

IEEE P2600 Hardcopy Device and System Security comments

Cl 00 SC 1 P 5 L 18 # 22
 Smithson, Brian Ricoh
 Comment Type E Comment Status D
 needs some kind of temporal reference
 SuggestedRemedy
 "when this document was published" or something like that
 Proposed Response Response Status W
 PROPOSED ACCEPT.

Cl 00 SC 1.3 P 6 L 16 # 23
 Smithson, Brian Ricoh
 Comment Type E Comment Status D
 grammatical error, and restructure to make it a bit more clear
 SuggestedRemedy
 "Unless noted otherwise, especially in Clauses 5-8, all text of this Guide applies to all four Protection Profiles..."
 Proposed Response Response Status W
 PROPOSED ACCEPT IN PRINCIPLE.
 See also comment #3

Cl 00 SC 2.2 P 8 L 34 # 20
 Smithson, Brian Ricoh
 Comment Type E Comment Status D
 word order of change would more clear help make the sentence
 SuggestedRemedy
 "For example, in specifying the FIA_UID SFR, IEEE Std. 2600.1 does not..."
 Proposed Response Response Status W
 PROPOSED ACCEPT.

Cl 00 SC 4.2.2.2 P 18 L 1 # 24
 Smithson, Brian Ricoh
 Comment Type E Comment Status D
 I am not certain that ours is a "unique way".
 SuggestedRemedy
 Remove first two sentences, and just start the next with "As indicated in Clause 5.2 in any PP..., by default, Users are not distinguished from Subjects."
 Proposed Response Response Status W
 PROPOSED ACCEPT.

Cl 00 SC 4.2.2.3 P 18 L 31 # 44
 Smithson, Brian Ricoh
 Comment Type T Comment Status D
 Specialized User roles should be categorized under either U.Normal or U.Administrator (or in some weird case, I suppose, U.USER), so that the ST maintains demonstrable conformance to the PP.
 SuggestedRemedy
 Add to the end of the paragraph "If specialized roles are defined in an ST, they should be defined as specializations of one of the defined kinds of users."
 Proposed Response Response Status W
 PROPOSED ACCEPT IN PRINCIPLE.

Will add suggested wording plus the idea of listing the actual roles mentioned in the comment to the end of the sentence.

Cl 00 SC 4.2.2.6 P 19 L 42 # 25
 Smithson, Brian Ricoh
 Comment Type E Comment Status D
 Bluetooth is a registered trademark of somebody.
 SuggestedRemedy
 Add the trademark symbol, and a footnote, and yet another informative reference?
 Proposed Response Response Status W
 PROPOSED ACCEPT.

IEEE P2600 Hardcopy Device and System Security comments

Cl 00 SC 4.2.5.2 P 23 L 16 # 21
 Smithson, Brian Ricoh

Comment Type E Comment Status D
 a nit: these aren't really examples, these are the two cases in which this situation occurs in the PPs

SuggestedRemedy
 change to "The two cases in which this situation..."

Proposed Response Response Status W
 PROPOSED ACCEPT.

Cl 00 SC 4.2.5.3 P 23 L 41 # 26
 Smithson, Brian Ricoh

Comment Type E Comment Status D
 it might be worth noting that other security objectives for printers are covered by the common PP in C and D

SuggestedRemedy
 Append to paragraph something like "For environments C and D, security objectives for printers are adequately covered by the common PP."

Proposed Response Response Status W
 PROPOSED ACCEPT IN PRINCIPLE.

Will add something similar to the suggested wording; not exactly clear where this new text is to be added in 4.2.5.3.

Cl 00 SC 5.2 P 25 L 39 # 27
 Smithson, Brian Ricoh

Comment Type E Comment Status D
 is PPM relevant? or does it illustrate that size doesn't matter?

SuggestedRemedy
 consider removing PPMs on this page/line and elsewhere in 5.2, or make the point that the intended use of the device determines the appropriate environment (and therefore the security features that are required to support that environment), not the size/speed/complexity of the device

Proposed Response Response Status W
 PROPOSED ACCEPT IN PRINCIPLE.

Add a footnote here that reminds the reader that the intended use of the device determines the appropriate environment (and therefore the security features that are required to support that environment), not the size/speed/complexity of the device.

Cl 00 SC 5.2 P 26 L 2 # 46
 Smithson, Brian Ricoh

Comment Type T Comment Status D
 doctor's daily schedule might contain HIPAA-covered data (patient names and type of appointment/treatment). Could we find a more benign example?

SuggestedRemedy
 change to something else, maybe like "the printer is being used to print blank forms or other office information"

Proposed Response Response Status W
 PROPOSED ACCEPT IN PRINCIPLE.

Perhaps printing blank patient information forms for completion by the patient.

Cl 00 SC 5.2 P 26 L 5 # 45
 Smithson, Brian Ricoh

Comment Type T Comment Status D
 rationale is a little off: OpEnv D provides some protection for networks, but provides no protection for document data!

SuggestedRemedy
 change rationale to something like "because the TOE does not need to protect document data, it only needs to be secured against network-based attacks that could be used to compromise other systems in the doctor's office".

Proposed Response Response Status W
 PROPOSED ACCEPT.

Cl 00 SC 5.3 P 28 L 21 # 29
 Smithson, Brian Ricoh

Comment Type E Comment Status D
 why is Hotel Business Center capitalized? others (doctor's office, auto repair shop, ...) are not

SuggestedRemedy
 change to lower case, many places in 5.3

Proposed Response Response Status W
 PROPOSED ACCEPT.

IEEE P2600 Hardcopy Device and System Security comments

Cl 00 SC 5.3 P 30 L 26 # 47
 Smithson, Brian Ricoh
 Comment Type T Comment Status D
 removing a disk to obtain customer data is not such a good example because OpEnv C does not promise protection of user data (except residual) and there is no NVS package
 SuggestedRemedy
 change rationale to something else, maybe like: "so that unauthorized persons are prevented from misusing the HCD"
 Proposed Response Response Status W
 PROPOSED ACCEPT.

Cl 00 SC 5.3 P 31 L 4 # 48
 Smithson, Brian Ricoh
 Comment Type T Comment Status D
 what? I think you can add OSPs and Security Objectives to an ST
 SuggestedRemedy
 where did this information come from? let's discuss...
 Proposed Response Response Status W
 PROPOSED ACCEPT IN PRINCIPLE.
 Additional OSPs can be added. It is not OK to add assumptions or remove OSPs.

Cl 00 SC 5.3 P 31 L 19 # 28
 Smithson, Brian Ricoh
 Comment Type E Comment Status D
 it isn't an "Operational Environment X company" or "this type of business", it's an intended use of the HCD...
 SuggestedRemedy
 line 19: change to "It makes sense, then, that for this kind of use..."
 line 20: change to "consistent with the OSPs in Operational Environment C"
 line 23: change to "consider Operational Environment B in a large company"
 Proposed Response Response Status W
 PROPOSED ACCEPT.

Cl 00 SC 5.3 P 33 L 5 # 30
 Smithson, Brian Ricoh
 Comment Type E Comment Status D
 auto repair shop could have several environments, let's be more specific
 SuggestedRemedy
 change to "Consider the difference between the front office of an auto repair shop versus the hotel business center used above"
 Proposed Response Response Status W
 PROPOSED ACCEPT.

Cl 00 SC 5.3 P 33 L 18 # 49
 Smithson, Brian Ricoh
 Comment Type T Comment Status D
 Several things are incorrect about this paragraph:
 User I&A is not required in OpEnv C
 There is no promise of user data security in OpEnv C
 There *are* some audit requirements in OpEnv C and FAU_GEN is present (the difference is in the required/recommended auditable events)
 Other than that, it's perfect :-).
 SuggestedRemedy
 redo the paragraph to show that user I&A is not required because we don't care who did what on the machine, audit requirements are less stringent because they are intended to log security violations and not to provide individual accountability
 Proposed Response Response Status W
 PROPOSED ACCEPT.

IEEE P2600 Hardcopy Device and System Security comments

Cl 00 SC 5.4.1 P 33 L 36 # 50
 Smithson, Brian Ricoh

Comment Type T Comment Status D

it would be more clear to describe the default case first (external audit storage), then internal, then both

SuggestedRemedy

Start with paragraph of line 42 first (but it is not by "inference", it is by OE that storage/access is provided by the environment)

Follow with the paragraph of line 36 and its bullets (but complete or correct the sentence on line 36-37)

Describe (or provide pointer to later in document) replacement objectives (O. for OE.) and additional SFRs.

Follow with paragraph of line 48. Describe (or provide pointer to later in document) how additional objectives and SFRs are needed, and that evaluation is performed as separate modes of operation.

Proposed Response Response Status W

PROPOSED ACCEPT.

Will re-order

Cl 00 SC 5.4.2 P 34 L 6 # 31
 Smithson, Brian Ricoh

Comment Type E Comment Status D

heading text seems inconsistent with 5.4.1

SuggestedRemedy

change to something like "Identification and Authentication inside or outside of the TOE"

Proposed Response Response Status W

PROPOSED ACCEPT.

Cl 00 SC 5.4.2 P 34 L 26 # 51
 Smithson, Brian Ricoh

Comment Type T Comment Status D

similar to comment about 5.4.1, three cases should be described: outside (default), inside, or outside and inside

SuggestedRemedy

see remedy for 5.4.1: if you talk about adding SFRs, you should also talk about adding or replacing objectives; otherwise, point to later in the document where this is covered

Proposed Response Response Status W

PROPOSED ACCEPT.

Will re-order and point to the later clause for more information.

Cl 00 SC 6.2.1 P 37 L 1 # 52
 Smithson, Brian Ricoh

Comment Type T Comment Status D

what? how can an SFR be performed by the IT environment or by another trusted IT system or product? the TSF performs whatever the SFR says.

SuggestedRemedy

Let's discuss lines 1-29 on this page...

Proposed Response Response Status W

PROPOSED ACCEPT IN PRINCIPLE.

Commenter and editor will reword to talk about fulfilling objectives not fulfilling SFRs.

Cl 00 SC 6.2.1 P 37 L 3 # 32
 Smithson, Brian Ricoh

Comment Type E Comment Status D

number list should restart

SuggestedRemedy

restart numbering on this list

Proposed Response Response Status W

PROPOSED ACCEPT.

IEEE P2600 Hardcopy Device and System Security comments

Cl 00 SC 6.2.1.1 P 37 L 42 # 33
 Smithson, Brian Ricoh
 Comment Type E Comment Status D
 I don't think an actual example is provided in 6.8.2 item 5a
 SuggestedRemedy
 change something like from "an example" to "further discussion"
 Proposed Response Response Status W
 PROPOSED ACCEPT.

Cl 00 SC 6.2.1.2 P 38 L 1 # 34
 Smithson, Brian Ricoh
 Comment Type E Comment Status D
 it is not so much whether an ST can claim NVS, it is whether it must claim NVS
 SuggestedRemedy
 change the intro sentence accordingly; also note in list item #1 that the ST author can claim NVS if they want to
 Proposed Response Response Status W
 PROPOSED ACCEPT.

Cl 00 SC 6.2.1.2 P 38 L 27 # 35
 Smithson, Brian Ricoh
 Comment Type E Comment Status D
 shouldn't we mention the case where NVS conformance is required, but cannot be claimed?
 SuggestedRemedy
 add another case: if the C&I is provided by a third party product but that product is not CC certified, and sufficient evidence is not available to certify it, then NVS conformance cannot be claimed
 Proposed Response Response Status W
 PROPOSED ACCEPT IN PRINCIPLE.
 Editor will work with commenter on the text.

Cl 00 SC 6.3 P 40 L 30 # 36
 Smithson, Brian Ricoh
 Comment Type E Comment Status D
 it is confusing to say that something has to be confidential because it shouldn't be modified
 SuggestedRemedy
 better to say "a user's password clearly has to be treated as protected information so that it cannot be modified by anyone other than the user or an administrator, because the user in question wouldn't then be able to authenticate himself or herself to access his or her files. However, a user's password must also be treated as confidential information so that it is not disclosed to anyone, because disclosure would make it possible for potential attackers to authenticate..."
 Proposed Response Response Status W
 PROPOSED ACCEPT.

Cl 00 SC 6.3 P 40 L 38 # 37
 Smithson, Brian Ricoh
 Comment Type E Comment Status D
 I'm not sure that "most users feel that usernames ... are personal information that should not be disclosed", and there are cases where usernames must be disclosed
 SuggestedRemedy
 change line 38 to "...guessing a user's password, but there are situations in which usernames are necessarily public information, such as to identify the owner of a print job or to grant shared access to a stored document." (or something like that...
 Proposed Response Response Status W
 PROPOSED ACCEPT.

Cl 00 SC 6.4 P 43 L 22 # 38
 Smithson, Brian Ricoh
 Comment Type E Comment Status D
 it might be worth noting that logging "TOE use" is often desirable in OpEnv B and OpEnv C, but such logging is for accounting purposes and not for security, therefore such requirements are not included in those PPs
 SuggestedRemedy
 find a nice way of saying that...
 Proposed Response Response Status W
 PROPOSED ACCEPT IN PRINCIPLE.
 Editor will work with commenter to find the right text.

IEEE P2600 Hardcopy Device and System Security comments

Cl 00 SC 6.5.1 P 44 L 25 # 53
 Smithson, Brian Ricoh
 Comment Type T Comment Status D
 the ST needs to choose, not define, one of the four audit detail levels
 SuggestedRemedy
 change "should define" to "needs to choose"
 Proposed Response Response Status W
 PROPOSED ACCEPT.
 "needs to select"

Cl 00 SC 6.5.1 P 44 L 30 # 39
 Smithson, Brian Ricoh
 Comment Type E Comment Status D
 this is a potentially very confusing area of the PP (my fault), and I think we should describe the audit requirements/recommendations tables column by column
 also note that use of the word "minimum" (to refer to what is minimally required by the PP) could be confused with "minimum" (referring to the CC defined level of audit detail)
 SuggestedRemedy
 let's walk through this during the meeting
 Proposed Response Response Status W
 PROPOSED ACCEPT IN PRINCIPLE.
 Editor and commenter will develop the specific wording to address this.

Cl 00 SC 6.5.1.1 P 46 L 10 # 54
 Smithson, Brian Ricoh
 Comment Type T Comment Status D
 it is not an audit requirement for the ECD, it is a recommendation
 SuggestedRemedy
 change to "recommends recording the event 'failure condition...functionality' for a Basic level of audit detail, and does not recommend any management functions."
 Proposed Response Response Status W
 PROPOSED ACCEPT.

Cl 00 SC 6.5.1.1 P 46 L 14 # 40
 Smithson, Brian Ricoh
 Comment Type E Comment Status D
 I don't know if we need to include such detail about this. It is unlikely that an ST will voluntarily add this audit event, and even if an ST does add this event, I am not sure that the SFR needs to be included in the NVS package or if the event can simply be added to the FAU_GEN SFR in the common section. Honestly, I don't know whether an ST divide up sections or roll the conforming sections together, there are benefits to doing it either way.
 In any case, they wouldn't add a table 7 and table 8, they'd actually specify the event in the FAU_GEN SFR (either in the common section or the NVS section)

SuggestedRemedy
 just mention that if the ST author wants to add this, OR IF THEY SPECIFY BASIC in the common section, then they'll want to add this event somewhere
 Proposed Response Response Status W
 PROPOSED ACCEPT IN PRINCIPLE.
 Editor and commenter will develop this text.

Cl 00 SC 6.5.2 P 48 L 11 # 43
 Smithson, Brian Ricoh
 Comment Type E Comment Status D
 general issue with access control rules: they are specified in the PP as what is denied, not what is allowed. for example, PRT doesn't require that a normal user is allowed to read their own documents (although it would be silly to deny that access). what PRT does is that it denies read access to all normal users other than the owner.
 SuggestedRemedy
 kind of a big change, but can you change the sense of the access control discussion from P48 L11 through P49 L9 from "allow" to "deny"?
 Proposed Response Response Status W
 PROPOSED ACCEPT IN PRINCIPLE.
 Editor and commenter will develop this text.

IEEE P2600 Hardcopy Device and System Security comments

Cl 00 SC 6.5.2 P 48 L 11 # 42
 Smithson, Brian Ricoh
 Comment Type E Comment Status D
 restart numbering
 SuggestedRemedy
 restart numbering
 Proposed Response Response Status W
 PROPOSED ACCEPT.

Cl 00 SC 6.5.2 P 49 L 2 # 41
 Smithson, Brian Ricoh
 Comment Type E Comment Status D
 typo
 SuggestedRemedy
 change "bare" to "are"
 Proposed Response Response Status W
 PROPOSED ACCEPT.

Cl 00 SC 6.5.2 P 49 L 3 # 55
 Smithson, Brian Ricoh
 Comment Type T Comment Status D
 this is not correct, we didn't relax a rule to allow the TOE to process documents (it always has that permission), we relaxed the rule to allow the owner of a document to grant permission to others to read their document while still retaining that ownership
 SuggestedRemedy
 change accordingly
 Proposed Response Response Status W
 PROPOSED ACCEPT.

Cl Globa SC 1 P 1 L 1 # 9
 Thrasher, Jerry Lexmark International I
 Comment Type T Comment Status D
 The Guide is missing a discussion of an error in IEEE 2600.1-2009.
 The error is:
 Page 19, Table 15: The auditable event listed for FTA_SSL.3 is ""Locking of an interactive session by the session locking mechanism"".á FTA_SSL.3 is for TSF-initiated termination of a session rather than session locking (that would be addressed by FTA_SSL.1 or FTA_SSL.2, which aren't included in the PP).á It appears that the auditable event specified for FTA_SSL.3 should be ""Termination of an interactive session by the session locking mechanism"" instead

It looks like this is simply an error in the table text...the rest of the profile is pretty clear that the session termination is the important event.
 SuggestedRemedy
 Add a discussion about the error.
 Proposed Response Response Status W
 PROPOSED ACCEPT IN PRINCIPLE.
 Add this to the ERRATA section of the GUIDE.

Cl Globa SC 1 P 1 L 1 # 7
 Thrasher, Jerry Lexmark International I
 Comment Type E Comment Status D
 There are many instances in the latter half of the document that have highlighted (yellow) references to external documents or cross-references within the document that need to be cleaned up...see 6.9.8 page 75 line 15 as an example.
 SuggestedRemedy
 Proposed Response Response Status W
 PROPOSED ACCEPT.

IEEE P2600 Hardcopy Device and System Security comments

Cl **Guide** SC 4.2.1.2 P 15 L 44 # 12
 Canon, Inc. Canon

Comment Type T Comment Status D
 Since PP includes SFR packages, description like ""PP or packages"" contradicts.

SuggestedRemedy
 Rephrase "PP or in the SFR packages" to "common PP or packages" or just "PP".

Proposed Response Response Status W
 PROPOSED ACCEPT IN PRINCIPLE.

Use "in the Common PP or in one or more of the SFR packages"

Cl **Guide** SC 5.3 P 29 L 19 # 13
 Canon, Inc. Canon

Comment Type T Comment Status D
 Description is generic to CC (not 2600 specific at all). Guide should focus on 2600 specific topics. (Also, saying maintaining log here would be confusing because external IT may maintain.)

SuggestedRemedy
 Delete lines 19-25 on page 29

Proposed Response Response Status W
 PROPOSED ACCEPT IN PRINCIPLE.

Information that might be considered by some to be CC generic is often useful in understanding the intent of those creating, evaluating, and validating the PPs. The group decided to leave this information in the GUIDE for clarity especially for some readers who may not be CC experts. Remember, the GUIDE is simply an informational document and is not required for compliance.

Add some text that reminds the reader that the audit log may be stored externally although the events are actually written there by the TOE.

Cl **Guide** SC 5.3 P 31 L 3 # 14
 Canon, Inc. Canon

Comment Type T Comment Status D
 Description is generic to CC (not 2600 specific at all). Guide should focus on 2600 specific topics. (Also, we don't understand why OSP cannot be added.)

SuggestedRemedy
 Delete lines 3-6 on page 31

Proposed Response Response Status W
 PROPOSED ACCEPT IN PRINCIPLE.

Re: OSPs -- See response to #48

Information that might be considered by some to be CC generic is often useful in understanding the intent of those creating, evaluating, and validating the PPs. The group decided to leave this information in the GUIDE for clarity especially for some readers who may not be CC experts. Remember, the GUIDE is simply an informational document and is not required for compliance.

Cl **Guide** SC 6.1 P 35 L 34 # 15
 Canon, Inc. Canon

Comment Type T Comment Status D
 Since required components (and SFRs) already include applicable features in the HCD, describing as if additionally requiring something would be misleading.

SuggestedRemedy
 Delete lines 34-36.

Proposed Response Response Status W
 PROPOSED ACCEPT IN PRINCIPLE.

This text was added in response to comments previously submitted by JBMIA.

Line 34: change "must also include" to "also includes"

(Line 31: change "enter HCD" to "entire HCD")

IEEE P2600 Hardcopy Device and System Security comments

Cl **Guide** SC **6.1** P **35** L **39** # **16**
 Canon, Inc. Canon

Comment Type **T** Comment Status **D**

Since PP includes SFR packages, description like "PP or packages" contradicts.

SuggestedRemedy

Rephrase "Protection Profiles, Packages" to "common PP or packages" or just "PP".

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

See #12

Cl **Guide** SC **6.1** P **36** L **2** # **10**
 Canon, Inc. Canon

Comment Type **E** Comment Status **D**

Since PP includes SFR packages, description like "PP or packages" contradicts.

SuggestedRemedy

Rephrase "Protection Profiles and those packages" to "common PP or packages" or just "PP".

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

See #12

Cl **Guide** SC **6.1** P **36** L **3** # **11**
 Canon, Inc. Canon

Comment Type **E** Comment Status **D**

Since PP includes SFR packages, description like "PP or packages" contradicts.

SuggestedRemedy

Rephrase "Protection Profiles and the packages" to "common PP or packages" or just "PP".

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

See #12

Cl **Guide** SC **6.5.6** P **51** L **9** # **17**
 Canon, Inc. Canon

Comment Type **T** Comment Status **D**

Since degauss makes HDD unusable (See NIST SP800-88 Appendix B), the example of using degauss won't be realistic at all. HDD malfunction caused by degauss is not limited to full encryption disk but applicable to disk used with integrity check, thus explanation is inadequate.

Since this topic is needed to recover WG's agreement on [detect or prevent] which was accidentally lost by editorial mistake, it should focus only on essentials.

SuggestedRemedy

Modify lines 9-19 FROM:

"In this case the ST Author should be able to argue that such fully encrypted disks should meet the requirements of FPT_CIP_EXP.1.2 because they do detect gross modification such as degaussing of the disk and, more importantly, they exceed the "detection" requirement by preventing modification depending on the surrounding implementation. For example, if the implementation "detects" that the disk is degaussed it might interpret that condition as being a new disk or a new HCD and assign the default administrator password; in that case the requirements of FPT_CIP_EXP.1.2 would not be met.

The one important caveat is that for the above arguments to hold the TOE must ensure that only such fully encrypted disk drives are used in the TOE. This means that the TOE must provide a function that either detects or, better, prevents unauthorized modifications to the data stored on the fully encrypted hard drives;"

TO:

"In this case the ST Author should be able to argue that such fully encrypted disks should meet the requirements of FPT_CIP_EXP.1.2 because they exceed the "detection" requirement by preventing modification.

The one important caveat is that the TOE must provide a function that either detects or, better, prevents unauthorized modifications to the data stored on the fully encrypted hard drives;"

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

Modify to paragraphs to include both the Canon suggested text and also include the information from Helmut.

IEEE P2600 Hardcopy Device and System Security comments

Cl **Guide** SC **6.7.3** P **57** L **1** # **18**
 Canon, Inc. Canon

Comment Type **T** Comment Status **D**

Some of the PP Guide is not consistent with generic CC information. It will cause to misleading. The Guide should focus on 2600-specific topics. It would be better to leave out the description of generic CC information and refer to the original CC.

SuggestedRemedy

Both clauses 6.7.3 and 6.7.4 should be removed from the Guide because the clauses contain text that is not consistent with generic CC information.
 For example, in 6.7.3 ST Security Problem Definition, item 1. Threat Agents, the phrase pertaining to "or weaker" is wrong. However, the issue is not to change this small point , but to remove the clause entirely.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

Fix the errors:

In 6.7.3 1) swap "weaker" and "stronger"
 In 6.7.3 3) swap "less restrictive" and "more restrictive"

(Make sure 6.7.4 is OK.)

The bottom line is that the TOE can always do more than is required by the PP.

Information that might be considered by some to be CC generic is often useful in understanding the intent of those creating, evaluating, and validating the PPs. The group decided to leave this information in the GUIDE for clarity especially for some readers who may not be CC experts. Remember, the GUIDE is simply an informational document and is not required for compliance.

Cl **Guide** SC **6.7.4** P **57** L **30** # **19**
 Canon, Inc. Canon

Comment Type **T** Comment Status **D**

Some of the PP Guide is not consistent with generic CC information. It will cause to misleading. The Guide should focus on 2600-specific topics. It would be better to leave out the description of generic CC information and refer to the original CC.

SuggestedRemedy

Both clauses 6.7.3 and 6.7.4 should be removed from the Guide because the clauses contain text that is not consistent with generic CC information.
 For example, in 6.7.3 ST Security Problem Definition, item 1. Threat Agents, the phrase pertaining to "or weaker" is wrong. However, the issue is not to change this small point, but to remove the clause entirely.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

See #18

Cl **Main** SC **1.3** P **6** L **18** # **3**
 Thrasher, Jerry Lexmark International I

Comment Type **E** Comment Status **D**

The sentence beginning "Within this Guide" needs rewriting (too many commas/semicolons/breaks)

SuggestedRemedy

Within this Guide, all text (especially in Clauses 5-8) covers all four Protection Profiles that comprise the IEEE 2600 Series of Protection Profiles unless specifically noted otherwise.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

See also #23

Cl **Main** SC **4.2.2.6** P **19** L **1** # **4**
 Thrasher, Jerry Lexmark International I

Comment Type **E** Comment Status **D**

No need to end this sentence with "is".....also Wi-Fi ALWAYS has a dash.

SuggestedRemedy

...same way as a Wi-Fi connection.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

IEEE P2600 Hardcopy Device and System Security comments

Cl Main SC 5.3 P 27 L 26 # 5
Thrasher, Jerry Lexmark International I
Comment Type E **Comment Status D**
remove the phrase "how to use" at the end of the sentence.
SuggestedRemedy
....can learn very quickly on their own.
Proposed Response **Response Status W**
PROPOSED ACCEPT.

Cl Main SC 6.2.1.1 P 36 L 34 # 6
Thrasher, Jerry Lexmark International I
Comment Type E **Comment Status D**
TBD probably should be IEEE 2600.1 Clause 10.8
SuggestedRemedy

Proposed Response **Response Status W**
PROPOSED ACCEPT.

Cl Main SC 8.1 P 85 L 21 # 8
Thrasher, Jerry Lexmark International I
Comment Type E **Comment Status D**
The reference to Germany Scheme seems a little off.
SuggestedRemedy
either German Scheme or Scheme from Germany??
Proposed Response **Response Status W**
PROPOSED ACCEPT.

Fixed in 44b

Cl PP An SC 6.5.8 P 51 L 17 # 2
AUBRY, Carmen oce
Comment Type T **Comment Status D**
PP guide version 44b:
You are only focusing on the scan path in P2600.2. Our discussions in the group and with Helmut addressed both print and scan path.
SuggestedRemedy
Please change this paragraph in something more general like: Protection of User Credentials Leaving/Entering an SMI Interface on IEEE Std 2600.2 Compliant Products Remove the explicit example of scan credentials and say that:
1) Credentials are example of TSF data and a trusted path is required when transferring them
2) Kerberized print and scan services are a way to satisfy this requirement without encrypting the entire flow (without encrypting user data).
Continue with the remark from Helmut (included in my previous comment)
Proposed Response **Response Status W**
PROPOSED ACCEPT IN PRINCIPLE.

Editor will work with commenter to get the right words.

IEEE P2600 Hardcopy Device and System Security comments

Cl PP An SC 6.5.8 P 51 L 24 # 1
AUBRY, Carmen oce

Comment Type T Comment Status D

PP GUIDE VERSION 44B: Helmut told us that Kerberized Scan service will satisfy the trusted path requirement concerning TSF data. For PP-B this means that we have at least a solution that will not force us to encrypt user data. Please mention it in this paragraph because from this paragraph one may say that the only solution is encrypting USER DATA.

SuggestedRemedy

Please mention what Helmut said:

Be aware that there are more ways to implement such a trusted channel than SSL/TLS or IPsec. Even signed and encrypted e-mail sent over a network counts as a trusted channel, since it ensures the identification of the end points, as well as the integrity and the confidentiality of the data transmitted. Kerberos is another example of a protocol that can provide a trusted channel. Even a simple protocol that adds checksums to the data and then encrypts both the data and the checksums using symmetric encryption can be regarded as a trusted channel as long as the encryption keys used are different for the different communication partners the TOE is communicating with. In this case the key that is shared between the TOE and one single external entity serves both for confidentiality protection and authentication. How this shared key is securely brought into the TOE and the remote entity is up to the product. Even a manual key distribution process works, provided the product guidance explains how this can be done in a secure way.

Proposed Response Response Status W

PROPOSED ACCEPT IN PRINCIPLE.

Editor will work with commenter to get the right words.