

IEEE P2600 Hardcopy Device and System Security Comments

Cl **Compl** SC 10.1.1.2 P 2 L 16 # 65  
Farrell, Lee Canon

Comment Type **E** Comment Status **X**  
[also clause 10.1.2.2]

The first sentence seems very awkward. I'm not sure how to parse the intent of the parenthetical phrase. Is it necessary? Could it be reworded and separated into a second sentence to qualify the first?

*SuggestedRemedy*

Either eliminate parenthetical phrase or reconstruct into two sentences.

Proposed Response Response Status **O**

Cl **Compl** SC 10.1.1.2 P 2 L 25 # 66  
Farrell, Lee Canon

Comment Type **E** Comment Status **X**  
[also in clauses 10.1.1.4.1.1, 10.1.2.2, 10.1.2.4.1.1, 10.1.3.2.1.1, and 10.1.4.1.1.1]

The example should be modified to read, ""à and limits ON the number of printed pages."" [Or if you prefer, ""TO""]

*SuggestedRemedy*

The example should be modified to read, ""à and limits ON the number of printed pages."" [Or if you prefer, ""TO""]

Proposed Response Response Status **O**

Cl **Compl** SC 10.1.1.4.1.1 P 3 L 1 # 64  
Farrell, Lee Canon

Comment Type **T** Comment Status **X**  
[also clauses 10.1.1.4.1.2, 10.1.1.5.1.1, 10.1.1.5.1.2, 10.1.2.4.1.1, 10.1.2.4.1.2, 10.1.2.5.1.1, 10.1.2.5.1.2, 10.1.3.2.1.1, 10.1.3.2.1.2, 10.1.3.3.1.1, 10.1.3.3.1.2, 10.1.4.1.1.1, 10.1.4.1.1.2, 10.1.4.2.1.1, and 10.1.4.2.1.2]

The heading level is one level too deep.

*SuggestedRemedy*

Make the heading levels correct.

Proposed Response Response Status **O**

Cl **Compl** SC 10.1.1.7 P 4 L 7 # 67  
Farrell, Lee Canon

Comment Type **E** Comment Status **X**  
[also in clauses 10.1.2.7, and 10.1.3.5]

Misspelling of security ("security")

*SuggestedRemedy*

Correct spelling

Proposed Response Response Status **O**

Cl **Compl** SC 10.1.2.9 P 7 L 8 # 62  
Farrell, Lee Canon

Comment Type **E** Comment Status **X**  
[also in clauses 10.1.3.7 and 10.1.4.5]

Why is the text here different to the text in 10.1.1.9? Is there significance to the different wording?

*SuggestedRemedy*

Make the text in all four clauses consistent to describe what appears to be the same goal.

Proposed Response Response Status **O**

Cl **Compl** SC 10.2.1.4 P 12 L 30 # 63  
Farrell, Lee Canon

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

Why is the example here different to the ones in 10.1.4.2? Is there significance to the different wording?

*SuggestedRemedy*

Make the example consistent

Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-A** SC **Section 5.5.3** P **13** L **9** # **61**

Yami, Sameer Toshiba

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

As per the July 2007 meeting, the resolution to add that that - "It is upto the ST author to define the relevant TSF data" is still missing.

Unless ,it is implied on Page 13, line 15 Section 5.5.3. However, I am not sure how.

SuggestedRemedy

Proposed Response Response Status **O**

Cl **Main** SC **3.2** P **14** L  # **1**

Thrasher, Jerry Lexmark

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

The acronym VPN is used in Clause 9, but is not included in 3.2.

SuggestedRemedy

Add ""VPN--Virtual Private Network in the acronym list.

Proposed Response Response Status **O**

Cl **Main** SC **10.1.1.4.1.1** P **145** L **7** # **56**

aubry, carmen oce

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

These comments concern the compliance clause v29.a:  
[http://grouper.ieee.org/groups/2600/drafts/compliance/IEEE\\_P2600\\_Clause\\_10\\_v29a.pdf](http://grouper.ieee.org/groups/2600/drafts/compliance/IEEE_P2600_Clause_10_v29a.pdf)

(10.1.1.4.1.1 From Disclosure)I think that this is an example for user authorization and not for User Document Data and Confidential Data protection against disclosure.

SuggestedRemedy

- For User Document Data protection against disclosure, I suggest something like:
- \* Providing local "secure printing," whereby the document is held on the HCD's local hard disk and not printed until the end user releases the document for printing by entering a valid job ID, password, or PIN code
  - \* Providing server-based "secure printing," whereby the document is held in a secure spool area on the print server's hard disk and not transmitted to the HCD for printing until the end user releases the document by authenticating at the HCD, whether by using an identity card, PIN codes, network security authentication data, or biometric authentication
  - \* Providing the capability for disabling unauthenticated document storage, retrieval, and proof printing capability in the HCD

For Confidential Data protection against disclosure, I suggest something like:

- \* Ensuring that any authentication data stored on the HCD are encrypted

Note: These examples come from the standard  
[http://grouper.ieee.org/groups/2600/drafts/FullSpec/IEEE\\_P2600\\_v29a.pdf](http://grouper.ieee.org/groups/2600/drafts/FullSpec/IEEE_P2600_v29a.pdf).

Similar remark for "Protecting User Document Data, User Function Data, Confidential Data, Protected Data, and Software: From Disclosure" in the other environments 5B, C and D).

Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security Comments

Cl Main SC 10.2 P 153 L 31 # 57  
 aubry, carmen oce

Comment Type T Comment Status X

In the main body, when describing general practices for systems in environment A (http://grouper.ieee.org/groups/2600/drafts/FullSpec/IEEE\_P2600\_v29a.pdf, page 31, line 8), we have something like:

\* Systems are placed behind firewalls and other network security devices to restrict access and filter unnecessary protocols. Furthermore, we are proposing as a Recommended Mitigation Techniques for IT Professionals (http://grouper.ieee.org/groups/2600/drafts/FullSpec/IEEE\_P2600\_v29a.pdf.) in preventing the DOS attacks:

\* Limiting network access to the HCDs to specific network nodes, such as print and mail servers, through the use of VLANs or similar technologies

The compliance clause, 10.2 Security Objectives for IT Professionals in Environment A doesn't mention anything similar.

SuggestedRemedy

I understand why it was removed from the PPs (because we removed the DOS attacks). Nevertheless, as long as DOS attacks are considered in the Compliance clauses, we should include something about it.

Proposed Response Response Status O

Cl Main SC 3.1.77 P 16 L 6 # 60  
 Yami, Sameer Toshiba

Comment Type E Comment Status X

User can be an internal entity also.

SuggestedRemedy

Add internal to 'An entity (human user or external IT entity)...' to make it 'An entity (human user or internal / external IT entity)...'

Proposed Response Response Status O

Cl Main SC 4.2.2.4 P 18 L 20 # 2  
 Thrasher, Jerry Lexmark

Comment Type E Comment Status X

The last sentence talks about HCD's creating color prints as well as black and white. The term ""prints"" may imply to some readers photo prints.

SuggestedRemedy

Change the word ""prints"" in that sentence to output.

Proposed Response Response Status O

Cl Main SC 7.2 P 44 L 27 # 47  
 Sukert, Alan Xerox

Comment Type E Comment Status X

In Table 3 and elsewhere in the document when discussing the T.ENV.DOS threat (e.g., clause 7.3.2.6, Table 51, pg. 68 & clause 8.6.1.1, pg. 110, line 25) you refer to the term 'denial-of-service'. Elsewhere in the document (e.g., clause 5.2.2, pg. 24, line 14) you refer to this term as 'denial of service'. You should be consistent in how you refer to this term throughout the document.

SuggestedRemedy

Suggest use 'denial of service' throughout the document to be consistent.

Proposed Response Response Status O

Cl Main SC Section 7.3.1(Table 4) P 45 L 8 # 59  
 Yami, Sameer Toshiba

Comment Type E Comment Status X

'of' is missing in the 'User Document Data' description.

SuggestedRemedy

Make it 'Information that is part' + 'of' and remove either

Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security Comments

Cl Main SC 8.1 P 71 L 13 # 48  
 Sukert, Alan Xerox

Comment Type E Comment Status X

Within clause 8.1 you use both the phrase 'SOHO' and 'SOHO-like' to refer to Operational Environment D. You should be consistent with what is used elsewhere in the document ('SOHO-like').

SuggestedRemedy

Change line 13 to read ""For example, a network in a typical SOHO-like environment..."".

Proposed Response Response Status O

Cl Main SC 8.1.2.3 P 72 L 18 # 3  
 Thrasher, Jerry Lexmark

Comment Type E Comment Status X

The last part of this sentence fragment needs modifying. The phrase ""amount of time or data that can be sent or received"" (time is not sent or received)

SuggestedRemedy

change to: ""amount of real time a fax job may consume or data that can be sent or received""

Proposed Response Response Status O

Cl Main SC 8.1.4.3 P 73 L 28 # 4  
 Thrasher, Jerry Lexmark

Comment Type E Comment Status X

Same comment about ""time"" as in comment about section 8.1.2.3

SuggestedRemedy

Proposed Response Response Status O

Cl Main SC 8.1.8.3 P 76 L 30 # 5  
 Thrasher, Jerry Lexmark

Comment Type E Comment Status X

The term ""wall clock time"" is unfamiliar to me anyway. The IEEE Standard Dictionary of Electrical and Electronics Terms has a term ""real time"" that might fit better.

SuggestedRemedy

Change ""wall clock time"" to ""real time"" here and in other places if used.

Proposed Response Response Status O

Cl Main SC 8.1.9.3 P 77 L 18 # 6  
 Thrasher, Jerry Lexmark

Comment Type E Comment Status X

Mis-used word in that sentence. ""giving"" should be ""given""

SuggestedRemedy

Proposed Response Response Status O

Cl Main SC 8.1.12.3 P 79 L 41 # 7  
 Thrasher, Jerry Lexmark

Comment Type E Comment Status X

The last line of that sentence fragment needs work. Remove ""be caused to""

SuggestedRemedy

reword to ...network traffic can be automatically filtered by the network interface

Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security Comments

Cl Main SC 8.2.2.3 P 83 L 26 # 41  
 Thrasher, Jerry Lexmark

Comment Type T Comment Status X

This sentence fragment suggest that user credentials be part of the log information that should be recorded....this is bad practice.

SuggestedRemedy

change the last part of the fragment to: ....including information about the authenticated user and the quantity....

Proposed Response Response Status O

Cl Main SC 8.3.3.4 P 87 L 43 # 8  
 Thrasher, Jerry Lexmark

Comment Type E Comment Status X

The last part of this sentence fragment ends poorly.

SuggestedRemedy

Reword to ...removing the disk while the location is unmonitored

Proposed Response Response Status O

Cl Main SC 8.3.8.3 P 91 L 17 # 42  
 Chen, Nancy Oki Data

Comment Type T Comment Status X

This technique can be by-passed.

SuggestedRemedy

Require that a HCD implementing this technique must also ensure that the server-based ôsecure printingö solution can not be bypassed.

Proposed Response Response Status O

Cl Main SC 8.3.15.4 P 97 L 36 # 9  
 Thrasher, Jerry Lexmark

Comment Type E Comment Status X

Fix the bullet numbering...(IEEE template gremlin..)

SuggestedRemedy

Proposed Response Response Status O

Cl Main SC 8.3.18.2 P 99 L 38 # 10  
 Thrasher, Jerry Lexmark

Comment Type E Comment Status X

The last sentence in the background section is incorrect and unnecessary.

SuggestedRemedy

Delete the sentence.

Proposed Response Response Status O

Cl Main SC 8.3.19.2 P 100 L 25 # 49  
 Sukert, Alan Xerox

Comment Type E Comment Status X

Minor grammatical error - should be "'Operational Environment A' rather than 'Operational Environments A'.

SuggestedRemedy

See comment above.

Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security Comments

Cl Main SC 8.4.1.3 P 101 L 31 # 11  
 Thrasher, Jerry Lexmark  
 Comment Type E Comment Status X  
 The mitigation techniques in this section no longer fit the threat definition. Somewhere along the line we lost the concept of using a small camera within the HCD that recorded the contents of scanned or printed hardcopy.  
 SuggestedRemedy  
 Remove all but the last technique in this section.  
 Proposed Response Response Status O

Cl Main SC 8.4.7.2 P 106 L 14 # 12  
 Thrasher, Jerry Lexmark  
 Comment Type E Comment Status X  
 This paragraph is no longer relative to the the threat definition. The threat does NOT include sensing internal signal emissions. The paragraph really doesn't provide much additional information anyway.  
 SuggestedRemedy  
 Remove the paragraph  
 Proposed Response Response Status O

Cl Main SC 8.6.1.3 P 110 L 33 # 50  
 Sukert, Alan Xerox  
 Comment Type E Comment Status X  
 In clause 8.6.1.3, item a) you refer to the terms 'black-list' and 'white-list'. In clauses 3.1.20 and 3.1.82, respectively, we define the terms as 'black list' and 'white list'.  
 SuggestedRemedy  
 Use the terms 'black list' and 'white list' in clause 8.6.1.3, item a).  
 Proposed Response Response Status O

Cl Main SC 9.2.2.1 P 114 L 21 # 13  
 Thrasher, Jerry Lexmark  
 Comment Type E Comment Status X  
 there's an extra space between the words instructs and users.  
 SuggestedRemedy  
 remove the space  
 Proposed Response Response Status O

Cl Main SC 9.2.2.1 P 114 L 31 # 14  
 Thrasher, Jerry Lexmark  
 Comment Type E Comment Status X  
 The use of the word chapter is not correct.  
 SuggestedRemedy  
 change to sub-clause  
 Proposed Response Response Status O

Cl Main SC 9.2.2.2 P 115 L 31 # 15  
 Thrasher, Jerry Lexmark  
 Comment Type E Comment Status X  
 Need a space between the bibliography reference [B14] and the word and.  
 SuggestedRemedy  
 Proposed Response Response Status O

Cl Main SC 9.2.2.7.2 P 121 L 13 # 16  
 Thrasher, Jerry Lexmark  
 Comment Type E Comment Status X  
 This sentence fragment is missing a word....  
 SuggestedRemedy  
 Reword to: Code signing can be an important tool to help maintain...  
 Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security Comments

Cl Main SC 9.2.2.7.3 P 121 L 37 # 17  
Thrasher, Jerry Lexmark

Comment Type E Comment Status X

This set of requirements in general uses the forbidden word "must", but specifically (e) requires that patches be "easily" reversible. This set of requirements/recommendations may have come from another source, possibly word for word. (Alan S. needs to advise)

SuggestedRemedy

Proposed Response Response Status O

Cl Main SC 9.2.2.7.5 P 122 L 18 # 18  
Thrasher, Jerry Lexmark

Comment Type E Comment Status X

Need to change the word "were" needs to be changed to "are".

SuggestedRemedy

Proposed Response Response Status O

Cl Main SC 9.3.2.1 P 123 L 19 # 19  
Thrasher, Jerry Lexmark

Comment Type E Comment Status X

The last sentence in the overview needs work.

SuggestedRemedy

Change to: Securing these components can prevent.....

Proposed Response Response Status O

Cl Main SC 9.3.6.1 P 126 L 7 # 20  
Thrasher, Jerry Lexmark

Comment Type E Comment Status X

The second sentence need rewording.

SuggestedRemedy

Change to: It may be possible to interpret the .....

Proposed Response Response Status O

Cl Main SC 9.3.6.2 P 126 L 17 # 21  
Thrasher, Jerry Lexmark

Comment Type E Comment Status X

the word "signal" in the last sentence needs an "s" and also includes the word "must".

SuggestedRemedy

Change to: Manufacturers should determine if such signals exist and if so,....

Proposed Response Response Status O

Cl Main SC 9.5.2.1 P 128 L 21 # 22  
Thrasher, Jerry Lexmark

Comment Type E Comment Status X

need to account for HCD's sending data to computers as well.

SuggestedRemedy

Reword the last part of the sentence to: communicate with and transfer data to and from the networked HCD.

Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security Comments

Cl Main SC 9.5.3.1 P 129 L 14 # 23  
Thrasher, Jerry Lexmark

Comment Type E Comment Status X

We need to add the concept that some of the back doors into HCDs aren't available to anybody other than the manufacturer.

SuggestedRemedy

Change the last part of the sentence to: shouldn't normally be available to a user or administrator.

Proposed Response Response Status O

Cl Main SC 9.6.1 P 130 L 17 # 24  
Thrasher, Jerry Lexmark

Comment Type E Comment Status X

This sentence fragment needs rewording.

SuggestedRemedy

Change to: Validating that the User Document Data being sent to or from the HCD is from an authenticated source

Proposed Response Response Status O

Cl Main SC 9.6.2.1 P 130 L 36 # 25  
Thrasher, Jerry Lexmark

Comment Type E Comment Status X

There's an extra word (it)

SuggestedRemedy

Remove (it)

Proposed Response Response Status O

Cl Main SC 9.6.2.1 P 130 L 37 # 26  
Thrasher, Jerry Lexmark

Comment Type E Comment Status X

The word ""chapter"" is used again...

SuggestedRemedy

Change to ""sub-clause""

Proposed Response Response Status O

Cl Main SC 9.6.2.2.1 P 131 L 11 # 27  
Thrasher, Jerry Lexmark

Comment Type E Comment Status X

This sentence needs rewording to use the defined acronym and lower case the words Web Accounts.

SuggestedRemedy

Change to: ...extensively for ATMs and web accounts and most people...

Proposed Response Response Status O

Cl Main SC 9.6.2.2.1 P 131 L 15 # 28  
Thrasher, Jerry Lexmark

Comment Type E Comment Status X

The wording of the sentence at the end of the line can be improved...

SuggestedRemedy

Change to: Therefore, with a fairly basic social engineering or brute force attack, an individual's .....

Proposed Response Response Status O

Cl Main SC 9.6.2.2.3 P 132 L 16 # 29  
Thrasher, Jerry Lexmark

Comment Type E Comment Status X

Need to change the word ""imaging"" to ""an HCD's""

SuggestedRemedy

Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security Comments

Cl Main SC 9.6.2.2.5 P 133 L 17 # 30  
Thrasher, Jerry Lexmark

Comment Type E Comment Status X

This paragraph is written such that it's not so descriptive of a current point and time.

SuggestedRemedy

Reword the paragraph to:

Smart cards are used in many environments throughout the world where multi-factor authentication is necessary. Examples include: the US Department of Defense for access authorization; the Transportation Security Administration for identification; financial services organizations for smart payment and credit cards; transit operators for fare collection; and in universities, the entertainment industry, and other enterprises for identification.

Proposed Response Response Status O

Cl Main SC 9.6.2.2.5 P 133 L 25 # 31  
Thrasher, Jerry Lexmark

Comment Type E Comment Status X

The sentence needs rewording..

SuggestedRemedy

Change to:

As described later in this sub-clause, there are many variations....

Proposed Response Response Status O

Cl Main SC 9.6.2.2.5 P 134 L 4 # 32  
Thrasher, Jerry Lexmark

Comment Type E Comment Status X

This paragraph discusses implementation alternatives and not very well.

SuggestedRemedy

Reword to:

Figure 7 indicates the basic architecture of a smart card system. Partitioning of this architecture can range from including all components of the system, the card reader (IFD), drivers (IFD handler) and the authentication infrastructure (ICC Aware Applications) as part of the HCD; to simply including the reader and leveraging some external authentication server via a secure channel.

Proposed Response Response Status O

Cl Main SC 9.6.2.2.5 P 135 L 43 # 33  
Thrasher, Jerry Lexmark

Comment Type E Comment Status X

This sentence doesn't provide any value.

SuggestedRemedy

Remove the sentence.

Proposed Response Response Status O

Cl Main SC 9.6.2.2.6 P 136 L 27 # 34  
Thrasher, Jerry Lexmark

Comment Type E Comment Status X

This paragraph describes the current state of the biometric industry but may not be true in the future. It doesn't provide any useful information.

SuggestedRemedy

Delete the paragraph.

Proposed Response Response Status O

Cl Main SC 9.6.2.3 P 137 L 12 # 35  
Thrasher, Jerry Lexmark

Comment Type E Comment Status X

The recommendation doesn't really provide any useful information as written.

SuggestedRemedy

Reword to:

Based on a security assessment of the particular environment, the IT professional should select HCDs that provide appropriate capabilities for the identification, authorization, and authorization; and deploy them per the manufacturer's recommendations.

Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security Comments

Cl Main SC 9.6.3.2 P 138 L 46 # 36  
 Thrasher, Jerry Lexmark

Comment Type E Comment Status X

Like 9.6.2.3, this recommendation doesn't provide any real guidance.

SuggestedRemedy

Reword to:  
 Based on a security assessment of the particular environment, the IT professional should select HCDs that provide appropriate capabilities for remote network authentication and access control, and deploy them per the manufacturer's recommendations.

Proposed Response Response Status O

Cl Main SC 9.8.1.3 P 142 L 27 # 37  
 Thrasher, Jerry Lexmark

Comment Type E Comment Status X

This recommendation doesn't provide any real guidance for IT professionals.

SuggestedRemedy

Reword to something similar to:  
 Based on a security assessment for the particular environment, the IT professional should select HCDs that provide appropriate capabilities for logging and auditing; and deploy them per the manufacturer's recommendations.

Proposed Response Response Status O

Cl Main SC 9.9.1.1 P 142 L 36 # 38  
 Thrasher, Jerry Lexmark

Comment Type E Comment Status X

Reword the sentence.

SuggestedRemedy

While there may be no way of eliminating the effect of these attacks, there are some technical measures that can.....

Proposed Response Response Status O

Cl Main SC 9.9.1.3 P 143 L 31 # 39  
 Thrasher, Jerry Lexmark

Comment Type E Comment Status X

This recommendation doesn't provide any real guidance..

SuggestedRemedy

Reword to:  
 Based on a security assessment for the particular environment, the IT professional should select HCDs that can provide appropriate levels of availability and system integrity, then follow the manufacturer's guidance for configuring and deploying the devices.

Proposed Response Response Status O

Cl Main SC 10.1 P 144 L 3 # 40  
 Thrasher, Jerry Lexmark

Comment Type E Comment Status X

there's an extra space between the word (product) and (is) in the sentence.

SuggestedRemedy

remove the space.

Proposed Response Response Status O

Cl main SC 10 P144 L # 44  
 Chen, Nancy Oki Data

Comment Type G Comment Status X

Example in each conformance sub-clause should provide a complete set of mitigation techniques required as an example æbest practiceÆ for conforming to the stated requirements.

SuggestedRemedy

For each conformance statement, provide a complete set of mitigation techniques like what is done in 10.1.1.10.

Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security Comments

Cl Main SC 10.1.1.7 P146 L 8 # 51  
 Sukert, Alan Xerox

Comment Type E Comment Status X  
 Another minor grammatical error - should be 'usage related events' and not 'usage related event'.

SuggestedRemedy  
 See comment above

Proposed Response Response Status O

Cl Main SC 10.1.1.10 P146 L 27 # 52  
 Sukert, Alan Xerox

Comment Type E Comment Status X  
 To be consistent with the acronym for denial of service defined in clause 3.1.32, the title of clauses 10.1.1.10, 10.1.2.10, 10.1.3.8 & 10.1.4.6 should be "Mitigation of DoS attack".

SuggestedRemedy  
 See comment above.

Proposed Response Response Status O

Cl Main SC 10.1.1.10 P146 L 37 # 53  
 Sukert, Alan Xerox

Comment Type T Comment Status X  
 In the new text that has been added for the various "Mitigation of DOS attack" subclauses in Clause 10, the last item is "Providing the capability to enable only protocols that require authentication before jobs can be sent to the HCD" from clause 8.1.9.3. I don't see how enabling only authenticated protocols will help mitigate a DoS attack. The first two items listed are sufficient as examples of techniques that can help meet the DoS mitigation requirements.

SuggestedRemedy  
 In clauses 10.1.1.10, 10.1.2.10, 10.1.3.8 & 10.1.4.6:  
 -- eliminate the reference to clause 8.1.9.3 in the "For example..." sentence  
 -- eliminate the third example dealing with enabling authenticated protocols

Proposed Response Response Status O

Cl Main SC 10.2 P153 L 31 # 58  
 aubry, carmen oce

Comment Type T Comment Status X  
 When describing general practices for systems in environment A (http://grouper.ieee.org/groups/2600/drafts/FullSpec/IEEE\_P2600\_v29a.pdf, page 31, line 6) we have

\*Security-related operating system and application patches and updates are tested and applied as soon as possible Recommended Mitigation Techniques for IT Professionals (http://grouper.ieee.org/groups/2600/drafts/FullSpec/IEEE\_P2600\_v29a.pdf,) in preventing the DOS attacks:  
 \* Ensuring that all networked devices have the latest security updates applied, and effective anti virus software installed and operational

The compliance clause, Security Objectives for IT Professionals in Environment A doesn't mention anything similar.  
 The same remarks apply to environment B.

SuggestedRemedy  
 As long as DOS attacks are considered in the Compliance clauses, we should include something about it.

Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security Comments

Cl Main SC 10.2.1.7 P154 L 8 # 54  
 Sukert, Alan Xerox

Comment Type T Comment Status X

Need to remove the TBDs in this clause. I believe this clause deals with the requirement that a user has to be authorized before being allowed to access specific HCD features or functions. A good example of this is that many customers want to have the ability in a color HCD to permit only specific users to be able to access color copy functions as a way to save costs. Another more general example of User Authorization would be a centralized authentication model where users can be given access to all or only specific HCD features, so when an authorized user is initially authenticated the user can only access those HCD features for which the administrator has granted the user access to.

SuggestedRemedy

Clauses 10.2.1.7 and 10.2.3.3 should be modified to read as follows:

Users shall be authorized prior to be granted permission to use the HCD.

For example, one possible technique may be found in 8.3.10.4:

Ensuring that only authorized users have access to only those HCD functions for which access has been granted by a security administrator.

Note - this would have to be added as clause 8.4.3.4, item c on page 103.

Proposed Response Response Status O

Cl Main SC 10.2.2 P154 L 39 # 55  
 Sukert, Alan Xerox

Comment Type T Comment Status X

A subclause for 'User Authorization' under Compliance Security Objectives for IT Professionals was included for Operational Environment A as clause 10.2.1.7 and in Operational Environment C as clause 10.2.3.3. It is not clear why this same clause was not included in clause 10.2.2 for Operational Environment B because Environment B will have the same general need for managing user authorization to access the HCD as in Environment A.

SuggestedRemedy

Add a clause 10.2.2.7 User Authorization with the same content as in clause 10.2.1.7.

Proposed Response Response Status O

Cl main SC 8 P71 L # 43  
 Chen, Nancy Oki Data

Comment Type G Comment Status X

It's not clear whether one or more, or all of the mitigation techniques listed for countering each threat are recommended by the main document. Some listed alternative techniques, thus requiring all will not make sense. However, "Best Practice" may require one of the techniques to accompany all the rest of alternatives. P2600 should have a clear "Best Practice" recommendation for mitigating each threat.

SuggestedRemedy

Clarify how the list of techniques should be used.

Proposed Response Response Status O

Cl Main SC 3.1.42 & 4.2.2.4 P8 & 18 L719 # 45  
 Chen, Nancy Oki Data

Comment Type T Comment Status X

æLEDÆ printer should be added as a kind of printer.

SuggestedRemedy

Add LED printer to the list.

Proposed Response Response Status O

Cl Main SC 8 P91 L # 46  
 Chen, Nancy Oki Data

Comment Type T Comment Status X

2. The sentence : "If the normal interfaces on the HCD allow an attacker to easily access the User Document Data assets on the HCD, any level of data protection applied to the User Document Data assets via encryption or other means is useless." Used in many sections in Clause 8 does not make sense.  
 o The fact is if the attacker have easy access to User Document Data storage area but does not have access to encryption key data at all, then with the use of an effective encryption algorithm, the User Document Data is very well protected from disclosure.

SuggestedRemedy

Delete or Reword the sentence appropriately to avoid giving users a distorted view of encryption technology.

Proposed Response Response Status O