

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP Gu** SC **0** P **1** L **1** # **7**  
 Smithson, Brian Ricoh

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

""Compliant with"" is not the usual phrase to use when referring to PPs.

*SuggestedRemedy*

Change to ""Conforming to"".

This change should be considered in many places.

Proposed Response Response Status **O**

Cl **PP Gu** SC **1.1** P **5** L **5** # **11**  
 Smithson, Brian Ricoh

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

(actually, this refers to footnote #2)

Nobody knows ""PP-A"", ""PP-B"", etc., except us!

*SuggestedRemedy*

Refer to the PPs as 2600.1, 2600.2, 2600.3, and 2600.4.

Proposed Response Response Status **O**

Cl **PP Gu** SC **0** P **1** L **2** # **9**  
 Smithson, Brian Ricoh

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

I found that it was cumbersome to keep referring to ""security targets or protection profiles conforming to this protection profile"", so in the PPs I just refer to ""security targets"" and included a note somewhere that the same things apply if someone wants to base a protection profile on this protection profile. Our main audience is (I assume) interested in writing STs, not PPs.

*SuggestedRemedy*

Do not refer to development of PPs in the title (and elsewhere), except for somewhere in the introductory material, like maybe in 1.2 Audience.

Proposed Response Response Status **O**

Cl **PP Gu** SC **2.1** P **8** L **10** # **12**  
 Smithson, Brian Ricoh

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

CCRA is ""Common Criteria Recognition Arrangement"", not ""...Agreement"".

*SuggestedRemedy*

Change Agreement to Arrangement, and check elsewhere in the document.

BTW if you want a link to the arrangement itself, it is here  
<http://www.commoncriteriaportal.org/files/operatingprocedures/cc-recarrange.pdf>

Proposed Response Response Status **O**

Cl **PP Gu** SC **0** P **1** L **3** # **8**  
 Smithson, Brian Ricoh

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

2600-2008 is not a protection profile, so the title is a little misleading and it is further confused by the footnote on page 5. But I am not sure what to put in the title, so I can only suggest some options...

*SuggestedRemedy*

- ""IEEE Std. 2600-series Protection Profiles""
- ""IEEE 2600-series Standards for Protection Profiles""
- ""IEEE Std. 2600.1-2009, 2600.2-2009, 2600.3-2009, and 2600.4-2009 Protection Profiles""
- ""IEEE Standard Protection Profiles for Hardcopy Devices""
- ""???""

Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP Gu** SC **2.2.1** P **9** L **30** # **13**  
 Smithson, Brian Ricoh

Comment Type **E** Comment Status **X**  
 What is described by the items in bullet (b) is the Security Problem Definition, not really the security environment. Items in (c) solve the problem. Items in (d) satisfy the objectives in (c).

SuggestedRemedy  
 In (b), change ""A definition of the intended description security environment including intended used assumptions..."" to ""A definition of the security problem to be addressed by the PP, in composed of...""

In (c), change ""rationale for each objective"" to ""rationale for how each objective solves that security problem"".

In (d), change ""address the document security objectives"" to ""satisfy those security objectives"".

Proposed Response Response Status **O**

Cl **PP Gu** SC **3.1** P **13** L **15** # **14**  
 Smithson, Brian Ricoh

Comment Type **E** Comment Status **X**  
 It is a bit US-centric. Also, the part about SOX seems incomplete.

SuggestedRemedy  
 Change to: IEEE Std 2600 was also necessitated by the enactment of a variety of laws and regulations related to information security and privacy. For example, in the United States, the (hipaa) requires healthcare ..., the Safeguards Rule in the (glba) calls on financial institutions..., and portions of {sox}... DOES WHAT?

Proposed Response Response Status **O**

Cl **PP Gu** SC **3.1.1** P **14** L **16** # **15**  
 Smithson, Brian Ricoh

Comment Type **E** Comment Status **X**  
 second-level bullet indents are strange

SuggestedRemedy  
 fix

Proposed Response Response Status **O**

Cl **PP Gu** SC **4.1** P **19** L # **10**  
 Smithson, Brian Ricoh

Comment Type **E** Comment Status **X**  
 Introduction says that this clause discusses why the PPs were created, but the clause does not say that.

SuggestedRemedy  
 The Guide should say why the PPs were created, need to add it to the clause.

Proposed Response Response Status **O**

Cl **PP-Gu** SC **5.2.1.1** P **34** L **29** # **2**  
 Chen, Nancy Oki Data

Comment Type **T** Comment Status **X**  
 In Table 6 (the security objective comparison table for 4 operational environments), the FDP\_ACC.1(b) for environment A and B is actually the same as the FDP\_ACC.1 for environment C, but they are listed as different SFRs. The same is true for the FDP\_ACF.1(b) in environment A and B and the FDP\_ACF.1 in environment C. The same is also true for FMT\_MSA.1(b) in env. A & B vs. FMT\_MSA.1 in env. C., and also true for FMT\_MSA.3(b) in env. A & B vs. FMT\_MSA.3 in env. C.

SuggestedRemedy  
 Change the subscript (a) to (for User Data), and (b) to (for TOE Functions). I.e. Name FDP\_ACC.1(a) as FDP\_ACC.1 (for User Data), FDP\_ACC.1(b) as FDP\_ACC.1 (for TOE Functions).

Make the same changes for FDP\_ACF.1(a), FDP\_ACF.1(b), FMT\_MSA.1(a), FMT\_MSA.1(b), FMT\_MSA.3(a), and FMT\_MSA.1(b).

Delete FDP\_ACC.1 and FDP\_ACF.1, FMT\_MSA.1, FMT\_MSA.3., and correct the comparison table to reflect the change accordingly.

Proposed Response Response Status **O**

Cl **PP-Gu** SC **5.2.2.1.7** P **56** L **10** # **3**  
 Chen, Nancy Oki Data

Comment Type **T** Comment Status **X**  
 In CC, audit levels are (minimum, basic, detailed), not (minimal, basic, detailed)

SuggestedRemedy  
 Change 'minimal' to 'minimum'.

Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-Gu** SC **5.2.2.7.1** P **57** L **7** # **4**

Chen, Nancy Oki Data

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

The Common Access Control SFP table needs update to be consistent with the latest PP version.

*SuggestedRemedy*

Update the Common Access Control SFP table to be consistent with the latest PP version.

Proposed Response Response Status **O**

Cl **PP-Gu** SC **5.2.2.7.1** P **58** L **38** # **5**

Chen, Nancy Oki Data

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

The violation example access control SFP table needs update to be consistent with the latest PP version.

*SuggestedRemedy*

Update the Common Access Control SFP table to be consistent with the latest PP version.

Proposed Response Response Status **O**

Cl **PP-Gu** SC **5.2.2.7.7** P **70** L **27** # **1**

Chen, Nancy Oki Data

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

There is no such key size as 156 bits for AES.

*SuggestedRemedy*

Change 156 to 256.

Proposed Response Response Status **O**

Cl **PP-Gu** SC **5.2.2.7.7** P **71** L **16** # **6**

Chen, Nancy Oki Data

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

I am confused by the guidance in this paragraph that tells ST authors could possibly use FDP\_ETC and FDP\_ITC to handle the actions taken in case the TOE detects an error when reading data from its previously removed NVS. FDP\_ETC and FDP\_ITC only takes care of User Data, not for TSF data. That is the reason that PPs uses the extended SFR FPT\_CIP\_EXP.1 for protecting confidentiality and integrity of both User Data and TSF Data on removable NVS.

*SuggestedRemedy*

Remove this paragraph or provide more appropriate guidance.

Proposed Response Response Status **O**