

IEEE P2600 Hardcopy Device and System Security comments

Cl All P SC P L # 50  
 Smithson, Brian Ricoh

Comment Type T Comment Status X

Identifying DoS threats is a problem, because it is often not possible to distinguish between a deliberate attack and a valid (although perhaps unusual) condition. If you can identify DoS attacks, mitigation is at best a problem and often an impossibility. Testing those mitigation techniques is not very meaningful (at least for EAL2 - EAL3).

SuggestedRemedy

Remove the T.DOS threats, O.RESILIENT, and any references to DoS attacks, from all PPs. Adjust the threat tables and analysis methodology annex in the main clauses.

Proposed Response Response Status O

Cl All P SC P L # 2  
 Ito, Takashi Konicaminolta Busines

Comment Type G Comment Status X

P2600 proposed PPs seem to intend to cover all of HCDs. IPA, Japanese 15408 certification authority, judges that "all of functions in PP have to be implemented into the target HCD" according to CC Part 1 definitions when you comply with PP. Based on the interpretation of the CC definitions, the HCDs that do not support Fax and/or HDD, which are often selected by customers because of price, cannot be covered by the present PPs. It means that the current PPs definitions can cover only very limited number of MFP or LP which support all of the functions in the PPs.

SuggestedRemedy

If P2600 wants to cover all of HCDs, will recommend to make separated PPs for each function modules such as for scanner, for copy, for print, for fax and so.

Proposed Response Response Status O

Cl All P SC P L # 49  
 Smithson, Brian Ricoh

Comment Type G Comment Status X

An updated version of NIAP's requirements (the CIMs) for CCv3.1 has not been published, and NIAP has given this update a "low priority" with no schedule for completion. Existing NIAP requirements for PPs and STs in Basic and Medium Robustness Environments are not internationally recognized by CCRA members. NIAP is not currently accepting new evaluation projects unless they are of interest to the NSA and target a Medium or High Robustness level. Therefore, even if we included NIAP requirements in our PPs, we would not be able to get the PPs successfully evaluated.

SuggestedRemedy

Do not fulfill CIM requirements in any PP. Remove references to NIAP robustness. Remove PP section 3.1 in its entirety. Remove PP Appendix D and any references to that appendix.

Proposed Response Response Status O

Cl All P SC 1.2.2, 1.2.3 P L # 55  
 Smithson, Brian Ricoh

Comment Type T Comment Status X

Firmware is not an asset? It is defined in "Miscellaneous" in 1.2.2, and under "Assets" in 1.2.3.

SuggestedRemedy

Define Firmware (and Applet) either as an Asset or as something else. I think that they are not assets, but in any case they should be defined consistently.

Proposed Response Response Status O

Cl All P SC 1.2.2, 1.2.3 P L # 54  
 Smithson, Brian Ricoh

Comment Type T Comment Status X

"Applet" is not defined in the terminology tables nor in the overview text.

SuggestedRemedy

Define it in Miscellaneous (table 4) and after Firmware in 1.2.3.

Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security comments

CI All P SC 1.2.3.3 P L # 6 [redacted]  
Ito, Takashi Konicaminolta Busines

Comment Type T Comment Status X

If toner and/or physical papers should be defined as assets to be protected, there should be some physical protection methods defined.  
However, PPs do not specify it.  
Besides, those methods will decrease the usability of the devices.

SuggestedRemedy

Will recommend to get rid of ""Resource"" from the assets to be protected.  
The secrecy of the services provided by HCDs should be defined as the assets (Fax receiving should be an exception).

Proposed Response Response Status O

CI All P SC 1.2.3.3 P L # 5 [redacted]  
Ito, Takashi Konicaminolta Busines

Comment Type T Comment Status X

User Document Data includes ""original documents"" and ""hard copies"".  
However, it is impossible to protect those physical materials with IT technology.

SuggestedRemedy

Protected Asset should be limited only User Document Data as digital data in HCD.

Proposed Response Response Status O

CI All P SC 3.1 P L # 3 [redacted]  
Ito, Takashi Konicaminolta Busines

Comment Type G Comment Status X

The idea ""Robustness"" in the PPs are US specific ones.  
The CCs as world wide standard do not have such definitions.  
If P2600 proceeds this PP with the idea, there is a possibility to have double standard between those PPs for US only and the CCs for others.

SuggestedRemedy

To meet the CCs' concept, will recommend to get rid of the ""Robustness"" itself from the PPs.  
If it would be very difficult, there is another recommendation which is to make clear and describe the correspondent EAL set conditions in CCs to each Robustness, in order to make sure that we can use CCs when we evaluate HCDs for the PPs in outside US such as Asia, EU and so.

Proposed Response Response Status O

CI All P SC 3.2.3 P L # 4 [redacted]  
Ito, Takashi Konicaminolta Busines

Comment Type T Comment Status X

The DoS attack is very difficult to protect even with OS and/or firewalls.  
Now, still HCD will have difficulty to distinguish the attacks from the proper services.  
Even PPs do not describe how to evaluate it.

SuggestedRemedy

Until we can have common understanding of the definition of DoS attack in HCD and its evaluation method, will recommend to get rid of this from the PPs.

Proposed Response Response Status O

CI All P SC 4.1 P L # 53 [redacted]  
Smithson, Brian Ricoh

Comment Type T Comment Status X

We have several objectives names in the PPs which have different definitions depending on the PP environment. For example, O.PROTECT includes user data, user function data, and management data in PP-A, user function and management data in PP-B, and only management data in PP-C.

SuggestedRemedy

Subdivide objectives as needed. I suggest that it would be better to divide them up as individual objectives (like O.PROTECT.UD, O.PROTECT.UFD, and O.PROTECT.MD) instead of using different groupings (like O.PROTECT.ALL, O.PROTECT.TSFD, and O.PROTECT.MD). By the way, I am not suggesting that we use names of this form; it may be better to make the naming structure consistent with the threat names.

Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security comments

Cl **All P** SC **4.1.6** P L # **7**  
 Ito, Takashi Konicaminolta Busines

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

In Japan, certification authority judges that audit log should cover all of issues related to SFRs described in PPs when you comply with PP.  
 However, to take all of logs, large storage devices such as HDD are required.  
 It will increase device cost a lot. Besides, users have to analyze all of the logs.  
 Those would be extra and huge burdens for users.

*SuggestedRemedy*

Will recommend to limit/minimize the numbers or kinds of audit logs due to price performance and/or usability for users.

Proposed Response Response Status **O**

Cl **All P** SC **sec. 3 and 4** P L # **52**  
 Smithson, Brian Ricoh

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

We have several threat names in the PPs which have different definitions depending on the PP environment. For example, T.TSF.CRED has a different meaning in each of the four environments. In PP-A, it includes NET, EM, MGMT, and GUESS. In PP-B, it includes NET, MGMT, and GUESS. In PP-C, NET and GUESS. In PP-D, only GUESS.

*SuggestedRemedy*

Unroll PP-categorized threats in the PPs and use the individual P2600 threat names instead. This will make the tables section 3.2 somewhat longer, but it will have the beneficial effect of allowing us to use the same short descriptions for each threat as we use in the main P2600 std. It will make Table 10 quite a bit longer, but it will become more clear because not all of the objectives assigned to the rolled-up threats will apply to all of the unrolled threats. Table 11 will get quite a bit longer also, but with the same beneficial effects that we would get from changing the tables in section 3.2 and from table 10.

Proposed Response Response Status **O**

Cl **All P** SC **section 1.2** P L # **51**  
 Smithson, Brian Ricoh

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

Some of the terminology used in the Asset/Actor/Access/Miscellaneous terminology tables in the PPs (especially PP-D) are not applicable to that environment. As examples, there's no Auditor role in PP-C, there's no Maintenance Port in PP-D, etc.

*SuggestedRemedy*

Review terminology in each environment and remove inapplicable terms from tables 1-4.

Proposed Response Response Status **O**

Cl **Globa** SC P L # **58**  
 Yami, Sameer Toshiba

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

""In D. PP conformance of CC v3.1 Part1, it is described that The ST shall contain all security objectives for the operational environment for PP conformance. It mean to have to oppose the threat that has been described to PP, even if HCD does not have the function to receive the threat. The threats of each functions (scanner,fax,printer etc...) are defined with PP. Only full functional HCD will be able to certify with PP conformance. The simple printer will not be able to certify with PP conformance. ""

*SuggestedRemedy*

""Only full functional HCD can use this PP, but HCD without FAX function and simple printer can not use this PP. If applying widely, the security objective might have to be divided (For example, PP is divided each function). ""

Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security comments

Cl **Globa** SC P L # 59  
 Yami, Sameer Toshiba  
 Comment Type **G** Comment Status **X**  
 ""Robustness only apply to North America.  
 If adding Robustness in PP , will not be able to CC certify in countries other than North America.  
 It contradicts the policy of IEEE as the world standard.""  
 SuggestedRemedy  
 To assume IEEE the world standard, Robustness must not be used. May be it can be used only in North America.  
 Proposed Response Response Status **O**

Cl **Globa** SC P L # 63  
 Yami, Sameer Toshiba  
 Comment Type **G** Comment Status **X**  
 ""It can be judged the environment appropriately managed by A.NETWORK and OE.NET\_MANAGE as a use environment of HCD.  
 Therefore, the threat """"Altering or deleting anotherEs User Document Data in transit by actively impersonating the destination (e.g. mail server) or the origin (e.g. print server), or by actively impersonating related service (e.g. domain name server)."""" may not occur.""  
 SuggestedRemedy  
 Review the description of A.NETWORK and OE.NET\_MANAGE, and not take up T.UD.IMP as Threat.  
 Proposed Response Response Status **O**

Cl **Globa** SC P L # 61  
 Yami, Sameer Toshiba  
 Comment Type **G** Comment Status **X**  
 ""Software/Firmware is just TOE.  
 It is necessary to correspond with Security Assurance Requirements (SAR) ADV\_ARC.1 to show that TOE is neither illegally falsified, TOE Security function (TSF) is not deactivated, TSF is not bypassed.  
 It is necessary to delete Software/Firmware (=TOE) from Asset because it is not possible to oppose it by the security function requirement (SFR).""  
 SuggestedRemedy  
 Review the description of A.NETWORK and OE.NET\_MANAGE, and not take up TOE Availability as Asset, DoS attack as Threat.  
 Proposed Response Response Status **O**

Cl **Main** SC P L # 60  
 Yami, Sameer Toshiba  
 Comment Type **G** Comment Status **X**  
 ""The judgement technique of Dos attack (threat of Avalability) or normal communication is difficult, and there is no complete technology to oppose DoS attack.  
 Therefore, it is not taken up as threat in the CC certification even like FireWall and IDS.  
 Moreover, O.RESILENT as security objective for T.DOS is assumed to be corresponding with Security Assurance Requirements (SAR) ATE\_FUN.1, it is violation of CC rule or manner. Security objective should correspond with Security Function Requirements (SFR).  
 ""  
 SuggestedRemedy  
 Review the description of A.NETWORK and OE.NET\_MANAGE, and not take up TOE Availability as Asset, DoS attack as Threat.  
 Proposed Response Response Status **O**

Cl **Globa** SC P L # 62  
 Yami, Sameer Toshiba  
 Comment Type **G** Comment Status **X**  
 External Environment should protect outside of TOE by Assumption and Operational environments (A.NETWORK and OE.NET\_MANAGE) because protecting with HCD is excessive.  
 SuggestedRemedy  
 Review the description of A.NETWORK and OE.NET\_MANAGE, and not take up External Environment as Asset.  
 Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security comments

**Cl Main** SC 3.1.94 P 10 L 33 # 34  
 Sukert, Alan Xerox  
 Comment Type E Comment Status X  
 Based on precedence used elsewhere in the standard, the reference to 'IEEE 802.11' should instead be to 'IEEE Std 802.11'.  
 Note this change would also have to be made as necessary in the other tables in Clause 8.  
 SuggestedRemedy  
 See above  
 Proposed Response Response Status O

**Cl Main** SC 4.1 P 16 L 15 # 57  
 Smithson, Brian Ricoh  
 Comment Type E Comment Status X  
 Some implementers have wondered if full MFP functionality is required for compliance. A more definite statement about that would help.  
 SuggestedRemedy  
 Add to last paragraph of 4.1:  
 ""However, this Standard can be applied to an HCD that is composed of any combination of those purposes and functions."  
 This is the minimal change. We may need more explanation. The PPs are another matter...  
 Proposed Response Response Status O

**Cl Main** SC 4.2.2.6 P 18 L 31 # 37  
 Sukert, Alan Xerox  
 Comment Type T Comment Status X  
 After reading through this section a couple of times, it is not clear to me that a general reader would understand what is meant by volatile storage and non-volatile storage. To make sure the discussion in the section is understandable, I would suggest adding these definitions to Clause 3.  
 SuggestedRemedy  
 Include definitions of volatile and non-volatile storage in Clause 3. Proposed definitions are:  
 volatile storage: Computer storage that is erased when the power is turned off.  
 non-volatile storage: Computer storage that is not lost when the power is turned off.  
 Proposed Response Response Status O

**Cl Main** SC 4.4.2 P 21 L 19 # 30  
 Sukert, Alan Xerox  
 Comment Type E Comment Status X  
 Based on the precedence used elsewhere in this section, I believe that the title of reference B101 (METI Policy on the Protection of Personal Information) should be italicized.  
 SuggestedRemedy  
 Italicize reference B101  
 Proposed Response Response Status O

**Cl Main** SC 5.1 P 23 L 14 # 31  
 Sukert, Alan Xerox  
 Comment Type E Comment Status X  
 Minor typo - 'ofoperational' should be split into two words.  
 SuggestedRemedy  
 See above  
 Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security comments

Cl Main SC 5.2.2 P 25 L 4 # 32  
 Sukert, Alan Xerox  
 Comment Type E Comment Status X  
 Based on how the phrase is written in Clause 8, I believe 'smartcard' on this line should be split into two words.  
 SuggestedRemedy  
 See above  
 Proposed Response Response Status O

Cl Main SC Clause 10 P 6 L 139 # 47  
 Sukert, Alan Xerox  
 Comment Type T Comment Status X  
 Should this be limited just to administrators (IÆm thinking here of certain user classes that might have special privileges for which a secure ID might provide them access).  
 SuggestedRemedy  
 See above  
 Proposed Response Response Status O

Cl Main SC 7.2, Table 3 P 41 L # 36  
 Sukert, Alan Xerox  
 Comment Type T Comment Status X  
 As a precursor to the possible inclusion of Production Sue software systems into the standard, in that environment protection is needed from not only rogue software applets, but from customer-created filters that allow them to write software to run on production systems. based on this, it is suggested that the definition of the T.TSF.SW.APPLET threat to include filters.  
 SuggestedRemedy  
 Redefine T.TSF.SW.APPLET threat to read ""Installing a rogue embedded software applet or filter on the HCD.""  
 Proposed Response Response Status O

Cl Main SC Clause 10 P 3 L 38 # 35  
 Sukert, Alan Xerox  
 Comment Type E Comment Status X  
 In keeping with convention used elsewhere in the standard protection profile should be capitalized.  
 SuggestedRemedy  
 Capitalize protection profile  
 Proposed Response Response Status O

Cl Main SC 7.3.2.1 P 44 L 2 # 33  
 Sukert, Alan Xerox  
 Comment Type E Comment Status X  
 Based on the precedence we established at the last meeting, I believe in Table 6 that the reference to '802.11' should be to IEEE Std 802.11  
 SuggestedRemedy  
 See above  
 Proposed Response Response Status O

Cl Main SC Clause 10 P 4 L 57 # 29  
 Sukert, Alan Xerox  
 Comment Type T Comment Status X  
 IÆm not sure what you mean by ðonly in front of the HCD if necessaryö.  
 SuggestedRemedy  
 Clarify wording  
 Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security comments

Cl Main SC Clause 10 P 4 L 60 # 39  
 Sukert, Alan Xerox  
 Comment Type T Comment Status X  
 You should add "software" to the items for which installation is limited to authorized users.  
 SuggestedRemedy  
 See above  
 Proposed Response Response Status O

Cl Main SC Clause 10 P 4 L 64 # 38  
 Sukert, Alan Xerox  
 Comment Type T Comment Status X  
 Many of your objectives cover copying and printing, but these objectives need to be expanded to include scanning and faxing where applicable. Specifically, I believe scanning needs to be included in the discussion for O.ACCESS, O.MONITOR and O.GENUINE.  
 SuggestedRemedy  
 Add references to scanning in the appropriate places.  
 Proposed Response Response Status O

Cl Main SC Clause 10 P 4 L 65 # 40  
 Sukert, Alan Xerox  
 Comment Type T Comment Status X  
 Seems like something is missing in this sentence "what type of limits on the number of pages are you referring to here?"  
 SuggestedRemedy  
 Clarify wording.  
 Proposed Response Response Status O

Cl Main SC Clause 10 P 4 L 72 # 41  
 Sukert, Alan Xerox  
 Comment Type T Comment Status X  
 I think you need to clarify what data is expected to be overwritten here - is it limited to User Document Data or does it include User Function Data and Management Data. Does it apply to permanent data or does it also apply to temporary data. Finally, this discussion addresses data stored on hard disks; there are other forms of non-volatile and volatile storage on an HCD in which data is stored "what requirements should be placed on them with respect to overwriting."  
 SuggestedRemedy  
 Clarify what overwriting is to be mandated.  
 Proposed Response Response Status O

Cl Main SC Clause 10 P 4 L 82 # 42  
 Sukert, Alan Xerox  
 Comment Type T Comment Status X  
 I'm not sure what encrypting network channels have to do with this particular objective; I would think it better belongs under the O.NETWORK discussion. More importantly, I think the objective that is missing here is requiring encryption of User Data and possible also Management Data stored on non-volatile (and possibly also volatile) storage.  
 SuggestedRemedy  
 Move the current mandated "encryption" function under O.NETWORK and add a new mandated disk encryption function under O.PROTECT  
 Proposed Response Response Status O

Cl Main SC Clause 10 P 5 L 93 # 43  
 Sukert, Alan Xerox  
 Comment Type T Comment Status X  
 Should we only be concerned here with ports that allow submission of jobs or should we be concerned also with ports that would allow an attacker access to the machine for installing rogue software, accessing shell scripts, etc?  
 SuggestedRemedy  
 Clarify what ports should be disabled.  
 Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security comments

Cl Main SC Clause 10 P 5 L 100 # 44  
 Sukert, Alan Xerox

Comment Type T Comment Status X

Probably need to clarify what you mean by "comprehensive" so there is no confusion whether a manufacturer has satisfied this requirement. I also wonder if this requirement should, as a minimum, include the security events required by the FAU\_GEN.1 SFR.

SuggestedRemedy

Clarify use of term "comprehensive"

Proposed Response Response Status O

Cl Main SC Clause 10 P 5 L 104 # 45  
 Sukert, Alan Xerox

Comment Type T Comment Status X

I think you should clarify here that this mandated function only applies to external interfaces and not to all (that would include internal interfaces) of the HCD.

SuggestedRemedy

Clarify what interfaces apply in this case.

Proposed Response Response Status O

Cl Main SC Clause 10 P 5 L 112 # 46  
 Sukert, Alan Xerox

Comment Type T Comment Status X

Probably need to clarify what you mean by "genuine" so there is no confusion whether a manufacturer has satisfied this requirement. You probably also need to clarify whether this requirement applies when the HCD is first installed by the manufacturer or whether it also applies to software upgrades provided by the manufacturer (personally I think it should).

SuggestedRemedy

Clarify what "genuine" means in this context and whether this applies to software upgrades.

Proposed Response Response Status O

Cl Main SC Clause 10 P 6 L 166 # 48  
 Sukert, Alan Xerox

Comment Type T Comment Status X

You've created a new actor here called "security administrator". I'm not saying that isn't a good idea, but if we want to do that we'll have to provide a definition for Clause 3 and determine if this actor should be included in the Protection Profile(s).

SuggestedRemedy

See above

Proposed Response Response Status O

Cl Main SC tables in 7.4, 7.5 P L # 56  
 Smithson, Brian Ricoh

Comment Type E Comment Status X

I think that tables 52-56 could be streamlined and made more useful by combining them into one or two tables.

SuggestedRemedy

Two choices:

(1) Combine tables 52-56 into a single table with column headings "Threat ID", "Clause", "PP-A Risk Rating", "Included in PP-A", "PP-B Risk Rating", "Included in PP-B", "PP-C Risk Rating", "Included in PP-C", "PP-D Risk Rating", and "Included in PP-D". For easier formatting, the four PP designations could span pairs of columns, each with subheadings "Risk Rating" and "Included"

(2) If choice (1) is too wide or otherwise unwieldy, combine tables 52-55 into a single table with column headings "Threat ID", "Clause", "PP-A Risk Rating", "PP-B Risk Rating", "PP-C Risk Rating", and "PP-D Risk Rating". For easier formatting, "Risk Rating" could be a heading that spans the last four columns, and each of those columns would only need to identify the PP. In this case, we would leave table 56 as is.

Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-A** SC P L # 1

Ito, Takashi Konicaminolta Busines

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

The current versions of the PP-A still seems to refer EAL2 and EAL3 seperately in the same PP.  
 (example)  
 EAL3 at 1.1 PP reference  
 EAL2 at 2.3 Conformance to Packages, 6.2 Table 12

Besides, there seems many mismatches between the main documents and each PP.

*SuggestedRemedy*

Will recommend to check the PPs and main documents again.

Proposed Response Response Status **O**

Cl **PP-A** SC P L # 17

shinichirou, Inohara Panasonic communica

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

1.2.2, Table 1 External Environment  
 The following problems have been identified in the ""External Environment"" description.  
 1)""External Environment"" should be protected by the environment external to the TOE.  
 Mandating the protection of the ""External Environment"" to the HCD implementation is impractical and thus the External Environment should be removed from the asset definition.  
 2)áAsset ""External Environment"" can not be removed if T.EA.FAXBRIDGE is to be left in the PP.  
 (note) T.EA.FAXBRIDGE does not address the asset ""External Environment"" as attack target, but should be included in the threat definition.  
 Further discussion is needed before merging the threats T.EA.PROXY, T.EA.DOS and T.EA.FAXBRIDGE.

*SuggestedRemedy*

Please reexamine by the above-mentioned viewpoint.

Proposed Response Response Status **O**

Cl **PP-A** SC P L # 14

shinichirou, Inohara Panasonic communica

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

1.2.2, Table 1 Management Data  
 The following data is defined as Management Data, ""user and administrator authentication data (e.g. passwords)"" , ""audit data,"" ""log data"" , ""device configuration data"" and ""network management data"" .

*SuggestedRemedy*

- 1) Propose to reclassify Management Data and User Function Data from the viewpoint of Primary and Secondary asset.
- 2)áAddition of Recommended ""Audit Data (Audit Function)"" descriptions.
- 3)áAddition of Recommended ""Device configuration data"" descriptions.

Proposed Response Response Status **O**

Cl **PP-A** SC P 1 L # 10

shinichirou, Inohara Panasonic communica

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

The ST must include all TOE Security Objectives from the PP (addition of Objectives is permitted).  
 The ST includes all Security Objectives for the Operational environment that is described in the PP, and addition of Objectives for the Operational environment is prohibited.  
 TOE Security Objectives provide protection for the assets by countering threats. The Security Objectives depend on the Functionality provided by the HCD. This PP not only defines Security Functions but also restricts the functions which can be implemented in the HCD.

*SuggestedRemedy*

Request is made to divide the TOE Security Objectives according to the functions of the HCD (Copy, Printer, FAX, ScanTrasmission etc.).

Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-A** SC P 1 L # 11  
shinichirou, Inohara Panasonic communica

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

TOE Security Objectives must be meet by Functional Requirements. Assurance Requirements assure that the Functional Requirement are enforced, but can not directly meet TOE Security Objectives.

Assurance Requirements (SAR) are traced to TOE Security Objectives.

*SuggestedRemedy*

Please reexamine by the above-mentioned viewpoint. A possible solution would be to define Explicitly stated Security Functional Requirements to meet TOE Security Objectives. Security Functional Requirements EXP\_FAX.1 assumes that there are no interfaces enabling access from public telephone network to the internal network. Definition of such Explicitly stated Security Functional Requirement should not be allowed. Please delete TOE security object if you cannot define an appropriate security functional requirement.

Proposed Response Response Status **O**

Cl **PP-A** SC 1.2.2 P 11 L # 8  
shinichirou, Inohara Panasonic communica

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

1.2.2, Table 1 Firmware

1)áThe Firmware boundary needs to be clarified.

From the PP description Firmware appears to be a part of the TOE. Since the TOE has Firmware update functionality, it is inconsistent to define the Firmware as an asset.

2) The Physical and Logical boundary of the TOE needs to be clarified.

Is the Firmware a part of the TOE? Is the Firmware TSF enforcing?

Is there any reason to define the Firmware as an asset, if it is not a part of the TOE?

3)áA counter measure is needed if the Firmware can be remotely updated.

*SuggestedRemedy*

Please reexamine by the above-mentioned viewpoint.

Proposed Response Response Status **O**

Cl **PP-A** SC 1.2.2 P 11 L # 16  
shinichirou, Inohara Panasonic communica

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

1.2.2, Table 1 TOE Availability

The definition of the threats against the asset is not complete. If Availability is considered as an asset, threats such as Malfunction, power failure, Natural disaster, DoS attack, exhaust of supply (toner, paper etc.) should be defined. Security Objectives to counter such threats should also be defined.

*SuggestedRemedy*

The threat of DoS attacks has not been addressed even in PPs for Firewall and Operating Systems. To mandate the implementation of counter measures against DoS attacks in HCD is impractical. Availability should be removed as an asset from this PP.

Also the description of A.NETWORK, OE.NETWORK, OE.NET\_MANAGE should be revised to implicitly remove the threat of DoS attacks.

Impact on threat description is as follows.

1)áT.DOS.NET

T.DOS.NET is r emoved as a result of TOE Availability being excluded from the asset definition.

Proposed Response Response Status **O**

Cl **PP-A** SC 1.2.2 P 11 L # 15  
shinichirou, Inohara Panasonic communica

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

1.2.2, Table 1 Resource

The protection of ""Resource"" is not limited to of consumable supplies for the TOE (e.g., paper, toner) but can be viewed as the same approach to protect User Document Data. If the asset ""Resource"" is the physical entity, both physical and logical protection is needed. Currently the Objectives define only the logical protection of the ""Resources"". Objectives to protect the ""Resource"" physically is yet to be defined.

*SuggestedRemedy*

Although further Study needed a possible resolution would be as follows.

Instead of defining the ""Resource"" as an asset, define the ""Service provided by the HCD"" as the asset which its confidentiality is protected. Doing so will enable to remove the need to define physical protection against the assumed threats.

Impact on threat description will be as follows.

1) Remove the threats T.RESOURCE.COPY, T.RESOURCE.PEER, and define a new threat that addresses the unauthorized usage of Services provided by the HCD.

Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-A** SC 1.2.2 P 11 L # 13  
shinichirou, Inohara Panasonic communica

Comment Type T Comment Status X

1.2.2, Table 1 User Function Data  
User Function Data is defined as, ""user identifiers for access control (excluding user authentication data such as passwords)""; ""destination lists for scanning"" and ""address books for facsimile delivery"". "" destination lists for scanning"" and ""address books for facsimile delivery"" are primary assets. The ""user identifiers for access control"" should be considered as a secondary asset used by the Security Function to protect the primary asset.

SuggestedRemedy

Please reexamine by the above-mentioned viewpoint.  
A possible solution would be to re-classify ""User Function Data"" along with ""Management Data"" from the viewpoint of Primary and Secondary asset.

Proposed Response Response Status O

Cl **PP-A** SC 1.2.2 P 11 L # 12  
shinichirou, Inohara Panasonic communica

Comment Type T Comment Status X

1.2.2, Table 1 User Document Data  
""User Document Data"" includes the original document in hardcopy form. Such physical entity can not be protected by IT measures. (Secure print only protects the digital data which has not yet been printed as a hardcopy)

SuggestedRemedy

Please reexamine by the above-mentioned viewpoint.  
  
A possible solution would be to limit ""User Document Data"" should be limited to digital data existing inside the HCD.  
Impact on threat description  
1) T.UD.PHY.OUTPUT  
This threat is against the document in hardcopy form, and thus should be omitted.

Proposed Response Response Status O

Cl **PP-A** SC 1.2.2 P 12 L # 25  
Masui, Takanori Fuji Xerox Co.,Ltd.

Comment Type T Comment Status X

Assets of ""Resource"" includes not IT assets such as toner and paper. It is difficult to protect these non IT assets by IT security function. Those non IT assets should be protected by physical security (e.g. Locking paper tray or front cover). Assets should be IT assets in this PP. And I think that asset of ""TOE availability"" represents one aspect of asset ""service(Copy/Scan/Fax/Print)"". This comment is also same for PP-B.

SuggestedRemedy

I think it is better merge two assets of ""Resource"" and ""TOE availability"" into one asset of ""service(Copy/Scan/Fax/Print)"".  
Threats are unauthorized use of service and unauthorized stop of the service.

Proposed Response Response Status O

Cl **PP-A** SC 3.1 P 19 L # 18  
shinichirou, Inohara Panasonic communica

Comment Type T Comment Status X

3.1 Robustness  
""Robustness"" is included in the PP. The term ""Robustness"" is unique to the US scheme and not valid in other countries.

SuggestedRemedy

A possible resolution would be to remove Robustness from the PP (Resolution enforces Definition requirements other than CC) .

Proposed Response Response Status O

Cl **PP-A** SC 3.2 P 20 L # 26  
Masui, Takanori Fuji Xerox Co.,Ltd.

Comment Type T Comment Status X

Now T.UD.SNIFF includes T.UD.SNIFF.EM(P2600 Threat), but I think it is hard to protect sniffing EM on MFP practically. I wonder if DOD requires any PCs and Displays to protect this EM sniffing. And skill of attackers who sniff EM may be beyond EAL3.

SuggestedRemedy

Focu on T.UD.SNIFF only as T.UD.SNIFF.NET.

Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-A** SC 3.2.1 P 19 L # 20  
 shinichirou, Inohara Panasonic communica

Comment Type T Comment Status X

3.2.1, Table 5 T.UD.ACC.HACK  
 The following problems have been identified.  
 1)If this threat is not merged with T.UD.ACC.NORMAL, it can be removed on the condition that the ""User Document Data"" can not be modified from the Service port and other normally used interfaces.  
 2)áIf this threat is not merged with T.UD.ACC.NORMAL, and there are no Service port and other normally used interfaces which can access ""User Document Data"", this threat can be left in the current state.

*SuggestedRemedy*

Please reexamine by the above-mentioned viewpoint.

Proposed Response Response Status O

Cl **PP-A** SC 3.2.1 P 19 L # 21  
 shinichirou, Inohara Panasonic communica

Comment Type T Comment Status X

3.2.1, Table 5 T.UD.SNIFF  
 The PP defines a excessive threat addressing Electromagnetic noise.

*SuggestedRemedy*

Threat T.UD.SNIFF.EM which addresses Electromagnetic noise should be removed.

Proposed Response Response Status O

Cl **PP-A** SC 3.2.1 P 19 L # 22  
 shinichirou, Inohara Panasonic communica

Comment Type T Comment Status X

3.2.1, Table 5 T.UD.IMP  
 A threat of actively impersonating the destination (e.g. mail server) or the origin (e.g. print server), or by actively impersonating related service (e.g. domain name server).  
 Identified problems are as follows.  
 TOE usage environment needs to be defined.  
 1) It is assumed that this threat implies the use of SSL communication (digital certificates). Such counter measures for communication between the TOE and servers on the local network is extreme.  
 2) The use of Internet servers and Internet services needs to be clarified.

*SuggestedRemedy*

This threat can be countered by properly administrating the destination (e.g. mail server) or the origin (e.g. print server), or servers providing related service. The enhancement of OE.NET\_MANAGE to include such measures, or defining a new Security Objective for the management which addresses the proper maintenance and administration of such servers, is recommended.

Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-A** SC **3.2.1** P **19** L # **19**  
 shinichirou, Inohara Panasonic communica

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

3.2.1, Table 5 T.UD.ACC.NORMAL

User Document Data handled in HCD can be classified into two categories, Spool and Filing. Since the external interfaces for the Spool is not provided, T.UD.ACC.NORMAL should be considered as a threat to the User Document Data stored on HCD using its Filing capabilities.

(Further study is needed to determine whether Secure Print should be handled as ""Spool"" , ""Filing"" or another Category.)

The following problems have been identified.

1)áIf the interfaces to access ""User Document Data"" can be identified,

T.UD.ACC.NORMAL can be left in the PP in the current form.

2)áThe interface to access the ""User Document Data"" is identified.

A threat must be derived with the attack agent and the adverse action against the asset.

When deriving the threat, consideration must be given to the attack agent, the asset, and the adverse action. But in the threat description, only the negative effect caused by the threat needs to be stated.

*SuggestedRemedy*

A possible resolution to the above problem is as follows.

1)áMerge the two threats T.UD.ACC.NORMAL?T.UD.ACC.HACK. And change the threat description to eliminate the need to identify the interface to access ""User Document Data"".

2)ááT.UD.SALVAGE is a threat which addresses residual data. Thus should not be merged with T.UD.ACC.NORMAL?T.UD.ACC.HACK.

3)áExplicitly state that ""User Document Data"" uses the Filing feature of the HCD.

Proposed Response Response Status **O**

Cl **PP-A** SC **3.2.4** P **21** L # **9**  
 shinichirou, Inohara Panasonic communica

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

3.2.4, Table 8 T.EA.FAXBRIDGE

1)If the asset is ""User Document Data"" and ""Management Data(excluding Firmware)"" , the interface to access these assets is needed.

2)áAsset ""HCD Availability"" is defined as an asset which its confidentiality needs to be protected.

However in the case of fax transmission, öHCD Availability"" is obvious and should be removed from the T.EA.FAXBRIDGE description.

3) If T.EA.FAXBRIDGE covers the attack on ""External Environment"" , a function to control access to the internal network from the public phone lines is needed.

*SuggestedRemedy*

1)áRemoval of T.EA.FAXBRIDGE from the PP.

2)áLeave T.EA.FAXBRIDGE in the PP due to high demand from customers. -> See comment No.9

Proposed Response Response Status **O**

Cl **PP-A** SC **3.2.4** P **22** L # **24**  
 Masui, Takanori Fuji Xerox Co.,Ltd.

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

According to the operational environment A which was described in section 5.2 of main document, there is no FAX connection to MFP. However, in PP-A it describes about threat of T.EA.FAXBRIDGE. There's inconsistency between environment and threat analysis.

*SuggestedRemedy*

Delete T.EA.FAXBRIDGE

Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-A** SC **3.2.5** P **25** L # **23**  
 shinichirou, Inohara Panasonic communica

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

3.2.5, Table 9 T.TSF.CRED

The description "Gaining the ability" is not suited for a threat description.  
 Assets directly addressed by threat T.TSF.CRED should be the Management Data. The other assets are jeopardized as a consequence of the attacker "Gaining the ability".

*SuggestedRemedy*

A possible resolution would be as follows.

Merge threats T.TSF.CRED?T.TSF.AUD?T.TSF.CONF. Define a new threat which jeopardizes the confidentiality and integrity of the "Management Data".

Proposed Response Response Status **O**

Cl **PP-A** SC **4.4.1** P L # **27**  
 Masui, Takanori Fuji Xerox Co.,Ltd.

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

T.DOS.NET is countermeasured by O.RESILIENT. However O.RESILIENT composed by SAR not by SFR. This means TOE has no security function against DOS attacks. I think recovery from end of DOS attacks concerns software quality. So if we have to care about DOS attacks, TOE must have security function against DOS attacks.

*SuggestedRemedy*

I think it is better delete threat of DOS attacks if we focus on only recovery from DOS attacks.

Proposed Response Response Status **O**

Cl **PP-B** SC P L # **28**  
 Masui, Takanori Fuji Xerox Co.,Ltd.

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

PP-B targets enterprise use, then I think robustness requirement is not necessary for PP-B. And Japanese evaluation scheme (JISEC) comments it is difficult to evaluate TOE which include current robustness because it involves US unique requirements.

*SuggestedRemedy*

Delete robustness requirements not only PP-B but PP-A. CIM of CCv3.1 is not released for a while, I think it is difficult to evaluate PP which includes robustness. We need DAPS comment on this issue (they still require robustness for MFP for US Government or not.)>

Proposed Response Response Status **O**