3: ASCII 097 (hex value 0x97) all bytes

 U.S. Government 3 Pass 1: Binary zeros (i.e., 0000 0000) all bytes
 AFSS 5020 Pass 2: Binary ones (i.e., 1111 1111) all bytes
 Pass 3: Any character (e.g., "a") all bytes
 Proposed Response Response Status O

Cl Main SC 8.4.2 P L # 2
 aubry, carmen oce
 Comment Type E Comment Status X
 d) Use of Kerberos system encryption;
 It is not clear.
 Kerberos is a trusted third-party authentication system that helps implementing data confidentiality solutions (it is not at the same level like the other examples). Kerberos authentication can optionally support encryption, although this is not a well-supported option.
 SuggestedRemedy
 Provide some references for the use of Kerberos like a data encryption solution.
 Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security comments

Cl Main SC 9.1 P 142 L 2 # 48
 Smithson, Brian Ricoh
 Comment Type T Comment Status X
 There is no security objective for the HCD (in any environment) to provide a procedure for verifying that the installed software is consistent with the authorized installed software.
 SuggestedRemedy
 Add an objective to all environments ""The HCD shall provide procedures to verify that the currently installed software in the HCD is consistent with the authorized installed HCD software."" and add examples such as checksums, CRCs, etc.
 Proposed Response Response Status O

Cl Main SC 9.1.1.10 P 144 L 39 # 38
 Smithson, Brian Ricoh
 Comment Type T Comment Status X
 Since DoS attack is outside of PP scope (and cannot be fully tested), it should be stated as *should* not shall. This comment also applies elsewhere in clause 9 if it appears in other environments.
 SuggestedRemedy
 ""The HCD should protect assets during denial of service attacks against the external HCD interfaces, and should restore normal operation without requiring human intervention upon termination of such attacks.""
 Proposed Response Response Status O

Cl Main SC 9.1 P 142 L 6 # 28
 Smithson, Brian Ricoh
 Comment Type E Comment Status X
 What exactly is the text/logo/whatever that a manufacturer can use to claim compliance?
 SuggestedRemedy
 Give the exact wording, reference to logos (if we get one from IEEE), etc.
 If this is already stated (per my other comment) in clause 1, then just put a pointer in clause 9 to the subclause of clause 1.
 Proposed Response Response Status O

Cl Main SC 9.1.1.2 P 142 L 22 # 52
 Smithson, Brian Ricoh
 Comment Type T Comment Status X
 No need to say that you deny permission to unauthorized users. No need to specify software install, it is covered by TSF data protection objective. This comment also applies elsewhere in clause 9 if it appears in other environments.
 SuggestedRemedy
 Remove this sentence from the objective.
 Proposed Response Response Status O

Cl Main SC 9.1.1.1, 9.1.1.2 P 142 L 10 # 53
 Smithson, Brian Ricoh
 Comment Type T Comment Status X
 These two subclauses could be combined into a single item (such as is done in 9.1.1.6 for administrators). This comment also applies elsewhere in clause 9 if it appears in other environments.
 SuggestedRemedy
 Combine 9.1.1.1 and 9.1.1.2 into a single objective ""The HCD shall require identification and authentication of Users, and shall ensure that Users are authorized in accordance with security policies before allowing them to use the HCD.""
 Proposed Response Response Status O

Cl Main SC 9.1.1.2 P 142 L 27 # 29
 Smithson, Brian Ricoh
 Comment Type E Comment Status X
 Example could use a little better wording. This comment also applies elsewhere in clause 9 if it appears in other environments, and should be reflected in the source of the example in clause 7.
 SuggestedRemedy
 ""Providing the ability for the administrator to define and set rules governing permissions given to users or groups of users, such as for access to print, scan, fax, or copy functions, access to color printing, or limits on the number of pages that can be processed""
 Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security comments

Cl Main SC 9.1.1.3 P 142 L 31 # 32
 Smithson, Brian Ricoh

Comment Type E Comment Status X

The objective is OK, but why not use the PP objective text (minus CC language)? This comment also applies elsewhere in clause 9 if it appears in other environments.

SuggestedRemedy

""The HCD shall protect deleted User Document Data in a nonvolatile storage medium that has been removed from HCD from unauthorized salvage.""

Proposed Response Response Status O

Cl Main SC 9.1.1.4 P 143 L 2 # 7
 Chen, Nancy Oki Data

Comment Type E Comment Status X

The title cannot be easily distinguished from 9.1.1.5.

SuggestedRemedy

Add ""in the HCD"" at the end of the title

Proposed Response Response Status O

Cl Main SC 9.1.1.4.1 P 143 L 4 # 45
 Smithson, Brian Ricoh

Comment Type T Comment Status X

The objective does not distinguish online access threat from offline salvage threat (for Document Data). Since the set of mitigation techniques would be different (e.g. ""secure printing"" does nothing for salvage threat), it should be a new objective.

SuggestedRemedy

Add a new objective that is specific to offline salvage of Document Data from removable nonvolatile storage, with example mitigation of encrypting data.

Proposed Response Response Status O

Cl Main SC 9.1.1.4.1 P 143 L 7 # 63
 Sukert, Alan Xerox

Comment Type E Comment Status X

The last technique listed in this subclause (Providing configurable access control mechanisms...) is not from either subclause 7.3.8 or 7.4.4; it is from subclause 7.3.10.

Note that the same comment applies to subclause 9.1.2.4.1, page 146, line 4

SuggestedRemedy

Either remove the last technique listed in subclause 9.1.1.4.1 or revise line 7 to read ""For example, possible techniques may be found in 7.3.8, 7.3.10 and 7.4.4: ""

Same suggestion for subclause 9.1.2.4.1

Proposed Response Response Status O

Cl Main SC 9.1.1.4.1 P 143 L 16 # 34
 Smithson, Brian Ricoh

Comment Type T Comment Status X

We should recommend authentication mechanisms for any user (not just admin) access. This comment also applies elsewhere in clause 9 if it appears in other environments, and should be reflected in the source of the example in clause 7.

SuggestedRemedy

""Providing support for strong authentication mechanisms for user and administrator access""

Proposed Response Response Status O

Cl Main SC 9.1.1.4.1 P 143 L 16 # 46
 Smithson, Brian Ricoh

Comment Type T Comment Status X

The example also applies to User access (for Document Data protection). This comment also applies elsewhere in clause 9 if it appears in other environments.

SuggestedRemedy

Add a similar example for authentication mechanisms for user access.

Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security comments

Cl Main SC 9.1.1.4.1 P 143 L 17 # 47
 Smithson, Brian Ricoh
Comment Type T **Comment Status** X
 The example also applies to documents and any confidential data, not just authentication data. This comment also applies elsewhere in clause 9 if it appears in other environments.
SuggestedRemedy
 Expand or add examples.
Proposed Response **Response Status** O

Cl Main SC 9.1.1.4.2 P 143 L 24 # 69
 Sukert, Alan Xerox
Comment Type G **Comment Status** X
 For consistency with the other subclause references used in subclause 9.1.1, change the subclause reference in line 24 from 7.3.10.3 to 7.3.10.
 A similar comment applies to other subclauses (e.g., 9.1.1.7, page 144, line 17 - use 7.4.3 instead of 7.4.3.3) throughout clause 9.
SuggestedRemedy
 In clause 9, make references to clause 7 subclauses consistent in terms of the subclause references (i.e., either always reference the main subclause like 7.3.10 or reference the specific subclause like 7.3.10.3 where the indicated technique(s) can be found).
Proposed Response **Response Status** O

Cl Main SC 9.1.1.4.2 P 143 L 25 # 35
 Smithson, Brian Ricoh
Comment Type T **Comment Status** X
 For consistency, we should provide the same examples for authentication mechanisms as in 9.1.1.4.1. This comment also applies elsewhere in clause 9 if it appears in other environments.
SuggestedRemedy
 use the authentication mechanism text from 9.1.1.4.1 (note that I recommend a change to that text in another comment)
Proposed Response **Response Status** O

Cl Main SC 9.1.1.6 P 144 L 7 # 31
 Smithson, Brian Ricoh
Comment Type E **Comment Status** X
 The objective is OK, but why not just use the PP objective (without CC-specific language)? This comment also applies elsewhere in clause 9 if it appears in other environments.
SuggestedRemedy
 The HCD shall require identification and authentication of Administrators, and shall ensure that Administrators, are authorized in accordance with security policies before allowing them to manage the HCD.
Proposed Response **Response Status** O

Cl Main SC 9.1.1.7 P 144 L 15 # 44
 Smithson, Brian Ricoh
Comment Type T **Comment Status** X
 ""keep track of"" is not very specific, and the objective is not just to log ""changes that effect security or operation"", it is to log the use of the HCD and security-relevant events. This comment also applies elsewhere in clause 9 if it appears in other environments.
SuggestedRemedy
 ""The HCD shall create and maintain a log of HCD use and security-relevant events.""
Proposed Response **Response Status** O

Cl Main SC 9.1.1.8 P 144 L 22 # 36
 Smithson, Brian Ricoh
Comment Type T **Comment Status** X
 We do not have an objective that the HCD shall mediate connections to SMIs? (e.g. the HCD only lets HCD apps talk to the network, it does not provide general-purpose network access). This comment also applies elsewhere in clause 9 if it appears in other environments.
SuggestedRemedy
 Modify 9.1.1.8 to have an expanded definition ("used as a proxy for or source of malicious attacks") or add a new subclause for that objective.
Proposed Response **Response Status** O

IEEE P2600 Hardcopy Device and System Security comments

Cl Main SC 9.1.1.8 P 144 L 27 # 14
Chen, Nancy Oki Data

Comment Type T Comment Status X

White list, black list, MAC, phone are not protocol or port, they are address filters.

SuggestedRemedy

(1) Delete ""(e.g., white list, black list of IP, MAC, phone etc.)"" from the example mitigation technique.

(2) Add an additional technique on page 109 that states: ""Providing address or destination filters to block/permit connections from unknown/known hosts (e.g., white list, black list of IP, MAC, phone etc.)""

Proposed Response Response Status O

Cl Main SC 9.1.1.9 P 144 L 31 # 37
Smithson, Brian Ricoh

Comment Type T Comment Status X

The objective should that the HCD cannot be used to *maliciously* bridge between *any* interface and network interfaces. This comment also applies elsewhere in clause 9 if it appears in other environments.

SuggestedRemedy

Restate the objective to clarify the that it shall not be used *maliciously* to bridge *any* interface, then give fax bridging as an example.

Proposed Response Response Status O

Cl Main SC 9.1.2.10 P 147 L 36 # 64
Sukert, Alan Xerox

Comment Type E Comment Status X

The subclause references are incorrect as stated on this line.

SuggestedRemedy

Change the subclause references to be 7.1.11.3 and 7.1.9.3, respectively.

Proposed Response Response Status O

Cl Main SC 9.1.3.5 P 149 L 19 # 8
Chen, Nancy Oki Data

Comment Type E Comment Status X

Wrong reference.

SuggestedRemedy

Change 8.4.3.3 to 7.4.3.3

Proposed Response Response Status O

Cl Main SC 9.1.3.5 P 149 L 19 # 65
Sukert, Alan Xerox

Comment Type E Comment Status X

The subclause reference on this line is incorrect.

SuggestedRemedy

Change the subclause reference to be 7.4.3.3

Proposed Response Response Status O

Cl Main SC 9.1.3.8 P 150 L 6 # 16
Chen, Nancy Oki Data

Comment Type T Comment Status X

This example is not appropriate for Env. C. It is reasonable for ""mission critical"" environment such as in an air fighter where automatic and timely recovery is critical. But unless somebody can show a RFP to prove this requirement for Env. C, it should be removed here.

SuggestedRemedy

Delete this example mitigation technique.

Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security comments

Cl Main SC 9.2.1.1 P 152 L 10 # 50
 Smithson, Brian Ricoh
 Comment Type T Comment Status X
 It is the HCD Owner's responsibility to ensure this. This comment also applies elsewhere in clause 9 if it appears in other environments.
 SuggestedRemedy
 ""The HCD owner shall ensure that HCD Administrators are aware of the security policies and procedures of their organization, have the training and competence to follow the manufacturer's guidance and documentation, and correctly configure and operate the HCD in accordance with those policies and procedures.""
 Proposed Response Response Status O

Cl Main SC 9.2.1.1 P 152 L 18 # 39
 Smithson, Brian Ricoh
 Comment Type T Comment Status X
 The 2nd example in 9.2.1.2 line 26 for Users should also apply to Administrators. This comment also applies elsewhere in clause 9 if it appears in other environments.
 SuggestedRemedy
 Add example ""Educating administrators to exercise care in selecting passwords and in entering user authentication data at the operator panel of the HCD""
 Proposed Response Response Status O

Cl Main SC 9.2.1.1 P 152 L 18 # 30
 Smithson, Brian Ricoh
 Comment Type E Comment Status X
 there is an editorial note left in this section on line 18
 SuggestedRemedy
 do what it says? then remove the note
 Proposed Response Response Status O

Cl Main SC 9.2.1.1 P 152 L 18 # 66
 Sukert, Alan Xerox
 Comment Type E Comment Status X
 The note on this line is an editorial comment and should be removed
 SuggestedRemedy
 See comment above
 Proposed Response Response Status O

Cl Main SC 9.2.1.10 P 154 L 2 # 54
 Smithson, Brian Ricoh
 Comment Type T Comment Status X
 ""exceptions"" doesn't really capture the intended objective, and ""regular intervals"" is too specific. Also, it is the HCD Owner responsibility to ensure this. This comment also applies elsewhere in clause 9 if it appears in other environments.
 SuggestedRemedy
 ""The HCD owner shall ensure that audit logs are reviewed at appropriate intervals for security violations or unusual patterns of activity.""
 Proposed Response Response Status O

Cl Main SC 9.2.1.11 P 154 L 16 # 68
 Sukert, Alan Xerox
 Comment Type G Comment Status X
 In this line the term antivirus is spelled as 'anti-virus'. Elsewhere in the document the term is spelled as 'antivirus'
 SuggestedRemedy
 Be consistent in how the term 'antivirus' is spelled within the document.
 Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security comments

Cl Main SC 9.2.1.2 P 152 L 20 # 51
 Smithson, Brian Ricoh
 Comment Type T Comment Status X
 It is the HCD Owner's responsibility to ensure this. This comment also applies elsewhere in clause 9 if it appears in other environments.
 SuggestedRemedy
 ""The HCD owner shall ensure that HCD Users are aware of the security policies and procedures of their organization, have sufficient training and competence, and follow those policies and procedures.""
 Proposed Response Response Status O

Cl Main SC 9.2.1.6 P 153 L 10 # 41
 Smithson, Brian Ricoh
 Comment Type T Comment Status X
 What is the purpose of this objective? If it is intended to suggest that there can be different administrative roles, then it should be stated as SHOULD. Otherwise, it should be covered in 9.1.1.6. This comment also applies elsewhere in clause 9 if it appears in other environments.
 SuggestedRemedy
 Depends on the intention of the objective, see Comment.
 Proposed Response Response Status O

Cl Main SC 9.2.1.3 P L # 33
 Smithson, Brian Ricoh
 Comment Type E Comment Status X
 It is OK as is, but the PP objective is a little more clear in its statement that a secure or monitored location is the objective. This comment also applies elsewhere in clause 9 if it appears in other environments.
 SuggestedRemedy
 ""The HCD shall be placed in secure or monitored area that limits the opportunity for unauthorized physical access to the HCD.""
 Proposed Response Response Status O

Cl Main SC 9.2.1.7 P 153 L 11 # 17
 Chen, Nancy Oki Data
 Comment Type T Comment Status X
 The example shows that this is a requirement for Manufacturers.
 SuggestedRemedy
 Delete. ""User authorization"" is already in the objectives for HCD manufacturers.
 Proposed Response Response Status O

Cl Main SC 9.2.1.5 P 153 L 8 # 40
 Smithson, Brian Ricoh
 Comment Type T Comment Status X
 Another (obvious) example would be to put the HCD behind a firewall. This comment also applies elsewhere in clause 9 if it appears in other environments, and should be reflected in the source of the example in clause 7.
 SuggestedRemedy
 Add an example of using a firewall. There should be one in clause 7, but if not, one should be added there.
 Proposed Response Response Status O

Cl Main SC 9.2.1.8 P 153 L 25 # 49
 Smithson, Brian Ricoh
 Comment Type T Comment Status X
 ""take steps to"" is a very weak way to state the objective. This comment also applies elsewhere in clause 9 if it appears in other environments.
 SuggestedRemedy
 ""The HCD owner shall establish trust that HCD Administrators will not use their privileged access rights for malicious purposes.""
 Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security comments

Cl Main SC 9.2.1.8 P 153 L 30 # 42
 Smithson, Brian Ricoh
Comment Type T **Comment Status** X
 The example given doesn't really address the requirement. This comment also applies elsewhere in clause 9 if it appears in other environments, and should be reflected in the source of the example in clause 7.
SuggestedRemedy
 Consider removing the example. Add new examples of rotation of duties, third party audits, background checks.
Proposed Response **Response Status** O

Cl Main SC 9.2.1.9 P 153 L 35 # 43
 Smithson, Brian Ricoh
Comment Type T **Comment Status** X
 Remote storage is outside of PP (and HCD) scope, so it should be stated as *should* not shall. This comment also applies elsewhere in clause 9 if it appears in other environments.
SuggestedRemedy
 ""Remotely stored records and logs that provide an audit trail for an HCD should be maintained and protected from unauthorized disclosure or alteration""
Proposed Response **Response Status** O

Cl Main SC 9.2.2 P 154 L # 18
 Chen, Nancy Oki Data
Comment Type T **Comment Status** X
 Missing ""Audit Trail Protection"" and ""Review Audit Trail for Unusual Patterns"" objectives in Env. B
SuggestedRemedy
 Add to Environment B, in Objectives for IT Professionals.
Proposed Response **Response Status** O

Cl Main SC 9.2.2 P 154 L 18 # 74
 Sukert, Alan Xerox
Comment Type T **Comment Status** X
 It is not clear to me why the 'Audit Trail Protection' and 'Review Audit Trail for unusual patterns' security objectives for IT professionals are included for Operational Environments A and C but not for Operational Environment B, especially since monitoring and recording security related events in a protected log is one of the general security expectations listed for Operational Environment B in subclause 4.3.4.
SuggestedRemedy
 Add the text for 'Audit Trail Protection' and 'Review Audit Trail for unusual patterns' in subclauses 9.2.1.9 and 9.2.1.10, respectively, to subclause 9.2.2 for Operational Environment B.
Proposed Response **Response Status** O

Cl Main SC 9.2.2.7 P 155 L 31 # 19
 Chen, Nancy Oki Data
Comment Type T **Comment Status** X
 ""User authorization"" is an objective for HCD Manufacturers.
SuggestedRemedy
 Delete from objectives for IT Professionals.
Proposed Response **Response Status** O

Cl Main SC 9.2.3 P 156 L # 22
 Chen, Nancy Oki Data
Comment Type T **Comment Status** X
 ""Protecting Data on Shared Communication Medium"" is an objective for Evn. C IT Professionals, based on P2600master-30b.
SuggestedRemedy
 Add.
Proposed Response **Response Status** O

IEEE P2600 Hardcopy Device and System Security comments

CI **Main** SC **9.2.3** P **156** L # **21**
Chen, Nancy Oki Data
Comment Type **T** Comment Status **X**
""Protecting from unmanaged public access"" is an objective for IT professionals in Env. C,
based on P2600master-30b.
SuggestedRemedy
Add.
Proposed Response Response Status **O**

CI **Main** SC **9.2.3.3** P **156** L **25** # **20**
Chen, Nancy Oki Data
Comment Type **T** Comment Status **X**
No ""User authorization"" requirement in Env. C for IT environment based on P2600master-
30b.
SuggestedRemedy
Delete.
Proposed Response Response Status **O**

CI **P2600** SC P L # **23**
Chen, Nancy Oki Data
Comment Type **T** Comment Status **X**
Delete ""Limited Physical Access"" objective from Environment C in P2600master-30b
SuggestedRemedy
HCDs in Environment C normally are openly accessible to the public, though maybe placed
in an area where visual monitoring is easy for administrative staff in some organizations.
Proposed Response Response Status **O**