

IEEE P2600 Hardcopy Device and System Security Comments

CI **PP-A** SC 17 P L # 16
 Nevo, Ron Sharp

Comment Type T Comment Status D

The NVS PP section 17 is not clear.
 ò It is more related to removal H.D that is external to the TOE.
 ò The SFRs are trying to protect ""transmission"" between the TOE and the removal H.D, instead of protecting the data that are stored in the H.D.
 ò The way it is written, it is not intended for internal H.D.
 ò The propose of this P.P is to protect data that are stored in the H.D, when the H.D is removed from the MFP
 ò

SuggestedRemedy

We need to find different SFRs such as the FCS family.(encryption) or no access control to the H.D while it is outside the TOE.

Proposed Response Response Status W

PROPOSED ACCEPT IN PRINCIPLE.

Will clarify that we mean storage to the NVS instead of transmission. (if of course the current proposal for the use of the export SFRs is adopted). Alternately, we may define an extended SFR that explicitly addressess our case.

CI **PP-A** SC 17.2 P L # 15
 Nevo, Ron Sharp

Comment Type T Comment Status D

Necessity of FDP_UCT.1:
 FDP_UCT.1 is a requirement to assure confidentiality in transmitting user data using external channel between TOE and trusted IT product. However, NVS is intended non volatile memory in HCD. So, it may be mis-selection of a functional requirement.
 Also FPT_ITC.1, which is selected due to dependency of FDP_UCT.1, is not appropriate.

SuggestedRemedy

Appropriate SFRs should be selected regarding NVS.
 They are probably FCS_COP.1, etc.

Proposed Response Response Status W

PROPOSED ACCEPT IN PRINCIPLE.
 See resolution to comment 16.

CI **PP-C** SC 11.4 P L # 5
 aubry, carmen oce

Comment Type T Comment Status D

Table 15: If all the users are allowed to create, read, modify and delete, there is no point of having an access control (What does it control?).

SuggestedRemedy

Remove FDP_ACC.1&FDP_ACF.1

Proposed Response Response Status W

PROPOSED ACCEPT.

CI **PP-A** SC 12.3 P L # 14
 Nevo, Ron Sharp

Comment Type T Comment Status D

Necessity of FIA_UAU.6:
 We are wondering why FIA_UAU.6 is necessary in PRT.
 Here we describe a situation based on PRT.
 At first, user needs to be identified and authenticated by HCD prior to print. Consequently, he sends print data to the HCD.
 After finishing the print data, the user performs identification and authentication in HCD to obtain the output.
 We think that this is the usual usage of PRT. FIA_UAU.6 is supposed to be the (re-)authentication after finishing sending the print data to the HCD.
 However, we think this is not re-authentication but identification and authentication.
 The first reason: The I&A before printout and the authentication after sending print data is different in channels that each feature is using (explained in 6.3.4).
 The second reason: If it is (re-)authentication that uses the same channel as sending print data, the security function is probably no meaning. That is, user sends print data to HCD from a physically distant position, and he has to (re-)authenticate from the physically distant position to obtain the printout.

SuggestedRemedy

Remove FIA_UAU.6 form PRT

Proposed Response Response Status W

PROPOSED ACCEPT IN PRINCIPLE.

Will add an application note that this is related to the PIN print use case for PRT only.

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-A** SC 11.8 P L # 13
 Nevo, Ron Sharp

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

Necessity of FPT_TEE.1:

- 1) The problem is that the specification of TOE is ambiguous (in the PP). In IEEE 2600.1-36c, TOE is interpreted as a whole MFD. In this case, external entity must exist outside the MFD. Does FPT_TEE.1 mean it? If yes, we are wondering if there is any meaning of FPT_TEE.1.
- 2) From the past, we have heard the recognition that TOE is firmware in HCD. If so, this should be described in TOE Overview and the other appropriate places. In this case, external entity that FPT_TEE.1 handles is hardware of HCD, and it is OK that you perform a test regarding the hardware properties.
- 3) In application note, there is a description that FPT_TEE.1 is a principal SFR to fulfil O.SOFTWARE.VERIFIED. However, FPT_TEE.1 verifies properties in external entities. If software is an external entity, what is TOE? OS?

SuggestedRemedy

Delete FPT_TEE.1

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

Will switch back to FPT_TST.

Cl **PP-A** SC 6 P L # 12
 Nevo, Ron Sharp

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

TOE Overview (APE_INT) explains not only PP area (where evaluation body evaluates using Common Criteria) but also SFR packages

SuggestedRemedy

The explanation should be limited to TOE area which is specified as PP.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

Refers to Clause 4 page 3 line 12. Also create a packages introduction.

Cl **PP-A** SC P L # 11
 Nevo, Ron Sharp

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

PP description and package description are mixed in PP area (where evaluation body evaluates using Common Criteria).
 For example, HCD functions are described in 6.3.2.3 Functions and they are specified as Attributes in 6.3.2.4, however Attributes do not exist in the PP. (+PRT is not necessary in PP area)

SuggestedRemedy

same as 12

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

Figure 1 should clarify that functions are optional and are addressed by SFR packages.

Clause 6.3.2.3 and 6.3.2.4 will be moved to the new packages introduction section.

Note: Also add an abstract reference for functions and attributes in the PP text.

Cl **PP-A** SC 4.2 P L # 10
 Nevo, Ron Sharp

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

CC Version is not identified in SFR Packages reference.

SuggestedRemedy

Describe CC version that corresponds to each package.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **PP-A** SC 4 P L # 9
 Nevo, Ron Sharp

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

SFR Packages reference is described in Protection Profiles introduction

SuggestedRemedy

same as 12

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

See response to comment 11.

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-A** SC P L # 8
 Nevo, Ron Sharp

Comment Type T Comment Status D

Document structure (2)
 If a whole document including packages is supposedly interpreted as a PP, it is just a PP, not a package.
 Though the new document describes assets, threats and objective policies with more abstract way than before, it is essentially no different from the one that was before Family PP. That is, ST/TOE required by 2600.1-36c is an MFP with full functions (PRT, SCN, CPY, FAX, DSR, NVS, and SMI).

SuggestedRemedy

Same as number 12

Proposed Response Response Status W

PROPOSED ACCEPT IN PRINCIPLE.

See response for comment 11.

Cl **PP-A** SC P L # 7
 Nevo, Ron Sharp

Comment Type T Comment Status D

Document structure (1):
 The document weaves PP part with package part (or packages are mixed in the PP). That may be based on 7 Conformance claims (page 11), however conformance to packages and document structure regarding PP and package are the different issues. In addition, people will misunderstand that certification is granted to packages unless PP part and package part are explicitly separated since no certification will be granted to any package.

SuggestedRemedy

- 1) Make packages independent as individual documents.
- 2) Make the document 3-part structure: PP area, package area, and the part that is required in IEEE P2600.

Proposed Response Response Status W

PROPOSED ACCEPT IN PRINCIPLE.

No to Suggested Remedy 1.

Each IEEE document contains two parts, a PP area and a package area. Will make sure that it is clear that an ST is only to include those packages that are applicable to the function of the TOE.

Cl **PP-A** SC P L # 6
 Nevo, Ron Sharp

Comment Type T Comment Status D

These comment related to stand alone copier(without DSR,NVS,SMI) or stand alone scanner (without DSR/NVS).(IF NVS or DSR is a mandatory requirements than they should be mandatory requirements).

HCD functions are specified (target of certification will be restricted).
 This means that the same things happen as you started creating Family-PP.
 For example, there are D.DOC and T.DOC in the assets and the threats described in 36c, however, these were not specified in 35a. In this case, we consider stand alone copier (no DSR/NVS/SMI). If there are no interfaces to scanned image or copied image, there occur threats to neither confidentiality nor integrity.

That is, you are going to create some interfaces to unnecessary point and then necessitate implementing the security function to protect them from the threat.

* If we follow the way of thinking from the past, for the machine that has each of the 120 combinations of the basic functions PRN, SCN, CPY and FAX and the options DSR, NVS and SMI, you need to verify at least the area where the PP covers, or inconsistency of the machine that the PP intends if it covers a certain area. Upon this verification, you may need to limit the machine that is covered by the PP or modify the PP (including SFR packages).

SuggestedRemedy

- 1) PP should be constructed from assets and threats that are derived from common features of HCD.
 Since functional requirements that are common to all HCD functions in IEEE 2600.1-35a are FAU_*, FIA_*, FMT_MTD, FMT_SMF, FMT_SMR, FPT_*, and FTA_*, you should create common features among them.
- 2) Limit the types of HCD that is intended to evaluate.
 For example: exclude scanner, or a machine that does not store user data in non volatile memory.

Proposed Response Response Status W

PROPOSED REJECT.

To achieve an audit trail you need either SMI for an external audit trail or NVS for a locally stored audit trail.. Neither is mandatory.

IEEE P2600 Hardcopy Device and System Security Comments

Cl **All P** SC 1.4.1 P 1 L 19 # 22
 Smithson, Brian Ricoh
 Comment Type **E** Comment Status **D**
 [MEC] IEEE doesn't like one subclause at any level.
 SuggestedRemedy
 Remove the 1.4.1 heading, just leave the body text.
 Proposed Response Response Status **W**
 PROPOSED ACCEPT.

Cl **All P** SC 2 P 2 L 14 # 23
 Smithson, Brian Ricoh
 Comment Type **E** Comment Status **D**
 [MEC] The "[Bn]" notation for reference documents is only used if the documents are in an informative bibliography.
 SuggestedRemedy
 Remove the "[Bn]" notation, just leave the document names.
 Proposed Response Response Status **W**
 PROPOSED ACCEPT IN PRINCIPLE.

Will move informative references to the Bibliography. Normative references will have the [Bn] notation removed.

Cl **All P** SC 2 P 2 L 14 # 24
 Smithson, Brian Ricoh
 Comment Type **E** Comment Status **D**
 [MEC] Normative reference documents should be listed only if they are cited somewhere in the standard.
 SuggestedRemedy
 Check to see if any of the referenced documents are not cited, and then either (a) cite them if appropriate, or (b) remove them from clause 2.
 Proposed Response Response Status **W**
 PROPOSED ACCEPT IN PRINCIPLE.

Will include only required reading in the Normative Reference section. So far IEEE2600 is the only Normative Reference.

Cl **All P** SC 3 P 2 L 27 # 25
 Smithson, Brian Ricoh
 Comment Type **E** Comment Status **D**
 [MEC] There is no need for clause 3 since it simply points to the glossary and acronym annexes.
 SuggestedRemedy
 Remove clause 3, but make sure that the annexes fully reference IEEE Std. 100.
 Proposed Response Response Status **W**
 PROPOSED ACCEPT.

Cl **All P** SC 4 P 3 L 16 # 26
 Smithson, Brian Ricoh
 Comment Type **T** Comment Status **D**
 [Kurth] There is an error on this line [it is a remnant from the FoPP text]
 SuggestedRemedy
 substitute "Protecton Profile" by "SFR Package"
 Proposed Response Response Status **W**
 PROPOSED ACCEPT.

Cl **All P** SC 4.1 P 3 L 30 # 40
 Sukert, Alan Xerox
 Comment Type **E** Comment Status **D**
 Because of the large revisions to the PPs, the acronyms MFD and MFP are used here for the first time without first being defined.
 SuggestedRemedy
 Defined the acronyms MFD and MFP when they are first used in all four PPs.
 Proposed Response Response Status **W**
 PROPOSED ACCEPT.

IEEE P2600 Hardcopy Device and System Security Comments

CI All P SC 4.2.6 P 4 L 22 # 37
 Smithson, Brian Ricoh

Comment Type T Comment Status D

We have been unable to find a suitable PP solution to assure protection from offline salvage of data from nonvolatile storage devices. See ["http://grouper.ieee.org/groups/2600/presentations/Longmont/no-offline-salvage.pdf"](http://grouper.ieee.org/groups/2600/presentations/Longmont/no-offline-salvage.pdf) for detailed explanation and rationale.

SuggestedRemedy

Remove references to NVS package in the common PP, and remove the NVS package.

Proposed Response Response Status W

PROPOSED ACCEPT IN PRINCIPLE.

Still working on it..

CI All P SC 4.2.6 P 4 L 27 # 2
 aubry, carmen oce

Comment Type T Comment Status D

In the SFR package reference it is mentioned "recovery of deleted data", while in 17.1 NVS SFR package introduction (page 43, line 7): "data that is stored on removable nonvolatile storage devices in the TOE".

SuggestedRemedy

Clarify what kind of protection is expected from this package (all stored data or only the deleted one).

Proposed Response Response Status W

PROPOSED ACCEPT IN PRINCIPLE.

Will clarify when the NVS SFR package usage is finalized.

CI All P SC 4.2.6 P 4 L 27 # 19
 Smithson, Brian Ricoh

Comment Type E Comment Status D

[Kurth] Clarification of the application of the package.

SuggestedRemedy

Explain that this package applies for TOEs that provide the ability to protect data stored on removable NVS devices from unauthorized disclosure and modification. If such protection is supplied by the TOE environment and not the TOE itself, this package can not be claimed.

Proposed Response Response Status W

PROPOSED ACCEPT IN PRINCIPLE.

Part of the NVS SFR package clarification writeup.

CI All P SC 4.2.7 P 4 L 35 # 20
 Smithson, Brian Ricoh

Comment Type E Comment Status D

[Kurth] Clarification of the application of the package.

SuggestedRemedy

Explain that this package applies for TOEs that provide a trusted channel function allowing for secure and authenticated communication with other IT systems. If such protection is supplied by the TOE environment and not the TOE itself, this package can not be claimed.

Proposed Response Response Status W

PROPOSED REJECT.

TOE must support the use of a trusted channel natively.

CI PP-D SC 5.2 P 4 L 45 # 114
 Sukert, Alan Xerox

Comment Type E Comment Status D

Appears that a part of the last sentence was accidentally left off - the paragraph ends with an incomplete sentence.

SuggestedRemedy

Complete the description of Operational Environment C in the last paragraph in subclause 5.2.

Proposed Response Response Status W

PROPOSED REJECT.

Paragraph is complete.

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-A** SC **6.1** P **6** L **15** # **75**
 Sukert, Alan Xerox

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

There is an inconsistency between the definition of the Nonvolatile storage package here and the corresponding definition in subclause 4.2.6, page 4, line 25. Subclause 4.2.6 says that this package is for "nonvolatile storage of document data in a storage device which can practically be removed...for analysis and recovery of data". Here it says that this package is for "persistent or temporary document storage on devices that could practically be removed and analyzed when the HCD is powered off." Note also that I believe it should be "practically" and not "practicably" in subclause 6.1.

A similar comment applies to the same subclauses in PP-B and PP-C.

SuggestedRemedy

Resolve the inconsistency in the definition of the Nonvolatile storage package between subclauses 4.2.6 and 6.1. Note: Make sure that what is decided here is also reflected in the F.NVS function definition in subclause 6.3.2.4, page 9, line 1 (Table 3).

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

Will clarify the definition and make consistent with the NVS SFR package re-write.

Cl **PP-A** SC **6.1** P **6** L **16** # **74**
 Sukert, Alan Xerox

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

There is an inconsistency between the definition here of the Document storage and retrieval package here and the corresponding definition in subclause 4.2.5, page 4, line 21. Subclause 4.2.5 says that the document is "persistently stored" during one job and can be retrieved "during one or more subsequent jobs". Here it makes no mention of persistent storage and says that the document is stored during one job for access "during a subsequent document processing job."

A similar comment applies to the same subclauses in PP-B and PP-C.

SuggestedRemedy

Resolve the inconsistency in the definition of the Document storage and retrieval package between subclauses 4.2.5 and 6.1. Note: Make sure that what is decided here is also reflected in the F.DSR function definition in subclause 6.3.2.4, page 9, line 1 (Table 3).

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **All P** SC **6.2** P **6** L **23** # **42**
 Sukert, Alan Xerox

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

This is a minor comment but might as well fix it now before the evaluators find it.

'TOE' is used as an acronym on this line for the first time but isn't defined until line 36 on this page.

SuggestedRemedy

Define the acronym 'TOE' when it is first used in subclause 6.2 in all four PPs.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **All P** SC **6.2** P **6** L **29** # **41**
 Sukert, Alan Xerox

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

In keeping with the convention used in this subclause, the words 'Users' and 'Subjects' on this line should be italicized because they are referring to the Common Criteria entities.

Same comment applies to the use of the word 'Objects' on line 40.

SuggestedRemedy

Italicize the words 'Users', 'Subjects' and 'Objects' in subclause 6.2 in all four PPs.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **All P** SC **6.2** P **6** L **29** # **45**
 Sukert, Alan Xerox

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

Subclause 6.2 implies that for this PP Users and Subjects are essentially the same thing ("the distinction between Users and Subjects is not necessary"). I noted however that the definitions of User and Subject in Annex A are different which would conflict with the above statement.

SuggestedRemedy

Add a note in subclause 6.2 in all four PPs that although the definitions of User and Subject are different in Annex A, the definitions of the two terms should be treated as being the same.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

Clarify that both definitions are included when referring to either.

IEEE P2600 Hardcopy Device and System Security Comments

CI All P SC 6.2 P 6 L 31 # 44

Sukert, Alan Xerox

Comment Type T Comment Status D

The description of Users and Subjects in this subclause implies an App Note is needed in the case that an ST or PP author wants to restore the distinction between Users and Subjects. However, no such App Note is included in this PP.

Note that a similar comment applies to the distinction between TSF and TOE in subclause 6.2, page 6, line 37.

SuggestedRemedy

Add an App Note in all four PPs that discusses the ST or PP author's ability to restore the distinction between Users and Subjects, and between the TSF and the TOE.

Proposed Response Response Status W

PROPOSED ACCEPT.

CI All P SC 6.2 P 6 L 40 # 43

Sukert, Alan Xerox

Comment Type T Comment Status D

The new definition of 'Objects' in subclause 6.2 differs from the definition of 'object' in Annex A. In subclause 6.2 an object is defined as ""data (which can be created, read, modified and deleted) and functions (which can be executed)"". Annex A, page 51, line 14 defines an object as ""A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.""

SuggestedRemedy

Make the definitions of 'object' consistent between subclause 6.2 and Annex A in all four PPs.

Proposed Response Response Status W

PROPOSED ACCEPT IN PRINCIPLE.

Resolution pending, editor will investigate.

CI All P SC 6.2 P 7 L 2 # 46

Sukert, Alan Xerox

Comment Type E Comment Status D

In Figure 1 the capitalization of the various SFR packages is not consistent with the corresponding capitalization of these SFR packages in subclause 6.1.

SuggestedRemedy

Make the capitalization of the various SFR packages in Figure 1 consistent with the corresponding capitalization of these SFR packages in subclause 6.1 in all four PPs.

Proposed Response Response Status W

PROPOSED ACCEPT.

CI All P SC 6.2 P 7 L 4 # 18

Smithson, Brian Ricoh

Comment Type E Comment Status X

[Kurth] Some additional explanation in the TOE model would be helpful.

SuggestedRemedy

In general for overall consistency the PP should explain that there are cases where user data and TSF data is generated outside of the TOE and transmitted to the TOE, as well as cases where user data and TSF data is generated and/or processed by the TOE and exported from the TOE. In those cases it is expected that sufficient security measures exist in the TOE environment that protect this data against unauthorized disclosure and modification. It should be explained that optionally the TOE can provide functionality to support this protection

Proposed Response Response Status O

CI PP-C SC P 7 L 9 # 4

aubry, carmen oce

Comment Type T Comment Status D

I think that there is a contradiction between:
 ""PP APPLICATION NOTEù In this environment, Normal Users are not necessarily identified or authenticated"" (page 7, line 9) and :
 ""All Users are identified and authenticated, and are authorized before being granted permission to perform TOE functions"" (page 10, line 29).

SuggestedRemedy

Use
 ""Administrators are identified and authenticated, and are authorized before being granted permission to manage TOE functions(it used to be like this in P2600.3-35a.pdf).

Proposed Response Response Status W

PROPOSED ACCEPT.

IEEE P2600 Hardcopy Device and System Security Comments

CI **All P** SC **6.3.2** P **7** L **10** # **47**
 Sukert, Alan Xerox

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

There is a minor but important difference between the definition of Object in this subclause and the corresponding definition of Object in Annex A. Here an object is defined as ""passive entities in the TOE, that contain or process information..."". Annex A (page 51, line 14) defines an object as ""passive entities in the TOE, that contain or receives information...""

SuggestedRemedy

Make the definition of an object consistent between subclause 6.3.2 and Annex A in all four PPs.

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

CI **PP-D** SC **6.3.2.2** P **7** L **14** # **115**
 Sukert, Alan Xerox

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

Since PP-D only has the SMI SFR package and thus only the F.SMI function, it is not clear why the other 5 functions need to be defined in Table 3 since they are never used in this PP.

SuggestedRemedy

Change Table 3 to only list the F.SMI function. You could put an APP Note if desired that tells the PP/ST author that the author can add these other functions if needed.

NOTE: If these functions are here because of the reference to the functions in the conformance claims in subclause 7, then instead of removing the unused functions in subclause 6.3.2.2 add an APP Note after Table 3 that indicates the unused functions are included in Table 3 because of the conformance claims in clause 7.

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

CI **PP-D** SC **6.3.2.3** P **8** L **1** # **116**
 Sukert, Alan Xerox

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

Since PP-D only has the SMI SFR package and thus only the +SMI attribute, it is not clear why the other 5 attributes need to be defined in Table 4 since they are never used in this PP.

SuggestedRemedy

Change Table 4 to only list the +SMI attribute. You could put an APP Note if desired that tells the PP/ST author that the author can add these other attributes if needed.

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

CI **PP-A** SC **6.3.2.1** P **8** L **3** # **76**
 Sukert, Alan Xerox

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

The definition of User Document Data in subclause 6.3.2.1 includes ""data created temporarily by the TOE while processing a document"". I noted that this aspect of User Document Data is not included in the additional sentence for the definition of User Document Data in Annex A, page 52, line 20.

A similar comment applies to PP-B (subclause 6.3.2.1, page 8, line 3 vs Annex A, page 52, line 23); PP-B (subclause 6.3.2.1, page 8, line 6 vs Annex A, page 47, line 23)

SuggestedRemedy

Add in the additional sentence for the definition of User Document Data in Annex A in all four PPs the concept that User Document Data includes data created temporarily by the TOE while processing a document.

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

Make sure definitions are consistent with the main P2600 standard.

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-A** SC **6.3.2.1** P **8** L **4** # **77**
 Sukert, Alan Xerox

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

The definition of User Function Data included in subclause 6.3.2.1 is very different from the definition of User Function Data ("the asset that consists of the information about a user's document or job to be processed by the HCD") in Annex A, page 52, line 22.

A similar comment applies to PP-B (subclause 6.3.2.1, page 8, line 4 vs. Annex A, page 52, line 26)

SuggestedRemedy

Make the definition of User Function Data consistent between subclause 6.3.2.1 and Annex A.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **All P** SC **6.3.2.2** P **8** L **7** # **49**
 Sukert, Alan Xerox

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

The definition of TSF Data has a big difference between subclause 6.3.2.2 and Annex A. Subclause 6.3.2.2 defines TSF data as "data created by and for the TOE and that might affect the operation of the TSF"; Annex A, page 52, line 3 defines TSF data as "data created by and for the TOE, that might affect the operation of the TOE".

I understand that as stated in subclause 6.2 for this PP TOE = TSF, but in Annex A the definitions of TOE and TSF are different, so in that sense the TSF definition in subclause 6.3.2.2 and Annex A are very different.

A similar comment applies to PP-B (subclause 6.3.2.2, page 8, line 7 vs Annex A, page 52, line 7); PP-C (subclause 6.3.2.2, page 8, line 7 vs. Annex A, page 47, line 7); PP-D (subclause 6.3.2.2, page 6, line 12 vs. Annex A, page 29, line 7)

SuggestedRemedy

Make the definition of TSF data in all four PPs consistent between subclause 6.3.2.2 and Annex A. You could add a note in subclause 6.3.2.2 about the TOE and TSF being the same for purposes of this PP if that will help.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **All P** SC **6.3.2.2** P **8** L **13** # **50**
 Sukert, Alan Xerox

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

The definition of TSF Confidential Data is not consistent between subclause 6.3.2.2 and Annex A. Subclause 6.3.2.2 says that for TSF confidential data both the disclosure and alteration of the data would effect the operational security of the TOE; in Annex A, page 52, line 4 is says that alteration of the data would effect the operational security of the TOE but disclosure of the data would be acceptable.

A similar comment applies to PP-B (subclause 6.3.2.2, page 8, line 13 vs. Annex A, page 52, line 8); PP-C (subclause 6.3.2.2, page 8, line 14 vs. Annex A, page 47, line 8); PP-D (subclause 6.3.2.2, page 7, line 1 vs. Annex A, page 29, line 8).

SuggestedRemedy

Make the definition of TSF Confidential Data in all four PPs consistent between subclause 6.3.2.2 and Annex A. Note: I believe in this case subclause 6.3.2.2 is correct and Annex A is not correct.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **All P** SC **6.3.2.2** P **8** L **15** # **56**
 Sukert, Alan Xerox

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

The APP Note in subclause 6.3.2.2 uses the acronym ST, but that acronym hasn't yet been defined here or in the text prior to its use here.

SuggestedRemedy

Define the acronym ST in all four PPs somewhere in the text before it's use in subclause 6.3.2.2 or define it here.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

IEEE P2600 Hardcopy Device and System Security Comments

CI All P SC 6.3.2.3 P 8 L 22 # 51
 Sukert, Alan Xerox

Comment Type T Comment Status D

We have defined a new term here - function - in the context of the TOE model underlying the PP. We should include a definition of this new term in Annex A also.

SuggestedRemedy

Add a definition for function in Annex A in all four PPs. Based on what is in subclause 6.3.2.3, I would suggest something like "Function: an entity in the TOE that performs processing, storage and transmission of data that may be present in the TOE."

Proposed Response Response Status W
 PROPOSED ACCEPT.

CI PP-A SC 6.3.2.3 P 9 L 1 # 78
 Sukert, Alan Xerox

Comment Type T Comment Status D

I noted an important inconsistency between the definition of the F.NVS function in Table 3 and the corresponding definition of the Nonvolatile storage package in subclause 4.2.6. Table 3 defines the F.NVS function as a function that "stores data in a nonvolatile storage device which can practicably be removed from the HCD by unauthorized people for analysis and recovery of data"; subclause 4.2.6 defines the Nonvolatile storage package as a package used for products that provide "nonvolatile storage of document data in a storage device which can practicably be removed from the HCD by unauthorized people for analysis and recovery of deleted data".

A similar comment applies to PP-B (Table 3, subclause 6.3.2.3, page 9, line 1 vs subclause 4.2.6, page 4); PP-C (Table 3, subclause 6.3.2.3, page 9, line 1 vs subclause 4.2.6, page 4)

SuggestedRemedy

Resolve the consistency as to what data is being analyzed in the definition of nonvolatile storage between subclauses 4.2.6 and 6.3.2.3.

Proposed Response Response Status W
 PROPOSED ACCEPT IN PRINCIPLE.

Will be addressed as part of the NVS SFR package re-write.

CI All P SC 8.1 P 9 L 4 # 126
 Chen, Nancy Oki Data

Comment Type E Comment Status D

Typos in Table 5.

SuggestedRemedy

Change "may" to "may be" in the description of T.DOC.DIS & T.DOC.ALT.

Proposed Response Response Status W
 PROPOSED ACCEPT.

CI All P SC 6.3.2.4 P 9 L 8 # 52
 Sukert, Alan Xerox

Comment Type T Comment Status D

In Table 4, the "DSR attribute is defined as data that is associated with "a document storage and retrieval job". There is no such thing as a document storage and retrieval job; rather as indicated in the definition of F.DSR in Table 3 this attribute should be associated with document storage and retrieval of a job for access by one or more subsequent jobs.

SuggestedRemedy

Change the definition of the +DSR attribute in Table 4 in all four PPs to something like "Indicates data that is associated with document storage and retrieval of a job".

Proposed Response Response Status W
 PROPOSED ACCEPT IN PRINCIPLE.

Will make the two references to a stored job for retrieval later consistent.

CI All P SC 6.3.4 P 9 L 14 # 53
 Sukert, Alan Xerox

Comment Type T Comment Status D

There is a difference between the definition of a channel in subclause 6.3.4 and in Annex A. Subclause 6.3.4 defines a channel as the "mechanisms through which information can be transferred into and out of the TOE"; Annex A, page 50, line 22 defines a channel as "Mechanisms through which data can be transferred into and out of the TOE".

SuggestedRemedy

Make the definition of channel in all four PPs consistent between subclause 6.3.4 and Annex A.

Proposed Response Response Status W
 PROPOSED ACCEPT.

IEEE P2600 Hardcopy Device and System Security Comments

CI All P SC 6.3.4 P 9 L 20 # 54
 Sukert, Alan Xerox

Comment Type T Comment Status D
 There is a difference between the definition of a Private Medium Interface in subclause 6.3.4 and in Annex A. Subclause 6.3.4 includes in the definition of a Private Medium Interface "operator controls and displays that are part of the TOE"; Annex A, page 51, line 24 includes in the definition of a Private Medium Interface "use physical input/display methods".

Note also that subclause 6.3.4 denotes this as 'Private Medium Interface' while Annex A denotes this as 'Private-medium interface'

SuggestedRemedy

Make the definition and title of Private Medium Interface in all four PPs consistent between subclause 6.3.4 and Annex A.

Proposed Response Response Status W
 PROPOSED ACCEPT.

CI All P SC 6.3.2.4 P 9 L 38 # 136
 Chen, Nancy Oki Data

Comment Type T Comment Status D
 (1) The identity of function (i.e. PRT, SCN,) is defined as a "security attribute" to distinguish the difference in the required SFRs among the different functions. However, these security attributes are actually used as the top-level designation of all security attributes that are associated with the indicated function governed by an access control rule that need to be evaluated. The security attributes that need to be evaluated according to an access control rule may include but not limited to the identity, role and permission rights of the subject requesting to operate the function.
 (2) Table 4 should be named "Security Attributes" to be clearer than just "Attributes" and be consistent with the section title.
 (3) The word "data" in the description of each security attribute in the table should be clarified as "security attribute data".

SuggestedRemedy

- (1) Clarify the term "security attributes" at line 4 as "the top-level designation of all security attributes that are associated with the indicated function governed by an access control rule that need to be evaluated".
- (2) Change the name of Table 4 to "Security Attributes".
- (3) Change "data" in the table to "security attribute data".

Proposed Response Response Status W
 PROPOSED ACCEPT IN PRINCIPLE.

Alternately, the Section title for 6.3.2.4 should be changed to Attributes from Security Attributes.

CI All P SC 6.3.4 P 10 L 6 # 55
 Sukert, Alan Xerox

Comment Type E Comment Status D
 Minor grammatical error -- says "...transferring User Document Data into of the TOE..."; should be "...transferring User Document Data into the TOE..."

Note: PP-B - subclause 6.3.4, page 10, line 6
 PP-C - subclause 6.3.4, page 10, line 6
 PP-D - subclause 6.3.4, page 8, line 20

SuggestedRemedy

Correct as indicated above.

Proposed Response Response Status W
 PROPOSED ACCEPT.

CI PP-D SC 7.4 P 10 L 26 # 117
 Sukert, Alan Xerox

Comment Type T Comment Status D
 The APP Note on this line refers to a Family of PPs; we no longer are using that approach. Is this APP Note even needed anymore?

SuggestedRemedy

Either modify the App Note on this line to refer to the packages approach we are now using to define this PP or remove it entirely if not needed.

Proposed Response Response Status W
 PROPOSED ACCEPT.

IEEE P2600 Hardcopy Device and System Security Comments

CI All P SC 6.4 P 10 L 32 # 57
 Sukert, Alan Xerox

Comment Type T Comment Status D

In comparing the list of major security features in Version 36c-proto with previous versions, I noted that in the previous versions it was indicated that User Function Data was only protected from unauthorized alteration, while now it is protected from both unauthorized disclosure and alteration.

I wanted to make sure that this change was done knowingly and not just a mistake in transferring from the prior version. Note also that subclause 8.1 only includes the threat for unauthorized alteration of User Function Data and not a threat for unauthorized disclosure of User Function Data.

SuggestedRemedy

Make sure the statement in Item b in subclause 6.4 is correct as stated in all four PPs.

Proposed Response Response Status W

PROPOSED ACCEPT.

Remove "disclosure" text.

CI All P SC 6.4 P 10 L 32 # 27
 Smithson, Brian Ricoh

Comment Type T Comment Status D

[Kurth] There is another major security feature.

SuggestedRemedy

Add the following security feature: Administrators can restrict the use of functions of the TOE to a subset of the users of the TOE.

Proposed Response Response Status W

PROPOSED REJECT.

Check with [Kurth] about the impact of this and what granularity of control is implied by this. Consider limiting the scope to particular Operating Environments.

CI All P SC 7.4 P 11 L 19 # 28
 Smithson, Brian Ricoh

Comment Type T Comment Status D

[Kurth] Clarification of the conformance rules.

SuggestedRemedy

Point c): add ""and claim compliance with the SFR package(s) associated with the function(s)"".

Proposed Response Response Status W

PROPOSED ACCEPT.

CI All P SC 7.4 P 11 L 20 # 58
 Sukert, Alan Xerox

Comment Type E Comment Status D

The APP Note in subclause 7.4 uses the acronym PP, but that acronym hasn't yet been defined here or in the text prior to its use here.

Note that for PP-D this is on page 10, line 20

SuggestedRemedy

Define the acronym PP in all four PPs somewhere in the text before it's use in subclause 7.4 or define it here.

Proposed Response Response Status W

PROPOSED ACCEPT.

CI PP-C SC 8.1 P 12 L 3 # 107
 Sukert, Alan Xerox

Comment Type E Comment Status D

Paragraph reference error on this line needs to be corrected.

SuggestedRemedy

Include the proper paragraph number reference on this line.

Proposed Response Response Status W

PROPOSED ACCEPT.

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-C** SC **8.1** P **12** L **4** # **134**
 Chen, Nancy Oki Data

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

Would like to have a more descriptive name/label for the threat. Here the threat is on the disclosure of RESIDUAL User Document Data. It is not the same threat (on all User Document Data) as described in PP-A or PP-B.

SuggestedRemedy

- (1) How about change T.DOC.NO_DIS to T.DOC_RES.NO_DIS?
- (2) Need to do a global change to change all occurrences in the document.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

Will be addressed as part of the NVS SFR package re-write.

Cl **PP-D** SC **9.1** P **12** L **4** # **118**
 Sukert, Alan Xerox

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

It is not clear why the objective around require admin identification and authorization is titled O.USER.AUTHORIZED - should it be titled O.ADMIN.AUTHORIZED to reflect what the true objective is here.

Same comment applies to the P.USER.AUTHORIZATION OSP in subclause 8.2, Table 6, page 11, line 11.

SuggestedRemedy

Change O.USER.AUTHORIZED and P.USER.AUITHORIZED to O.ADMIN.AUTHORIZED and P.ADMIN.AUITHORIZED, respectively in subclauses 8.2 and 9.1 and everywhere else this objective and OSP are listed.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **PP-D** SC **9.1** P **12** L **4** # **119**
 Sukert, Alan Xerox

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

This is a comment against Version 35a that I think applies here. The O.USER.AUTHORIZED objective indicates that the admin will be authorized in accordance with security policies. It really should be in accordance with security policies and procedures.

Also, you want the admin to be be able to manage the TOE, not use the TOE.

SuggestedRemedy

Change the description of the O.USER.AUTHORIZED objective to read "...authorized in accordance with security policies and procedures before allowing them to manage the TOE".

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **PP-C** SC **8.1** P **12** L **4** # **108**
 Sukert, Alan Xerox

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

- In Table 5 for the T.DOC.DIS threat, there are two issues: in the definition
1. The definition for PP-C indicates that this threat is for User Document Data that has been deleted; I noted that the corresponding threat definition in PP-A and PP-B don't restrict the threat to deleted data. Note a similar comment applies to the corresponding O.DOC.NO_DIS objective in Table 9 (subclause 9.1, page 14, line 4)
 2. There is a grammatical error - states "...may disclosed to unauthorized persons"; should be "...may be disclosed to unauthorized persons."

SuggestedRemedy

1. Make sure that the T.DOC.DIS threat (and by implication the O.DOC_NO_DIS threat) is supposed to apply only when UDD is deleted.
2. Correct the indicated grammatical error.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

Address as part of the NVS SFR package re-write. See comment 134.

IEEE P2600 Hardcopy Device and System Security Comments

Cl **All P** SC **8.2** P **12** L **11** # **59**
 Sukert, Alan Xerox

Comment Type **T** Comment Status **D**
 In the definition of the P.CHANNEL_MANAGEMENT OSP in Table 7, it is not clear what ""security policies' channel operation is to be managed in accordance with - is it the security policies of the TOE owner, for example, or some other set of security policies.

Same comment applies to the O.CHANNELS.MANAGED security objective in subclause 9.1, page 14, line 4 (Table 9).

SuggestedRemedy
 Clarify what security policies channel operation must comply with in the definition of the P.CHANNEL_MANAGEMENT OSP in Table 7 and the O.CHANNELS.MANAGED objective in Table 9 in all four PPs.

Proposed Response Response Status **W**
 PROPOSED ACCEPT.
 Policy of the TOE owner.

Cl **All P** SC **8.2** P **12** L **11** # **38**
 Smithson, Brian Ricoh

Comment Type **T** Comment Status **D**
 We have been unable to find a suitable PP solution to assure that fax-to-network bridging cannot occur and that network services cannot be misused to attack a customer network. Fax-to-network bridging is not a real vulnerability in modern HCDs, and misuse of network services is more appropriately handled by CC vulnerability assessment. See ""http://grouper.ieee.org/groups/2600/presentations/Longmont/no-smi-mediation.pdf"" for explanation and rationale.

SuggestedRemedy
 Remove P.CHANNEL.MAANGEMENT and O.CHANNELS.MANAGED from the PP, and FMT_SMF.1 from the SMI package.

Proposed Response Response Status **W**
 PROPOSED REJECT.

Cl **PP-D** SC **9.4** P **12** L **14** # **120**
 Sukert, Alan Xerox

Comment Type **T** Comment Status **D**
 Since P.USER.AUTHORIZATION and O.USER.AUTHORIZED have been modified to reflect admin management of the TOE and not user usage, it is not clear why objective OE.USER.AUTHORIZED was not similarly changed and still refers to users authorized to use the TOE; as it now reads OE.USER.AUTHORIZED is inconsistent with the other two user-related OSPs and assumptions.

SuggestedRemedy
 Modify the wording in OE.USER.AUTHORIZED to be consistent with the changes made in P.USER.AUTHORIZATION and O.USER.AUTHORIZED - something like ""The TOE Owner shall grant permission to Administrators to be authorized to manage the TOE according to the security policies and procedures of their organizations.""

Might consider changing the title as was suggested for P.USER.AUTHORIZATION and O.USER.AUTHORIZED.

Proposed Response Response Status **W**
 PROPOSED ACCEPT.
 Remedy is correct, comment is a little off.

Cl **PP-C** SC **9.1** P **14** L **4** # **135**
 Chen, Nancy Oki Data

Comment Type **T** Comment Status **D**
 Would like to have a more descriptive name/label for the objective O.DOC.NO_DIS. Here the objective is on the protection of RESIDUAL User Document Data. It is not the same objective (protection of all User Document Data) as described in PP-A or PP-B.

SuggestedRemedy
 (1) How about change O.DOC.NO_DIS to O.DOC_RES.NO_DIS?
 (2) Need a global change to replace all occurrences in the document.

Proposed Response Response Status **W**
 PROPOSED ACCEPT IN PRINCIPLE.
 See 134 Comment response.

IEEE P2600 Hardcopy Device and System Security Comments

Cl **All P** SC **9.3** P **14** L **10** # **127**

Chen, Nancy Oki Data

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

Would like to have more descriptive name for OE.AUDIT.STORAGE & OE.AUDIT.ACCESS to match the description of these two objectives.

SuggestedRemedy

How about OE.EXPORTED_AUDIT.PROTECTED, and OE.EXPORTED_AUDIT.READABILITY?

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

Find a better name, maybe not the suggested remedy.

Cl **PP-A** SC **9.3** P **14** L **10** # **79**

Sukert, Alan Xerox

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

In Table 10, the definition of objective OE.AUDIT.STORAGE talks about exporting the audit records to another trusted IT 'device' while objective OE.AUDIT.ACCESS talks about exporting the audit records to another trusted IT 'product'. The two should be the same.

This same comment applies to PP-B (Table 10, subclause 9.3, page 14, line 10) and PP-C (Table 10, subclause 9.3, page 14, line 10)

SuggestedRemedy

Make what the audit records are exported to the same between the OE.AUDIT.STORAGE and OE.AUDIT.ACCESS objectives in subclause 9.3, Table 10.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

Use terminology from CC (product).

Cl **PP-A** SC **9.3** P **14** L **10** # **80**

Sukert, Alan Xerox

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

In the definition of the OE.AUDIT.ACCESS security objective, it is stated that the TOE owner ensures the records can be analyzed by authorized persons but doesn't preclude anyone else from analyzing these records. This objective should preclude anyone but an authorized person from analyzing these records.

This same comment applies to PP-B (Table 10, subclause 9.3, page 14, line 10) and PP-C (Table 10, subclause 9.3, page 14, line 10)

SuggestedRemedy

Modify the definition of the OE.AUDIT.ACCESS objective to read "...the TOE Owner shall ensure that those records can be analyzed only by authorized persons in order to..."

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **PP-D** SC **11.4** P **14** L **15** # **121**

Sukert, Alan Xerox

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

Since there are no objectives or threats associated with User Data mentioned in subclause 8, why would there be a need to define a Common Access Control SFP around User Document Data in subclause 11.4 - it seems inconsistent with subclause 8. Further, there are no class of Users defined in subclause 6.3.1 except for the administrator, so again why would Table 12 specify a U.USER subject for access to user documents.

SuggestedRemedy

Clarify the need for a Common Access Control SFP in subclause 11.4. If it is needed, make sure it reflects the TOE model and associated threats and objectives for PP-D specified in subclauses 6 and 8.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **PP-D** SC **11.4** P **14** L **18** # **122**

Sukert, Alan Xerox

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

The references to Table 15 on this line and on lines 22 and 24 I believe should be to Table 12.

SuggestedRemedy

Reference the proper table in the lines indicated above.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-D** SC **11.4** P **15** L **4** # **123**
 Sukert, Alan Xerox

Comment Type **T** Comment Status **D**
 The APP Note on this line indicates that FDP_ACC.1 fulfills O.DOC.NO_DIS. However, O.DOC.NO_DIS is not listed as an objective in subclause 9.1, Table 8. A similar comment applies to subclause 11.4, page 15, line 1 for the FDP_RIP.1 SFR.

Note that O.DOC.NO_DIS is included in Table 14 in subclause 11.12.

SuggestedRemedy

Resolve the inconsistency between subclauses 9.1 and 11.4 as to whether O.DOC.NO_DIS is an objective for PP-D.

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

Fix the APP Note.

Cl **All P** SC **9.4** P **15** L **5** # **60**
 Sukert, Alan Xerox

Comment Type **E** Comment Status **D**
 Minor error here - text refers to the ""SMI TOE""; should only refer to the ""TOE"".

In PP-D it is on page 12, line 13

SuggestedRemedy

Revise subclause 9.4, line 5 in all four PPs to read ""...environment for the TOE.""

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

Cl **All P** SC **9.4** P **15** L **6** # **35**
 Smithson, Brian Ricoh

Comment Type **T** Comment Status **D**
 OE.ADMIN.AUTHORIZED is not needed -- it is a remnant from the FoPP in which there was a separate OSP for admin authorization.

SuggestedRemedy

Remove OE.ADMIN.AUTHORIZED from table 11.

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

Cl **PP-A** SC **9.5** P **15** L **10** # **81**
 Sukert, Alan Xerox

Comment Type **T** Comment Status **D**
 The OE.ADMIN.AUTHORIZED objective listed in Table 11 are not included in the security objectives rationale in Table 12.

In a related comment, I noted that in subclause 8.2, Table 7 there is no P.ADMIN.AUTHORIZATION OSP that would be mapped to this objective as there was in previous versions of this PP.

SuggestedRemedy

Include the OE.ADMIN.AUTHORIZED objective in the security objectives rationale in Table 12. If it is to be included, add the P.ADMIN.AUTHORIZATION OSP to subclause 8.2, Table 7.

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

See Comment 35 Response.

Cl **PP-A** SC **11.1** P **17** L **4** # **82**
 Sukert, Alan Xerox

Comment Type **T** Comment Status **D**
 Two comments on the APP Note on line 4 in subclause 11.1. First it essentially duplicates the APP Note in subclause 9.3 - I'm not sure why the same APP Note is needed in both places.

Having said that I noted that the APP Note in subclause 9.3 references both objectives OE.AUDIT.STORAGE and OE.AUDIT.ACCESS, while the corresponding App Note in subclause 11.1 only references objective OE.AUDIT.STORAGE.

Note that the APP Note in line 9 is repeated in both subclauses 9.3 and 11.1 also.

Same comment applies to PP-B and PP-C (same subclauses, pages and lines)

SuggestedRemedy

Determine if the same APP Notes are needed in both subclause 9.3 and 11.1. If so, make sure the two APP Notes are the same.

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

Make consistent.

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-A** SC 11.1 P 17 L 30 # 83
 Sukert, Alan Xerox

Comment Type **E** Comment Status **D**
 Small grammatical error - this line states "...required by Table 13 and the any audit level specified..."; should state "...required by Table 13 and any audit level specified..."

Same comment applies to PP-B and PP-C (same pages and lines)

SuggestedRemedy

Correct the grammatical error as indicated above.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

"and by any audit level specified.."

Cl **PP-B** SC 11.1 P 18 L 7 # 100
 Sukert, Alan Xerox

Comment Type **E** Comment Status **D**
 There is a table number reference error on this line.

SuggestedRemedy

Provide the proper table number reference in the indicated line.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **All P** SC 11.1 P 18 L 9 # 36
 Smithson, Brian Ricoh

Comment Type **T** Comment Status **D**
 The events listed in the "Auditable event" column of Tables 13 and 14 may not be completely consistent with CC definitions (in cases where Basic or Minimal audit level is also specified).

SuggestedRemedy

Check the contents of that column against the actual CC audit recommendations and make sure they are consistent.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **PP-A** SC 11.1 P 18 L 12 # 84
 Sukert, Alan Xerox

Comment Type **T** Comment Status **D**
 Table 14 includes recommended audit data for SFR FIA_AFL.1. However, SFR FIA_AFL.1 is not included in the FIA SFRs described in subclause 11.5.

SuggestedRemedy

Either include SFR FIA_AFL.1 in subclause 11.5 or delete its reference from Table 14. Note that if the reference to FIA_AFL.1 is deleted in Table 14 it also has to be removed from the APP Notes in subclause 11.1, page 18, lines 15 and 25.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Delete from table and App Notes.

Cl **All P** SC 11.4 P 19 L 8 # 61
 Sukert, Alan Xerox

Comment Type **T** Comment Status **D**
 Table 15 introduces the new acronyms D.DOC and D.FUNC. In the new TOE model it is not clear to me at all what these acronyms stand for, which makes understanding whether the Common Access Control SFP is correct very difficult. I'm making some assumptions based on previous PP versions - that D.DOC means User Document Data and D.FUNC means User Function Data - but these might not be correct assumptions.

Same comment applies to PP-B for both D.DOC and D.FUNC; to PP-C for only D.DOC and to PP-D for D.DOC.

SuggestedRemedy

Please define here or in subclause 6 what D.DOC and D.FUNC stand for in all four PPs.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

Find a place to define the shorthand notation.

IEEE P2600 Hardcopy Device and System Security Comments

Cl **All P** SC 11.4 P 19 L 27 # 17
 Smithson, Brian Ricoh

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

FDP_ACC.1 is also a dependency of FMT_MSA.1, but is not indicated as such in the app note.

SuggestedRemedy

Add the dependency to the app note.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **All P** SC 11.4 P 20 L 11 # 128
 Chen, Nancy Oki Data

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

The FDP_ACF.1.1 cited "the indicated security attributes in Table 15" which are "any" according to the Table. "any" here means any of these security attributes: +PRT, +SCN, +FAX, +CPY, +DSR, +SMI. These attributes only tell evaluators which type of D.DOC shall be evaluated for the associated Access Control SFP rule. However, according to the rules in the Table, there shall be other security attributes associated with U.ADMINISTRATOR or U.NORMAL or U.USER that are required to be evaluated according to the specified rules.

SuggestedRemedy

Make Application Note to clarify this point accordingly.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

Find appropriate descriptive work to replace the word "any". (check with [Kurth])

Cl **PP-A** SC 11.4 P 20 L 18 # 85
 Sukert, Alan Xerox

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

I understand that in the context of the PP User = Subject. However, the modified SFR FDP_ACF.1.2 states that the TSF shall enforce the following rules - rules specified in the Common Access Control SFP in table 15 governing access among Users and controlled objects..."

I note that Table 15 lists subjects, not users, as a column heading. From a PP/ST Author perspective, to help them understand better what to do, for consistency with SFR FDP_ACF.1.2 as originally stated in CC Part 2 and for consistency with Table 15, this SFR should refer to Subjects instead of Users.

Same comment applies to PP-B and PP-C

SuggestedRemedy

Revise SFR FDP_ACF.1.2 to state that the TSF shall enforce the following rules - rules specified in the Common Access Control SFP in table 15 governing access among Subjects and controlled objects..."

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **PP-A** SC 11.4 P 20 L 34 # 129
 Chen, Nancy Oki Data

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

Since we are also protecting D.FUNC from being altered, D.FUNC shall be added in the object assignment of FDP_RIP.1.1.

SuggestedRemedy

Add D.FUNC in the object assignment of FDP_RIP.1.1.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-A** SC 11.4 P 20 L 35 # 86

Sukert, Alan Xerox

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

Missing comma after O.DOC.NO_DIS on this line.

Same comment applies to PP-B (subclause 11.4, page 20, line 31).

SuggestedRemedy

Revise the APP Note to read ""FDP_RIP,1 is a principal SFR to fulfil O.DOC.NO_DIS, O.DOC.NO_ALT, and O.FUNC.NO_ALT.""

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **All P** SC 11.5 P 21 L 24 # 62

Sukert, Alan Xerox

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

It is not clear why the APP Note on this line is needed because it duplicates the wording in the second sentence of the App Note in subclause 11.5, page 21, line 22.

Same comment applies to PP-B, PP-C and PP-D.

SuggestedRemedy

Clarify in all four PPs the need for the App Note on subclause 11.5, page 21, line 24. Note"" I'm wondering if this APP Note should say ""If user authentication is performed externally, then...""

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

Second sentence of the first APP Note needs to be removed.

Cl **All P** SC 11.5 P 21 L 29 # 73

Sukert, Alan Xerox

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

The APP Note on this page indicates that FIA_UAU.1 is a principal SFR to fulfill O.USER.AUTHORIZED. It is also a principal SFR to fulfill O.CHANNELS.MANAGED.

Same comment applies to PP-B and PP-C and PP-D.

SuggestedRemedy

Indicate in this App Note in all four PPs that FIA_UAU.1 is a principal SFR that fulfills both O.USER.AUTHORIZED and O.CHANNELS.MANAGED.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **All P** SC 11.5 P 21 L 29 # 63

Sukert, Alan Xerox

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

The APP Note on this line indicates that FIA_UAU.1 is a dependency of FIA_AFL.1 and FIA.UAU.7. However, neither SFR is described in subclause 11.5.

Same comment for PP-B (page 21, line 19); PP-C (page 21, line 18); PP-D (page 16, line 26)

SuggestedRemedy

Modify in all four PPs the APP Note on subclause 11.5, page 21, line 29 to read ""FIA_UAU.1 is a principal SFR to fulfill O.USER.AUTHORIZED.""

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **PP-D** SC 11.12 P 22 L 1 # 125

Sukert, Alan Xerox

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

In Table 15, it is indicated that FMT_MTD.1 is the principal SFR that fulfills O.PROT.NO_ALT and O.CONF_NO_ALT. However, the stated purpose for this SFR in the table for these objectives is ""Prevents disclosure by restricting access""; there is no mention of preventing any type of alteration.

SuggestedRemedy

Modify the purpose for the FMT_MTD.1 SFR in Table 15 to read ""Prevents disclosure and alteration by restricting access"".

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

"Prevents disclosure or alteration by restricting access"

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-D** SC **11.12** P **22** L **1** # **124**
 Sukert, Alan Xerox

Comment Type **T** Comment Status **D**
 In Table 15, in the discussion for O.USER.AUTHORIZED the description states
 ""Authorization of Users and Administrators to use the TOE"". However,
 O.USER.AUTHORIZED only covers users (the administrator part was removed because it
 is now an objective of the IT environment).

SuggestedRemedy

Change the description for O.USER.AUTHORIZED in the indicates table to read
 ""Authorization of Users to use the TOE"".

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

Should be authorization of admins to manage the TOE.

Cl **All P** SC **11.5** P **22** L **14** # **64**
 Sukert, Alan Xerox

Comment Type **T** Comment Status **D**
 The APP Note on this line indicates that FIA_UID.1 is a dependency of FIA.UAU.7.
 However, this SFR is not described in subclause 11.5.

Same comment for PP-B (page 22, line 7); PP-C (page 21, line 23; PP-D (page 17, line 20)

SuggestedRemedy

Modify in all four PPs the APP Note on subclause 11.5, page 22, line 14 to read
 ""FIA_UAU.1 is a principal SFR to fulfill O.USER.AUTHORIZED and is a dependency of
 FIA_UAU.1, FAU_GEN.2 and FMT_SMR.1.""

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

Cl **All P** SC **11.5** P **22** L **29** # **65**
 Sukert, Alan Xerox

Comment Type **T** Comment Status **D**
 The APP Note on this line says that FIA_USB.1 is a supporting SFR that fulfills
 O.USER.AUTHORIZED. However, subclause 11.12, page 26, line 8 (Table 17) indicates
 that FIA_USB.1 is a principal SFR that fulfills O.USER.AUTHORIZED.

Same comment for PP-B (page 22, line 21); PP-C (page 22, line 19); PP-D (page 17, line
 34)

SuggestedRemedy

Resolve in all four PPs the inconsistency between subclauses 11.5 and 11.12 as to
 whether FIA_USB is a principal or supporting SFR for O.USER.AUTHORIZED.

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

Determine which one.

IEEE P2600 Hardcopy Device and System Security Comments

CI All P SC 11.6 P 23 L 3 # 66
 Sukert, Alan Xerox

Comment Type T Comment Status D

FMT_MSA.1.1 as stated in CC Part 2 mentions both access control and information flow control SFPs. Since the Common SFRs only discuss access control SFPs (there are no information flow control SFPs) that would suggest that FMT_MSA.1.1 should be altered to reflect the SFPs for the Common SFRs, just as was done in previous versions of this PP. The altering would also reflect a reference to the Common Access Control SFP similar to what is done in other SFRs like FDP_ACF.1.1.

Note that a similar comment applies to FMT_MSA.1 on line 13 on page 23.

Same comment applies to applicable SFRs in subclause 11.6 in PP-B, PP-C and PP-D.

SuggestedRemedy

Alter FMT_MSA.1.1 and FMT_MSA.3.1 in all four PPs to read something like the following:

FMT_MSA.1.1(b) The TSF shall enforce the Common Access Control SFP to restrict the ability to [selection: change_default, query, modify, delete, [assignment: other operations]] the security attributes [assignment: list of security attributes] to [assignment: the authorised identified roles].

FMT_MSA.3.1(b) The TSF shall enforce the Common Access Control SFP to provide [selection: choose one of: restrictive, permissive, [assignment: other property]] default values for security attributes that are used to enforce the SFP.

Probably would want to alter the other selections and assignments appropriately on both SFRs - I'm just not sure what those changes should be.

Proposed Response Response Status W

PROPOSED ACCEPT IN PRINCIPLE.

Specify the common access control SFP but leave open assignment for others.

CI All P SC 11.6 P 23 L 31 # 68
 Sukert, Alan Xerox

Comment Type T Comment Status D

The description of FMT_MTD.1.1(c) uses the term ""user profile"". That term is not defined anywhere previously in the description of the common SFRs for PP-A, so it is not clear what is meant by a ""user profile"" in this context.

Same comment applies to PP-B, subclause 11.6, page 23, line 32; PP-C, subclause 11.6, page 23, line 31; PP-D, subclause 11.6, page 19, line 7.

SuggestedRemedy

Define in all four PPs what is meant by a ""user profile"" in the context of the definition of FMT_MTD.1 in PP-A.

Proposed Response Response Status W

PROPOSED ACCEPT IN PRINCIPLE.

Add a description of what is meant by user profile and what is expected of the ST author.

CI All P SC 11.6 P 23 L 7 # 29
 Smithson, Brian Ricoh

Comment Type T Comment Status D

[Kurth] Clarification of FMT_MSA.1

SuggestedRemedy

Add an application note stating that there are only a few mandatory security attributes for subjects and objects defined in the PP. For those, the PP does not make any restriction on how they can be managed. The author of a ST that claims compliance to this PP has to define the management policy for the security attributes. The PP also allows to instantiate ""none"" for the ""authorized identified roles"" thereby allowing a ST to state that some management functionality for security attributes (like changing or deleting the security attribute) is not allowed for any user or administrator.

Proposed Response Response Status W

PROPOSED ACCEPT.

IEEE P2600 Hardcopy Device and System Security Comments

CI **All P** SC 11.6 P 23 L 19 # 30
 Smithson, Brian Ricoh

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

[Kurth] Clarification of FMT_MSA.3

SuggestedRemedy

Add an application note stating that user and object security attributes are usually initialized when the user or object is created. The PP does not restrict the way security attributes are initialized, leaving it to the ST author to describe the product's policy for this.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

CI **All P** SC 11.6 P 23 L 30 # 31
 Smithson, Brian Ricoh

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

[Kurth] Correction to how FMT_MTD.1.1 is expressed.

SuggestedRemedy

To be correct, this needs to be rephrased to:
 The TSF shall restrict the ability to create D.PROT data to [selection: U.ADMINISTRATOR, U.NORMAL for data associated with his/her own jobs, [assignment: other authorized identified roles except U.ADMINISTRATOR, U.NORMAL]].
 An application note should explain that multiple selections are allowed, but the role ""none"" can not be selected with other roles.

In a similar way also FMT_MTD.1.1(b), FMT.1.1(c), and FMT_MTD.1.1(d) should be modified.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

CI **All P** SC 11.6 P 23 L 30 # 67
 Sukert, Alan Xerox

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

The definition for SFR FMT_MTD.1.1(a) used the data object D.PROT. However, this data object is not defined anywhere in PP-A prior to its use here.

Note that a similar comment applies to the use of the data object D.CONF in the definition of SFR FMT_MTD.1.1(c) in subclause 11.6, page 24, line 1.

Same comment applies to the applicable SFRs in subclause 11.6 in PP-B, PP-C and PP-D .

SuggestedRemedy

Define in all four PPs the data objects D.PROT and D.CONF in all four PPs prior to their use in the FMT_MTD SFR descriptions in subclause 11.6.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

CI **All P** SC 11.8 P 25 L 8 # 130
 Chen, Nancy Oki Data

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

Should we allow TOE to obtain time stamps from internal realtime clock or external reliable time service?

SuggestedRemedy

If so, add Application Note to make clear that time stamps can be generated by TOE internally, obtained from a external reliable global time source, or allowing both in which case the two should be provided as separate mode of operation.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

Refer to both as "reliable" time sources.

Also add an App Note or assumption for the environment for the external time source in the case an external time source is used.

IEEE P2600 Hardcopy Device and System Security Comments

CI **PP-B** SC **11.10** P **25** L **28** # **101**
 Sukert, Alan Xerox

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

This APP Note states that FTA_SSL.3 is a principal SFR to fulfill O.USER.AUTHORIZED. However, subclause 11.12, page 26, line 6 (Table 18) indicates that FTA_SSL.3 is also a principal SFR for O.CHANNELS.MANAGED.

Same comment applies to PP-C (subclause 11.10, page 25, line 28 vs. subclause 11.12, page 26, line 5) and PP-D (subclause 11.10, page 21, line 7 vs. subclause 11.12, page 22, line 1) .

SuggestedRemedy

Indicate in subclause 11.10 that FTA_SSL.3 SFR is a principal SFR for both O.USER.AUTHORIZED and O.CHANNELS.MANAGED.

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

CI **PP-A** SC **11.10** P **25** L **30** # **87**
 Sukert, Alan Xerox

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

This APP Note states that FTA_SSL.3 is a principal SFR to fulfill O.USER.AUTHORIZED and O.ADMIN.AUTHORIZED. However, subclause 11.12, page 26, line 8 (Table 17) indicates that FTA_SSL.3 is a principal SFR for O.USER.AUTHORIZED and O.CHANNELS.MANAGED.

SuggestedRemedy

Resolve the inconsistency between subclauses 11.10 and 11.12 as to what objectives the FTA_SSL.3 SFR is a principal SFR for.

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

CI **All P** SC **11.12** P **27** L L # **1**
 aubry, carmen oce

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

I don't think that FIA SFRs are sufficient in order to cover O.CHANNELS.MANAGED. For instance, if we want to prevent bridging between telephone line and the network, I don't think that user authentication is sufficient. I would rather expect some form of access control (resulting from some architectural decisions). As bridging must be made explicit, not necessarily prohibited, an access control policy would be appropriate.

SuggestedRemedy

The TOE should control data flow. Use FDP_ACC.1&FDP_ACF.1 or FDP_IFC.1&FDP_IFF.1 in order to express this requirement.

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

[Kurth] has a mechanism to address this comment.

CI **PP-A** SC **11.12** P **27** L **1** # **98**
 Sukert, Alan Xerox

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

In Table 18, it is indicated that FMT_MTD.1 is the principal SFR that fulfills O.PROT.NO_ALT and O.CONF_NO_ALT. However, the stated purpose for this SFR in the table for these objectives is "Prevents disclosure by restricting access"; there is no mention of preventing any type of alteration.

I noted also that except for the SMI SFR package there is no other place in P2600.1 where the protection of TSF data from alteration is even brought up, so it is important that it be included here so it applies to all the other SFR packages by default.

Same comment applies to PP-B (Table 18, page 27, line 1).

SuggestedRemedy

Modify the purpose for the FMT_MTD.1 SFR in Table 18 to read "Prevents disclosure and alteration by restricting access".

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

See comment 125 response.

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-C** SC **11.12** P **27** L **1** # **113**
 Sukert, Alan Xerox

Comment Type **T** *Comment Status* **D**
 In Table 18, in the discussion for O.USER.AUTHORIZED the description states
 ""Authorization of Users and Administrators to use the TOE"". However,
 O.USER.AUTHORIZED only covers users (the administrator part was removed because it
 is now an objective of the IT environment).

The comment also applies to Table 21 (subclause 12.4, page 29, line 22); Table 23
 (subclause 13.3, page 31, line 22); Table 26 (subclause 14.3, page 33, line 20); Table 30
 (subclause 15.3, page 35, line 22) and Table 33 (subclause 16.3, page 37, line 20).

SuggestedRemedy

Change the description for O.USER.AUTHORIZED in the indicates tables to read
 ""Authorization of Users to use the TOE"".

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

See comment 94 response.

Cl **PP-B** SC **11.12** P **27** L **1** # **102**
 Sukert, Alan Xerox

Comment Type **T** *Comment Status* **D**
 In Table 18, in the discussion for O.USER.AUTHORIZED the description states
 ""Authorization of Users and Administrators to use the TOE"". However,
 O.USER.AUTHORIZED only covers users (the administrator part was removed because it
 is now an objective of the IT environment).

The comment also applies to Table 21 (subclause 12.4, page 30, line 6); Table 24
 (subclause 13.3, page 33, line 1); Table 27 (subclause 14.3, page 36, line 1); Table 30
 (subclause 15.3, page 39, line 1) and Table 33 (subclause 16.3, page 42, line 2).

SuggestedRemedy

Change the description for O.USER.AUTHORIZED in the indicates tables to read
 ""Authorization of Users to use the TOE"".

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

See comment 94 response.

Cl **PP-A** SC **11.12** P **27** L **1** # **94**
 Sukert, Alan Xerox

Comment Type **T** *Comment Status* **D**
 In Table 18, in the discussion for O.USER.AUTHORIZED the description states
 ""Authorization of Users and Administrators to use the TOE"". However,
 O.USER.AUTHORIZED only covers users (the administrator part was removed because it
 is now an objective of the IT environment).

The comment also applies to Table 21 (subclause 12.4, page 30, line 6); Table 23
 (subclause 13.3, page 32, line 28); Table 26 (subclause 14.3, page 36, line 1); Table 29
 (subclause 15.3, page 39, line 28) and Table 33 (subclause 16.3, page 42, line 2).

SuggestedRemedy

Change the description for O.USER.AUTHORIZED in the indicates tables to read
 ""Authorization of Users to use the TOE"".

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

Add a parenthetical (Normal and Admin) descriptors when the reserved term User is used.

Cl **All P** SC **12.2** P **28** L **10** # **32**
 Smithson, Brian Ricoh

Comment Type **T** *Comment Status* **D**
 [Kurth] Need to add management functions to support access control of executing functions.

SuggestedRemedy

The access control rule specified in the first row of table 19 implies a management policy
 allowing the administrator to define the users allowed to use the functionality. This implies
 that management SFRs need to be added:
 FMT_MTD.1 to define that the administrator is allowed to define, modify and delete
 authorizations to use the print function and FMT_SMF.1 to define the management function
 for managing access rights to the print function.

[These would be inserted as a new clause 12.4 Class FMT]

This statement applies also to the SCN, CPY, FAX, and DSR packages.

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

Discuss the impact to a product requirement relating to specific roles. See Comment 27.

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-A** SC **12.2** P **28** L **10** # **131**
 Chen, Nancy Oki Data

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

In Table 19, PRT Access Control Table, Normal Users are allowed to execute PRT function only when they are authorized by Administrator. The security attribute of the normal user need to be evaluated in the access control rule.

Note: The same applies to Table 22 SCN Access Control Table, Table 25 CPY Access Control Table, Table 28 FAX Access Control Table, Table 31 DSR Access Control Table.

SuggestedRemedy

Clarify that ""none"" security attribute does not mean no security attribute need to be evaluate for the associated access control rule. Or maybe we change the attribute(s) from 'None' to '+PRT_PERMISSION' - which should be defined as the permission rights authorized by Administrator to the normal user for executing the PRT function?

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

Discuss and resolve with help from [Kurth].

Cl **PP-A** SC **12.2** P **28** L **10** # **88**
 Sukert, Alan Xerox

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

In the PRT Access Control SFP it indicates that a normal user is allowed to access the PRT function if authorized by the administrator. I note that the administrator can perform some print-related functions such as causing a secure print job to complete under some conditions. Given that, I was wondering why in Table 19 an entry shouldn't be added for F.PRT that allows the U.ADMINISTRATOR the ability to perform the Execute operation.

Same comment applies to PP-B and PP-C.

SuggestedRemedy

Consider adding to Table 19 an entry for F.PRT that allows the U.ADMINISTRATOR the ability to perform the Execute operation.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

Add also for SCN CPY FAX etc.

Cl **PP-A** SC **12.2** P **29** L **4** # **89**
 Sukert, Alan Xerox

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

This comment may be a result of my lack of understanding of the new TOE model.

It is not clear why in the description of SFR FDP_ACF.1 in the PRT SFR Package FDP_ACF.1.1 states that the TSF shall enforce the PRT Access Control SFP to subjects and objects based only on the PRT Access Control SFP, while the description of SFR FDP_ACC.1.1 indicates that the TSF shall enforce the PRT Access Control SFP on subjects, objects and operations among those covered by the Common Access Control SFP.

I would expect FDP_ACF.1.1 to be consistent with FDP_ACC.1 .1 in terms of what access control SFP subjects and objects would be enforced against, whether that be the Common Access Control SFP, the PRT Access Control SFP, or both.

A similar comment applies to the P2600.1-SCN SFR Package (subclause 13.2, page 32, line 3); the P2600.1-CPY SFR Package (subclause 14.2, page 35, line 3); the P2600.1-FAX SFR Package (subclause 15.2, page 38, line 5) and the P2600.1-DSR SFR Package (subclause 16.2, page 41, line 9).

SuggestedRemedy

Clarify and make sure FDP_ACF.1 and FDP_ACC.1 are consistent in terms of what access control SFPs are enforced in these two SFRs in all the P2600.1 SFR packages noted above.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

See Comment 109 Response.

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-B** SC 12.2 P 29 L 4 # 103

Sukert, Alan Xerox

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

This comment may be a result of my lack of understanding of the new TOE model.

It is not clear why in the description of SFR FDP_ACF.1 in the PRT SFR Package FDP_ACF.1.1 states that the TSF shall enforce the PRT Access Control SFP to subjects and objects based only on the PRT Access Control SFP, while the description of SFR FDP_ACC.1.1 indicates that the TSF shall enforce the PRT Access Control SFP on subjects, objects and operations among those covered by the Common Access Control SFP.

I would expect FDP_ACF.1.1 to be consistent with FDP_ACC.1 .1 in terms of what access control SFP subjects and objects would be enforced against, whether that be the Common Access Control SFP, the PRT Access Control SFP, or both.

A similar comment applies to the P2600.2-SCN SFR Package (subclause 13.2, page 32, line 3); the P2600.2-CPY SFR Package (subclause 14.2, page 35, line 3); the P2600.2-FAX SFR Package (subclause 15.2, page 38, line 5) and the P2600.2-DSR SFR Package (subclause 16.2, page 41, line 9).

SuggestedRemedy

Clarify and make sure FDP_ACF.1 and FDP_ACF.1 are consistent in terms of what access control SFPs are enforced in these two SFRs in all the P2600.2 SFR packages noted above.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

See Comment 109 Response.

Cl **PP-C** SC 12.2 P 29 L 4 # 109

Sukert, Alan Xerox

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

This comment may be a result of my lack of understanding of the new TOE model.

It is not clear why in the description of SFR FDP_ACF.1 in the PRT SFR Package FDP_ACF.1.1 states that the TSF shall enforce the PRT Access Control SFP to subjects and objects based only on the PRT Access Control SFP, while the description of SFR FDP_ACC.1.1 indicates that the TSF shall enforce the PRT Access Control SFP on subjects, objects and operations among those covered by the Common Access Control SFP.

I would expect FDP_ACF.1.1 to be consistent with FDP_ACC.1 .1 in terms of what access control SFP subjects and objects would be enforced against, whether that be the Common Access Control SFP, the PRT Access Control SFP, or both.

A similar comment applies to the P2600.1-SCN SFR Package (subclause 13.2, page 32, line 3); the P2600.1-CPY SFR Package (subclause 14.2, page 35, line 3); the P2600.1-FAX SFR Package (subclause 15.2, page 38, line 5) and the P2600.1-DSR SFR Package (subclause 16.2, page 41, line 9).

SuggestedRemedy

Clarify and make sure FDP_ACF.1 and FDP_ACF.1 are consistent in terms of what access control SFPs are enforced in these two SFRs in all the P2600.1 SFR packages noted above.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

Packages should only refer to their own SFPs.

IEEE P2600 Hardcopy Device and System Security Comments

CI **PP-B** SC 12.2 P 29 L 20 # 104
 Sukert, Alan Xerox

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

The APP Note here says that the dependency of FDP_ACF.1 to FMT_MSA.3 is resolved by ""P2600.1"". However, P2600.2-PRT is part of P2600.2, so this seems like circular referencing to me. I think what was meant here was to refer to subclause 11.6 for the FMT_MSA.3 discussion.

A similar comment applies to the P2600.2-SCN SFR Package (subclause 13.2, page 32, line 20); the P2600.2-CPY SFR Package (subclause 14.2, page 35, line 20); the P2600.2-FAX SFR Package (subclause 15.2, page 38, line 22); the P2600.2-DSR SFR Package (subclause 16.2, page 41, line 26) and the P2600.2-SMI SFR Package (subclause 18.2, page 46, line 10 for the FAU_GEN.1 SFR and line 22 for the FAU_GEN.2 SFR).

SuggestedRemedy

Change the APP Note in the subclauses noted above to reference subclause 11.6 instead of ""P2600.2"".

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

Consult with [Kurth].

CI **PP-A** SC 12.2 P 29 L 20 # 90
 Sukert, Alan Xerox

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

The APP Note here says that the dependency of FDP_ACF.1 to FMT_MSA.3 is resolved by ""P2600.1"". However, P2600.1-PRT is part of P2600.1, so this seems like circular referencing to me. I think what was meant here was to refer to subclause 11.6 for the FMT_MSA.3 discussion.

A similar comment applies to the P2600.1-SCN SFR Package (subclause 13.2, page 32, line 19); the P2600.1-CPY SFR Package (subclause 14.2, page 35, line 20); the P2600.1-FAX SFR Package (subclause 15.2, page 38, line 22); the P2600.1-DSR SFR Package (subclause 16.2, page 41, line 25) and the P2600.1-SMI SFR Package (subclause 18.2, page 46, line 10 for the FAU_GEN.1 SFR and line 22 for the FAU_GEN.2 SFR);

SuggestedRemedy

Change the APP Note in the subclauses noted above to reference subclause 11.6 instead of ""P2600.1"".

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

Consult with [Kurth].

CI **PP-C** SC 12.2 P 29 L 20 # 110
 Sukert, Alan Xerox

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

The APP Note here says that the dependency of FDP_ACF.1 to FMT_MSA.3 is resolved by ""P2600.3"". However, P2600.3-PRT is part of P2600.3, so this seems like circular referencing to me. I think what was meant here was to refer to subclause 11.6 for the FMT_MSA.3 discussion.

A similar comment applies to the P2600.1-SCN SFR Package (subclause 13.2, page 32, line 19); the P2600.1-CPY SFR Package (subclause 14.2, page 35, line 20); the P2600.1-FAX SFR Package (subclause 15.2, page 38, line 22); the P2600.1-DSR SFR Package (subclause 16.2, page 41, line 25) and the P2600.1-SMI SFR Package (subclause 18.2, page 46, line 10 for the FAU_GEN.1 SFR and line 22 for the FAU_GEN.2 SFR);

SuggestedRemedy

Change the APP Note in the subclauses noted above to reference subclause 11.6 instead of ""P2600.3"".

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

Consult with [Kurth].

CI **PP-A** SC 12.3 P 29 L 31 # 132
 Chen, Nancy Oki Data

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

Users who have authenticated to execute PRT, may need to be re-authenticated before the release of D.DOC to output handler.

SuggestedRemedy

Remove the qualification of users ""who is not authenticated using operator controls or displays on the TOE"".

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

Clarify text to describe the use case. May add an app note about the walk up USB stick print case.

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-A** SC **12.3** P **29** L **31** # **91**

Sukert, Alan Xerox

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

The description of SFR FIA_UAU.6.1 uses the +PRT notational convention associated with an object. However, the use of the '+' convention in this context is not described in the Notational Conventions in subclause 1.4.1.

Same comment applies to PP-B.

SuggestedRemedy

Include the use of the '+' notation with data objects in the list of notational conventions in subclause 1.4.1.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **PP-A** SC **12.4** P **30** L **6** # **96**

Sukert, Alan Xerox

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

In Table 21, the description for O.DOC_NO_DIS is ""Protection of User Data from unauthorized disclosure"". However, O.DOC_NO_DIS in Table 9 (subclause 9.1, page 14, line 4) is described as protecting ""User Document Data"" from unauthorized disclosure. The description in Table 21 is inconsistent with the description of O.DOC_NO_DIS in Table 9.

Same comment applies to Table 24, subclause 13.3, page 33, line 1; Table 27, subclause 14.3, page 36, line 1; Table 30, subclause 15.3, page 39, line 1; Table 33, subclause 16.3, page 42, line 2 and Table 35, subclause 17.3, page 44, line 10 vs. Table 9.

SuggestedRemedy

Make the description of O.DOC_NO_DIS in the tables listed above consistent with the description of O.DOC_NO_DIS in Table 9 (suggest changing the description in the ""sufficiency"" tables to read ""Protection of User Document Data from unauthorized disclosure"")

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **PP-B** SC **12.4** P **30** L **6** # **106**

Sukert, Alan Xerox

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

In Table 21, the description for O.DOC_NO_DIS is ""Protection of User Data from unauthorized disclosure"". However, O.DOC_NO_DIS in Table 9 (subclause 9.1, page 14, line 4) is described as protecting ""User Document Data"" from unauthorized disclosure. The description in Table 21 is inconsistent with the description of O.DOC_NO_DIS in Table 9.

Same comment applies to Table 24, subclause 13.3, page 33, line 1; Table 27, subclause 14.3, page 36, line 1; Table 30, subclause 15.3, page 39, line 1; Table 33, subclause 16.3, page 42, line 2 and Table 35, subclause 17.3, page 44, line 10 vs. Table 9.

SuggestedRemedy

Make the description of O.DOC_NO_DIS in the tables listed above consistent with the description of O.DOC_NO_DIS in Table 9 (suggest changing the description in the ""sufficiency"" tables to read ""Protection of User Document Data from unauthorized disclosure"")

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **Globa** SC **12.2** P **31** L **19** # **3**

aubry, carmen oce

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

This comment concerns PP-E Table 19: D.DOC should be removed (PP-E in the previous form: we have already agreed that we can not password protect job release in production environments). FIA_UAU.6 should also be removed(for the same reason).

SuggestedRemedy

Remove D.DOC on table 19 and FIA_UAU.6.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

IEEE P2600 Hardcopy Device and System Security Comments

Cl **PP-B** SC **15.2** P **37** L **25** # **105**
 Sukert, Alan Xerox

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

The APP Note on this line indicates that the FDP_ACC.1 SFR fulfills O.DOC.NO_DIS, O.DOC_NO_ALT and O.USER.AUTHORIZED. However, O.DOC_NO_ALT is not listed in Table 29 (subclause 15.3, page 38, line 30).

SuggestedRemedy

Resolve the inconsistency as to whether the FDP_ACC.1 SFR fulfills O.DOC_NO_ALT between subclauses 15.2 and 15.3.

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

Cl **PP-A** SC **15.2** P **37** L **25** # **92**
 Sukert, Alan Xerox

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

The APP Note on this line indicates that the FDP_ACC.1 SFR fulfills O.DOC.NO_DIS, O.DOC_NO_ALT and O.USER.AUTHORIZED. However, O.DOC_NO_ALT is not listed in Table 29 (subclause 15.3, page 38, line 30).

SuggestedRemedy

Resolve the inconsistency as to whether the FDP_ACC.1 SFR fulfills O.DOC_NO_ALT between subclauses 15.2 and 15.3.

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

Cl **PP-A** SC **16.2** P **40** L **10** # **93**
 Sukert, Alan Xerox

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

The DSR Access Control SFP is centered around activities for ""reading"" User Document Data, where read is related to disclosure of information. I compared this with the DSR Access Control Policy in the previous PP-A version, and I noted that in the previous version this SFR was centered on the concept of retrieval of User Document Data that had been stored in the TOE, which is the main focus of the DSR function. It is not clear why this concept of retrieval is also not included for the P2600.1-DSR SFR Package in this latest version.

Comment also applies to PP-B.

SuggestedRemedy

Consider including the concept of UDD retrieval in the P2600.1-DSR SFR Package.

Proposed Response Response Status **W**
 PROPOSED REJECT.

Cl **PP-C** SC **18.2** P **41** L **6** # **111**
 Sukert, Alan Xerox

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

There is a Table number reference error on this line that needs to be corrected.

SuggestedRemedy

Correct the indicated table number error reference.

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

Cl **PP-A** SC **17.1** P **43** L **7** # **95**
 Sukert, Alan Xerox

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

The NVS SFR Package states that the package defines the requirements for ""removable nonvolatile storage devices"" in the TOE. I note that in the previous versions of this PP the NVS TOE applies to ""nonvolatile storage devices"".

It is not clear why the NVS SFR package only applies now to removable NVS media and not to all NVS media. I understand that the FDP_ITC.1 SFR applies to export of TSF data, but if you can assume that ""transmission"" in the context of this package refers to storage on an NVS device, then it shouldn't make a difference whether the media is removable or not. You want to protect the confidentiality of data stored on in NVS whether that media is removed from the TOE or is accessed while the data is ""at rest"" on the TOE. By limiting the NVS SFR package to only removable media you ignore all of the threats associated with accessing data stored in NVS when it resides inside the machine, which was part of the original intent of the NVS TOE in the prior model.

I also note that if you change the concept of transmission to apply to storage on a nonvolatile media the FPT_ITC.1 SFR would apply just as well as it does now to the NVS SFR Package.

Same comment applies to PP-B and PP-C

SuggestedRemedy

Revise the P2600.1-NVS. P2600.2-NVS Packages to apply to data stored in any nonvolatile storage media, not just removable nonvolatile storage media. Changes would be needed in subclauses 17.1, the FTP_ITC1.1 SFR, and the PP APP Note in subclause 17.3, page 44, line 14 as a minimum.

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

Will be addressed as part of the NVS SFR package re-write.

IEEE P2600 Hardcopy Device and System Security Comments

CI **All P** SC 17.1 P 43 L 7 # 21
 Smithson, Brian Ricoh

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

[Kurth] Some more explanation of the purpose and applicability of this package should be added.

SuggestedRemedy

The NVS package should be included for products that have a function to protect the confidentiality and integrity of data exported to the NVS device. This can for example be done by using encryption techniques or by using function of the NVS device to "lock" the data on the device. In the first case, no further assumption needs to be made on the environment to protect the confidentiality and integrity (interpreted as detectability of modifications) of data. In the second case, assumption have to be made on the quality of the "locking" mechanism of the NVS device.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

Will be addressed as part of the NVS SFR package re-write.

CI **PP-C** SC 19 P 44 L 4 # 112
 Sukert, Alan Xerox

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

Table 39 with the applicable SARs listed ALC_FLR.2 instead of ALF_FLR.1 which is what this PP is augmenting EAL2 with.

SuggestedRemedy

List ALC_FLR.1 in Table 39.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

CI **PP-A** SC 17.3 P 44 L 10 # 97
 Sukert, Alan Xerox

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

In Table 35, the description for O.CONF_NO_DIS is "Protection of TSF Data from unauthorized disclosure". However, O.CONF_NO_DIS in Table 9 (subclause 9.1, page 14, line 4) is described as protecting "TSF Confidential Data" from unauthorized disclosure. The description in Table 35 is inconsistent with the description of O.DOC_NO_DIS in Table 9.

Same comment applies to PP-B (Table 35, subclause 17.3, page 44, line 10 vs. Table 9, subclause 9.1, page 14, line 4).

SuggestedRemedy

Make the description of O.CONF_NO_DIS in the tables listed above consistent with the description of O.CONF_NO_DIS in Table 9 (suggest changing the description in the "sufficiency" tables to read "Protection of TSF Confidential Data from unauthorized disclosure")

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Should be TSF Confidential Data

CI **PP-A** SC 18.2 P 45 L 27 # 99
 Sukert, Alan Xerox

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

The PP App Note on this line refers to Table 24 which is the sufficiency table for the SCN SFR Package. I believe Table 36 was meant here.

SuggestedRemedy

Reference the proper table in the indicated APP Note.

Proposed Response Response Status **W**

PROPOSED REJECT.

This comment was WITHDRAWN by the commenter.

IEEE P2600 Hardcopy Device and System Security Comments

Cl All P SC 18.2 P 46 L 15 # 33
 Smithson, Brian Ricoh

Comment Type T Comment Status D

[Kurth] The SFR FAU_GEN.2 can be removed from the package since it is already part of the base PP and multiple instances of this SFR are not useful since they contain the same text and not an assignment, selection or refinement that is specific for the additional audit event defined in the package. Since FAU_GEN.2 applies to all audit events (even additional ones the author of a ST adds) it also applies for the additional audit event defined in the SMI package.

SuggestedRemedy

Remove FAU_GEN.2 from SMI package.

Proposed Response Response Status W

PROPOSED ACCEPT.

Cl All P SC 18.3 P 46 L 27 # 34
 Smithson, Brian Ricoh

Comment Type T Comment Status D

[Kurth] FMT_SMF.1 is not used correctly in the SMI package. If such a management function is really intended to be specified, another SFR needs to be used which also specifies who is allowed to define the ""permit"" or ""deny"".

SuggestedRemedy

The correct SFR for this is FMT_MOF.1 with the following instantiation:

FMT_MOF.1.1

The TSF shall restrict the ability to disable and enable the function to exchange data between any Interface and a Shared-medium Interface to [selection: U.ADMINISTRATOR, none].

Proposed Response Response Status W

PROPOSED ACCEPT.

Cl All P SC 18.3 P 46 L 33 # 69
 Sukert, Alan Xerox

Comment Type T Comment Status D

SFR FMT_SMF.1.1 states that it applies to exchange of data between any Interface and a Shared-medium Interface. Any interface could include a Shared-Medium Interface, so this requirement includes data exchanged between one Shared-medium interface and another Shared-medium interface if I understand the requirement as stated - is that what was meant.

There are other questions such as how can one deny exchange of data between two interfaces that is inherently denied already.

Same comment applies to PP-B, subclause 18.3 (page 46, line 33).

If I read the APP Note on page 47 associated with this SFR correctly, the requirement as stated doesn't preclude bridging because it allows permission of data exchanged between interfaces except when inherently denied, and I don't think you can assume that bridging is inherently denied on the basis of TOE architecture, design or implementation.

I'm hoping this comment can serve as a vehicle to discuss this SFR at the next meeting because I'm having trouble understanding how it meets the intended purpose in the APP Note.

Note: This comment applies to PP-B, PP-C and PP-D (subclause 12.2) also.

SuggestedRemedy

Make sure the FMT_SMF.1.1 requirement in all four PPs is stated to meet the intent indicated in its associated APP Note on page 47, line 1 .

Note also that the associated APP Note really needs to do more to clarify this SFR (e.g., whether or not this requirement applies to shared-medium to shared-medium interface data exchanges).

Proposed Response Response Status W

PROPOSED ACCEPT IN PRINCIPLE.

SMI Package restructure and re-write will address these concerns.

IEEE P2600 Hardcopy Device and System Security Comments

CI **PP-A** SC **18.4** P **47** L **9** # **133**
 Chen, Nancy Oki Data

Comment Type **E** Comment Status **D**
 Copy error of FTP_ITC.1.1 from CCv3.1R2. ""The TSF shall provide a communication channel between itself another trusted IT productà""

SuggestedRemedy
 Change to ""The TSF shall provide a communication channel between itself and another trusted IT productà""

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

CI **All P** SC **18.5** P **48** L **1** # **70**
 Sukert, Alan Xerox

Comment Type **T** Comment Status **D**
 In Table 38, the O.CHANNELS.MANAGED description is ""Authorization of Users and Administrators to use the TOE"". Per subclause 9.1 this objective has to do with managing the operation of input-output channels in accordance with security policies, which would not seem to have anything directly to do with authorizing users and administrators to use the TOE.

Same comment applies to PP-B, Table 38, subclause 18.5, page 48, line 1; PP-C, Table 38, subclause 18.5, page 43, line 1; PP-D, table 17, subclause 12.4, page 25, line 14.

SuggestedRemedy
 Change the description in all four PPs for O.CHANNELS.MANAGED in the applicable tables to better agree with the definition of this objective in subclause 9.1 (suggest ""Management of input-output channels"" as was done in PP-A, subclause 11.12, Table 18, page 27 for this objective)

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

CI **All P** SC **Annex A** P **50** L **1** # **71**
 Sukert, Alan Xerox

Comment Type **E** Comment Status **D**
 The following terms included in Annex A no longer are used or referenced within the PPs:
 - Authorization
 - Compromise
 - External entity
 - Unauthorized user

SuggestedRemedy
 Remove the unused terms from Annex A in all four PPs.

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

Scrub the terms section following the re-writes.

CI **All P** SC **Annex A** P **52** L **18** # **48**
 Sukert, Alan Xerox

Comment Type **T** Comment Status **D**
 The definition of User Data in Annex A should be changed to reflect the new definition of TSF in CCv3.1 as 'TOE security functionality' and not 'TOE security function' as was the case in CCv2.3.

SuggestedRemedy
 Change the definition of User Data in Annex A in all four PPs to read ""Data created by and for the User, that do not affect the operation of the TOE security functionality.""

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

IEEE P2600 Hardcopy Device and System Security Comments

Cl **All P** SC **Annex B** P **53** L **1** # **72**
Sukert, Alan Xerox

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

The following acronyms are no longer used in the PPs:

- ID
- SAL
- SAR (to mean security assurance requirement)
- TSFI

SuggestedRemedy

Remove the unused acronyms from Annex B in all four PPs.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

Scrub the Acroynms list following the re-write.

Cl **All P** SC **Introduction** P **iii** L **12** # **39**
Sukert, Alan Xerox

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

I was just wondering if the capitalization of ""Compliance clause"" here and in line 13 shouldn't be 'Compliance Clause' for consistency.

SuggestedRemedy

Determine how ""Compliance clause"" should properly be capitalized.

Proposed Response Response Status **W**

PROPOSED ACCEPT.