

IEEE P2600 Hardcopy Device and System Security comments

Cl All P SC 10.1 P 20 L 12 # 14
 Sukert, Alan Xerox

Comment Type T Comment Status X

For SFR FAU_GEN.1 we allow the ST author to choose their level of audit, but then also define the level of audit that is required for specific functions in Table 14. The levels of audit in this table could conflict with the chosen level of audit, which will create confusion on the part of the evaluators and/or evaluation sponsor. Additionally, the text at FAU_GEN.1.2 item 3 is somewhat incoherent. It would not be difficult to come up with a plausible definition for this item that conflicted with each other. Additionally, all of the items in Table 14 must be audited with the specificity found in the CC Part 2 Audit Specification for each of those requirements. When you consider that O.USER.AUTHORIZED specifies that all users must be identified and authorized, and that O.AUDIT.LOGGED requires that all TOE use be logged, these audit requirements could become quite onerous. Imagine for instance, an audit entry every time someone makes a single copy.

Also, conspicuously absent are any requirements having to do with allowing the sorting, querying, or selection of audit records for review (if the TOE must keep them, it must give the admin some way to view them, especially in light of P.AUDIT.LOGGING). Also absent are requirements stating how the audit logs will be protected in case of audit storage exhaustion or failure (Is it circular? Does it stop auditing? Does it copy them elsewhere? Does it clear the file and start over?), again especially in light of P.AUDIT.LOGGING.

Finally, it is not clear that any HCD that was to comply with this PP would be able to comply with Table 14 and collect all of the listed auditable events at the audit level indicated. We don't want to get into a situation where we define a set of auditable event collection requirements in a governing PP that can not practically be collected so that no HCD could ever comply as the result of an evaluation.

These comments apply to the discussion of the FAU_GEN.1 common SFR in subclause 10.1 in the other three PPs.

SuggestedRemedy

1. Make the required auditable events listed in Table 14 recommended auditable events.
2. Clarify the FAU_GEN.1 requirements to address the issues discussed above.

Proposed Response Response Status O

Cl All P SC 10.1 P 21 L 9 # 1
 Smithson, Brian Ricoh

Comment Type E Comment Status X

CC-defined audit levels sometimes use "Minimum" and sometimes use "Minimal" to mean the same thing. We discussed this in a previous meeting and decided that "Minimum" should be used consistently in the PPs.

SuggestedRemedy

Change references to audit levels from "Minimal" to "Minimum" as needed in PP-A/B/C.

Proposed Response Response Status O

Cl All P SC 10.10 P 32 L 5 # 17
 Sukert, Alan Xerox

Comment Type T Comment Status X

The FTA_SSL.3 SFR, especially because of its tie to O.INTERFACE.MANAGED will apply to all input/output devices of the TOE, to include the document output tray, the scanner, any user interfaces, and the Ethernet port (for example). That means that to be compliant a TOE would have to ensure that any session involving any external interface would have to have some type of TSF-initiated termination. This is far beyond the original intent for including this SFR.

This same comment applies to PP-B (subclause 10.10, page 31, line 4); PP-C (subclause 10.10, page 26, line 19) and PP-D (subclause 10.10, page 20, line 19).

SuggestedRemedy

Remove the FTA_SSL.3 SFR since it is not a dependency of any of the other listed SFRs.

Proposed Response Response Status O

Cl All P SC 10.4 P 22 L 8 # 6
 Smithson, Brian Ricoh

Comment Type T Comment Status X

The criterion for allowing modify/delete access to D.FUNC is ownership of documents. However, D.FUNC is defined as being information about a document or a job (could be either, or both), and the owner of a job may not be the same user as the owner of a document in a job. The criterion should allow for both cases.

SuggestedRemedy

Change access control rule for D.FUNC from ""Denied, except for his/her own documents"" to ""Denied, except for his/her own function data"".

Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security comments

Cl All P SC 10.4 P 22 L 24 # 15
 Sukert, Alan Xerox

Comment Type T Comment Status X

For the FDP_ACC.1 and FDP_ACF.1 SFRs it was not entirely clear what is trying to be accomplished here. Users are subjects, but the refinement seems to be attempting to treat users as both subjects and objects for the purposes of the Common Access Control SFP. This is slightly incoherent.

These comments also apply to the discussion of the FDP_ACC.1 and FDP_ACF.1 common SFR in subclause 10.4 in the other three PPs.

SuggestedRemedy

Consider clarification via an additional or modified PP Note on what the intent of specifying these SFRs is and how users are being treated for purposes of these SFRs.

Proposed Response Response Status O

Cl All P SC 10.5 P 26 L 1 # 16
 Sukert, Alan Xerox

Comment Type T Comment Status X

For the FIA_UAU.1 it is not clear what difference the selection refinement makes, and we cannot foresee a situation when the TSF could allow conflicting mediated actions on behalf of the user. Refining SFRs can cause interesting things to happen. The application note after FIA_UAU.1.1 is slightly ambiguous. The öpingö command is not generally understood to be a TSF-mediated action as there is no security function associated with it, so specifying a non-security-relevant action in the requirement as a TSF-mediated action would be incorrect.

This same comment applies to PP-B (subclause 10.5, page 25, line 1); PP-C (subclause 10.5, page 21, line 13) and PP-D (subclause 10.5, page 16, line 25).

SuggestedRemedy

Clarify (possibly via a PP APP Note) why the refinement is included for the FIA_UAU.1 SFR.

Modify the APP Note after FIA_UAU.1.1 to provide a technically correct example.

Proposed Response Response Status O

Cl All P SC 10.6 P 28 L 1 # 2
 Smithson, Brian Ricoh

Comment Type E Comment Status X

App notes about dependencies and management functions for FMT_MSA.1(a) and FMT_MSA.1(b) should refer to the SFRs that correspond to their respective iterations, i.e. (a) to (a) and (b) to (b).

SuggestedRemedy

In the FMT_MSA.1 iterations:
 Change ""FMT_MSA.1 is a dependency of FMT_MSA.3"" to ""FMT_MSA.1(a) is a dependency of FMT_MSA.3(a)"" and ""FMT_MSA.1(b) is a dependency of FMT_MSA.3(b)"".

Change ""FMT_MSA.1 performs management functions that are recommended for FDP_ACF.1"" to ""FMT_MSA.1(a) performs management functions that are recommended for FDP_ACF.1(a)"" and ""FMT_MSA.1(b) performs management functions that are recommended for FDP_ACF.1(b)"".

In the FMT_MSA.3 iterations:
 change ""FMT_MSA.3 is a dependency of FDP_ACF.1"" to ""FMT_MSA.3(a) is a dependency of FDP_ACF.1(a)"" and ""FMT_MSA.3(b) is a dependency of FDP_ACF.1(b)""

Proposed Response Response Status O

Cl All P SC 16.2 P 48 L 12 # 5
 Smithson, Brian Ricoh

Comment Type T Comment Status X

Incoming fax rule is too restrictive. It disallows administrator access to incoming faxes in cases where an administrator has transferred ownership to a normal user.

SuggestedRemedy

Change the Subject of the incoming fax rule from U.USER to U.NORMAL.

Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security comments

Cl **All P** SC **19.4** P **58** L **5** # **3**
 Smithson, Brian Ricoh
 Comment Type **E** Comment Status **X**
 missing word in FTP_ITC.1.1
 SuggestedRemedy
 Change ""between itself another trusted IT product"" to ""between itself and another trusted IT product"".
 Proposed Response Response Status **O**

Cl **All P** SC **7.3** P **13** L **1** # **12**
 Sukert, Alan Xerox
 Comment Type **T** Comment Status **X**
 P.SOFTWARE.VERIFICATION and P.INTERFACE.MANAGEMENT do not appear to be valid Organizational Security Policies (OSPs). OSPs define rules, guidelines or policies that the organization operating the TOE must adhere to as opposed to policies the TOE must comply with. These two OSPs seem to place requirements on the TOE that would not be able to be met. For example, P.SOFTWARE.VERIFICATION seems to require that the TOE be able to verify its software, and P.INTERFACE.MANAGEMENT specifies all input/output devices, which could easily be read to mean any User Interface (whether on the device or a web interface), USB, Parallel Port, Serial Port, Firewire, Paper Output Tray, Scanner, etc.
 This same comment applies to the OSP table in subclause 7.3 in each of the other three PPs.

This is probably not what was intended for OSPs.
 SuggestedRemedy
 In all four PPs determine if P.SOFTWARE.VERIFICATION and P.INTERFACE.MANAGEMENT should be OSPs and, if so, define them in terms of operational policies as is done for P.AUDIT.LOGGING, as an example, rather than as requirements that are better defined via SFRs.
 Proposed Response Response Status **O**

Cl **All P** SC **8.1** P **14** L **4** # **13**
 Sukert, Alan Xerox
 Comment Type **T** Comment Status **X**
 There are some concerns about the security objectives for the TOE as stated in Table 10:
 1. O.INTERFACE.MANAGED has the problem that P.INTERFACE.MANAGEMENT does (see applicable comment) regarding types of input/output devices, and this will cause issues with the SFRs.
 2. O.SOFTWARE.VERIFICATION requires that the TOE be able to self-verify its software. It's not sufficient for the administrator to view the configuration report if the TOE has to verify itself.
 3. O.USER.AUTHORIZED requires that users be identified and authorized; this could easily be read to mean all users, including someone who just walks up to make a single copy. The TOE wouldn't just have to be capable of this, this would be required in the evaluated configuration.
 4. O.AUDIT.LOGGED requires that the TOE audit TOE use, but doesn't narrow the scope of this use. The scope would presumably be defined in FAU_GEN, but could easily be interpreted more broadly by evaluators.

These comments apply to the security objectives listed above in the applicable Security Objectives table in subclause 8.1 in the other three PPs.
 SuggestedRemedy
 Clarify in all four PPs the indicated TOE security objectives to resolve the issues listed above.
 Proposed Response Response Status **O**

Cl **All P** SC **8.2** P **14** L **6** # **8**
 Sukert, Alan Xerox
 Comment Type **T** Comment Status **X**
 The explanatory sentence for this subclause now reads as "This section describes the security objectives that must be fulfilled by IT methods in the environment of the TOE." This is not correct given that the title of this subclause is 8.2 Security objectives for the IT environment.
 The same comment applies to PP-B, subclause 8.2, page 13, line 6; PP-C, subclause 8.2, page 13, line 6 and PP-D, subclause 8.2, page 13, line 6.
 SuggestedRemedy
 It would be more accurate to revise the indicated sentences in all four PPs to read ""This section describes the security objectives that must be fulfilled by IT methods in the IT environment of the TOE.""
 Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security comments

Cl All P SC 8.3 P 15 L 2 # 9
Sukert, Alan Xerox

Comment Type T Comment Status X

The explanatory sentence for this subclause now reads as "This section describes the security objectives that must be fulfilled by non-IT methods in the environment of the TOE." This is not correct given that the title of this subclause is 8.3 Security objectives for the non-IT environment.

The same comment applies to PP-B, subclause 8.3, page 14, line 2; PP-C, subclause 8.3, page 14, line 2 and PP-D, subclause 8.3, page 13, line 10.

SuggestedRemedy

It would be more accurate to revise the indicated sentences in all four PPs to read ""This section describes the security objectives that must be fulfilled by IT methods in the non-IT environment of the TOE.""

Proposed Response Response Status O

Cl All P SC 9 P 16 L 3 # 7
Sukert, Alan Xerox

Comment Type E Comment Status X

'Protectioon' is misspelled in line 3.

The same comment applies to PP-B, subclause 9, page 15, line 3; PP-C, subclause 9, page 15, line 3 and PP-D, subclause 9, page 14, line 7.

SuggestedRemedy

Replace 'Protectioon' by 'Protection' on the indicated pages and lines in all four PPs.

Proposed Response Response Status O

Cl All P SC 9.2 P 19 L 3 # 10
Sukert, Alan Xerox

Comment Type E Comment Status X

There appears to be a grammatical error on this line. The line currently states "Quite often a TOE is supposed to perform specific checks process data received on one external interface...". It's not clear whether what was meant was "Quite often a TOE is supposed to perform specific checks on process data received on one external interface..." or "Quite often a TOE is supposed to perform specific checks or process data received on one external interface..." (or something else).

The same comment applies to PP-B, subclause 9.2, page 17, line 44; PP-C, subclause 9.1, page 16, line 20 and PP-D, subclause 9.1, page 15, line 32.

SuggestedRemedy

Revise the sentences on the pages and lines indicated above for all four PPs to clarify what is meant.

Proposed Response Response Status O

Cl All P SC 9.2 P 19 L 4 # 11
Sukert, Alan Xerox

Comment Type T Comment Status X

The rationale on page 19 in several places refers to just 'interface' when describing why this new extended component is necessary. Since this new extended component specifically deals with external interfaces and in a TOE there can be both external and internal interfaces, for clarity all references to just 'interface' in this rationale really should be to 'external interface'.

The same comment applies to PP-B, subclause 9.2, page 17, line 45; PP-C, subclause 9.1, page 16, line 21 and PP-D, subclause 9.1, page 15, line 33.

SuggestedRemedy

Change all references to 'interface' in the rationale in the subclauses indicated above for all four PPs to 'external interface'.

Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-A** SC **10.4** P **25** L **13** # **28**
 Sukert, Alan Xerox

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

The CC conventions is that a PP author has to either fill in assignments or leave them blank. For the FDP_RIP.1, we've attempted to both fill it in and leave it blank which violates this convention.

This same comment applies to PP-B (subclause 10.4, page 24, line 13)and PP-C (subclause 10.4, page 20, line 33)

SuggestedRemedy

Revise the FDP_RIP.1 SFR description to follow the CC convention.

Proposed Response Response Status **O**

Cl **PP-A** SC **18.1** P **54** L **7** # **24**
 Sukert, Alan Xerox

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

This line was modified to indicated that removable NVS was to be protected when the "devices are removed from the protection of its environment". Line 7 is unclear from which environment removal of the NVS is to be protected.

Looking at the changes that were made in lines 14 and 16, the protection is to be for removal from the environment of the TOE. For clarify the environment referenced in line 7 should also be for protection of removal from the environment of the TOE.

SuggestedRemedy

Revise page 54, line 7 to read "...,devices are removed from the protection of the environment of the TOE."

Proposed Response Response Status **O**

Cl **PP-A** SC **18.1** P **54** L **9** # **29**
 Sukert, Alan Xerox

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

In the NVS SFR Package subclause 18.1 states that: "Removable Nonvolatile Storage device is a nonvolatile storage device that is part of the evaluated TOE but is designed to be removed from and re-inserted into the TOE by authorized non-service personnel." The term "non-service personnel" could be interpreted to be the system administrator, but not the service technician.

This SFR package defines requirements for devices that have hard drives that are designed to be removed, swapped, replaced, etc. by system administrators. There appears to be no reason why the security functionality here has to be defined by an extended requirement and couldn't instead be articulated by a combination of standard CC requirements (data recovery, integrity, etc.).

Additionally (and most importantly), this extended component could be read and interpreted by an evaluator to include compact flash drives, USB drives, or any other type of non-volatile device that could be connected to the TOE, which was clearly not the intent of this extended component.

This comment also applies to PP-B (subclause 18.1, page 54, line 9).

SuggestedRemedy

Remove the FTP_CIP_EXP.1 extended component from subclause 18 and instead determine the appropriate CC SFRs that can be applied to removable NVS to meet the desired confidentiality and integrity requirements.

Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security comments

CI **PP-A** SC **19.2** P **56** L **8** # **30**
 Sukert, Alan Xerox

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

For the SMI SFR Package, is there a reason that the FMT_FDI_EXP extended component was used instead of accomplishing the necessary protection using the Flow Control SFRs?

Also, as FAU_GEN.1 is repeated here, does this version supersede the FAU_GEN.1 SFR requirements specified in subclause 10.1?

Finally, after reading the shared-medium interface definition in the glossary, this could mean everything from an Ethernet port to a Bluetooth transmitter. The definition of shared-medium interface has to be clarified to limit the scope to the type of external interfaces it is meant to address like the Fax PSTN.

SuggestedRemedy

Consider removing the FMT_FDI_EXP extended component and replacing it with the applicable flow control SFR.

Clarify (possible via an PP APP Note) how the FAU_GEN.1 SFR defined for the SMI SFR Package relates to the FAU_GEN.1 SFR defined in subclause 10.1.

Clarify the definition of a shared-medium interface in subclauses 5.3.4 and Annex A to limit the scope of what a shared-medium interface to those interfaces for which SMI SFR requirements apply to.

Proposed Response Response Status **O**

CI **PP-A** SC **20** P **60** L **1** # **25**
 Sukert, Alan Xerox

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

Somehow an extraneous Subclause 20 with an empty Table 43 was included in the MS Word version of this PP.

SuggestedRemedy

Remove the extraneous Subclause 20.

Proposed Response Response Status **O**

CI **PP-A** SC **7.3** P **13** L **1** # **19**
 Sukert, Alan Xerox

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

In Table 8 in the P.INTERFACE.MANAGEMENT row there are two periods at the end of the Defenition for this OSP (...controlled by the TOE and its IT environment.").

SuggestedRemedy

Revise page 13, line 1 to read ""controlled by the TOE and its IT environment.""

Proposed Response Response Status **O**

CI **PP-A** SC **9.1** P **17** L **1** # **20**
 Sukert, Alan Xerox

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

This line now reads "FPT_CIP_EXP.1 Confidentiality and Integrity of Stored Data, provides for the protection of user and TSF data stored on storage container that..." May be more grammatically correct for the sentence to read "FPT_CIP_EXP.1 Confidentiality and Integrity of Stored Data, provides for the protection of user and TSF data stored on a storage container that..."

SuggestedRemedy

Modify page 17, line 1 as indicated above.

Proposed Response Response Status **O**

CI **PP-A** SC **9.1** P **17** L **13** # **27**
 Sukert, Alan Xerox

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

The discussion of the FTP_CIP_EXP.1 extended component defines a proposed set of actions that should be auditable for this extended component. The definition as currently stated in subclause 9.1 indicates that the event ""should"" be collected. In terms of specifications ""should"" means that it is not a requirement which implies that this is a recommended auditable event to be collected rather than a required auditable event. The discussion in subclause 9.1 doesn't indicate either way whether this auditable event is required or recommended.

SuggestedRemedy

Clarify in subclause 9.1 whether the auditable event defined for the FTP_CIP_EXP.1 extended component is recommended or required.

Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-A** SC **9.1** P **17** L **31** # **21**
 Sukert, Alan Xerox

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

The sentence on line 31 contains a grammatical error - "...protection and integrity protection, those components are defined different for user data and TSF..." should be "...protection and integrity protection, those components are defined differently for user data and TSF..."

SuggestedRemedy

Revise page 17, line 31 as indicated above.

Proposed Response Response Status **O**

Cl **PP-A** SC **9.1** P **17** L **33** # **22**
 Sukert, Alan Xerox

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

In keeping with the conventions used elsewhere in this PP, 'protection profile' on this line should be captialized.

SuggestedRemedy

On page 17, line 33 replace ""protection profile"" with ""Protection Profile"".

Proposed Response Response Status **O**

Cl **PP-A** SC **9.1** P **17** L **40** # **23**
 Sukert, Alan Xerox

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

The last paragraph on this page provides rationale why the extended component was created. The logic used in the paragraph doesn't appear to be correct - it is indicated that since it addresses the protection of TSF data, it was not viewed as appropriate to put this component into the FDP class related to user data protection; then it states that because the requirement contributes to the protection of the TSF it was appropriate to have this extended SFR be seen as a member of the FDP class; finally it is stated that the extended component does not fit well into any of the existing families within the class, which lead the authors to the definition of a new family with just one member.

What is never explained here is that the new extended component can be placed in the FTP clas because it does protect TSF data and then why it was decided to place the new extended component in the FTP class.

SuggestedRemedy

Revise the last paragraph on page 17 to make the rationale as to why the new extended component is in the FTP class clearer as indicated above.

Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-A** SC **9.2** P **18** L **34** # **26**
 Sukert, Alan Xerox

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

The discussion of the FMT_FDI_EXP.1 extended component defines a proposed set of actions that should be auditable for this extended component. First of all it is not clear how these recommended auditable events relate to the required auditable event listed in Table 40, subclause 19.2, page 57, line 5 because (among other things) the event defined in subclause 9.2 is at the 'Basic' audit level while the auditable event in Table 40 is at the 'Minimal' auditable level. It is not clear why these auditable events are even defined here since they don't appear at all as either SMI SFR audit data requirements or recommendations.

More importantly, the definition as currently stated in subclause 9.2 indicates that the event ""should"" be collected. In terms of specifications ""should"" means that it is not a requirement which implies that this is a recommended auditable event to be collected rather than a required auditable event. The discussion in subclause 9.2 doesn't indicate either way whether this auditable event is required or recommended.

SuggestedRemedy

Clarify in subclause 9.2 whether the auditable event defined for the FMT_FDI_EXP.1 extended component is recommended or required, and show the relationship between these auditable events and the required auditable events for the SMI SFR Package shown in the indicated tables.

Proposed Response Response Status **O**

Cl **PP-A** SC **A** P **60** L **40** # **4**
 Smithson, Brian Ricoh

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

We refer to "jobs" throughout the PPs, but don't have a definition. It is not used as a formal object in the PPs, but I think it would help to have some kind of a definition in the annex.

SuggestedRemedy

Add the definition (adapted from PWG semantic model):

Job: A document processing task submitted to the hardcopy device. A single document processing task may process one or more documents.

Proposed Response Response Status **O**

Cl **PP-B** SC **11** P **35** L **4** # **32**
 Sukert, Alan Xerox

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

In Table 20 the titles of the following SARs are incorrect:

1. ADV_FSP.2 -- It should be ""Security-enforcing functional specification""
2. ALC_CMC.2 -- It should be ""Use of a CM system""
3. ALC_CMS.2 -- It should be ""Parts of the TOE CM coverage""
4. ATE_COV.1 -- It should be ""Evidence of coverage""

SuggestedRemedy

Correct the titles of the SARs indicated above in Table 20.

Proposed Response Response Status **O**

Cl **PP-B** SC **12.1** P **36** L **17** # **31**
 Sukert, Alan Xerox

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

Missing paragraph reference on this line (now gives "Reference not found" error message).

SuggestedRemedy

Provide the proper paragraph reference on page 36, line 7.

Proposed Response Response Status **O**

Cl **PP-B** SC **18.1** P **54** L **7** # **37**
 Sukert, Alan Xerox

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

This line was modified to indicate that removable NVS was to be protected when the "devices are removed from the protection of its environment". Line 7 is unclear from which environment removal of the NVS is to be protected.

Looking at the changes that were made in lines 14 and 16, the protection is to be for removal from the environment of the TOE. For clarify the environment referenced in line 7 should also be for protection of removal from the environment of the TOE.

SuggestedRemedy

Revise page 54, line 7 to read "...,devices are removed from the protection of the environment of the TOE."

Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-B** SC 9.1 P 15 L 24 # 33
 Sukert, Alan Xerox

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

This line now reads "FPT_CIP_EXP.1 Confidentiality and Integrity of Stored Data, provides for the protection of user and TSF data stored on storage container that..." May be more grammatically correct for the sentence to read "FPT_CIP_EXP.1 Confidentiality and Integrity of Stored Data, provides for the protection of user and TSF data stored on a storage container that..."

SuggestedRemedy

Modify page 15, line 24 as indicated above.

Proposed Response Response Status **O**

Cl **PP-B** SC 9.1 P 16 L 7 # 39
 Sukert, Alan Xerox

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

The discussion of the FTP_CIP_EXP.1 extended component defines a proposed set of actions that should be auditable for this extended component. The definition as currently stated in subclause 9.1 indicates that the event "should" be collected. In terms of specifications "should" means that it is not a requirement which implies that this is a recommended auditable event to be collected rather than a required auditable event. The discussion in subclause 9.1 doesn't indicate either way whether this auditable event is required or recommended.

SuggestedRemedy

Clarify in subclause 9.1 whether the auditable event defined for the FTP_CIP_EXP.1 extended component is recommended or required.

Proposed Response Response Status **O**

Cl **PP-B** SC 9.1 P 16 L 24 # 34
 Sukert, Alan Xerox

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

The sentence on line 24 contains a grammatical error - "...protection and integrity protection, those components are defined different for user data and TSF..." should be "...protection and integrity protection, those components are defined differently for user data and TSF..."

SuggestedRemedy

Revise page 16, line 24 as indicated above.

Proposed Response Response Status **O**

Cl **PP-B** SC 9.1 P 16 L 26 # 35
 Sukert, Alan Xerox

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

In keeping with the conventions used elsewhere in this PP, 'protection profile' on this line should be capitalized.

SuggestedRemedy

On page 16, line 26 replace "protection profile" with "Protection Profile".

Proposed Response Response Status **O**

Cl **PP-B** SC 9.1 P 16 L 33 # 36
 Sukert, Alan Xerox

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

The last paragraph on this page provides rationale why the extended component was created. The logic used in the paragraph doesn't appear to be correct - it is indicated that since it addresses the protection of TSF data, it was not viewed as appropriate to put this component into the FDP class related to user data protection; then it states that because the requirement contributes to the protection of the TSF it was appropriate to have this extended SFR be seen as a member of the FDP class; finally it is stated that the extended component does not fit well into any of the existing families within the class, which lead the authors to the definition of a new family with just one member.

What is never explained here is that the new extended component can be placed in the FTP clas because it does protect TSF data and then why it was decided to place the new extended component in the FTP class.

SuggestedRemedy

Revise the last paragraph on page 16 to make the rationale as to why the new extended component is in the FTP class clearer as indicated above.

Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security comments

CI **PP-B** SC **9.2** P **17** L **28** # **38**
 Sukert, Alan Xerox

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

The discussion of the FMT_FDI_EXP.1 extended component defines a proposed set of actions that should be auditable for this extended component. First of all it is not clear how these recommended auditable events relate to the required auditable event listed in Table 40, subclause 19.2, page 57, line 5 because (among other things) the event defined in subclause 9.2 is at the 'Basic' audit level while the auditable event in Table 40 is at the 'Minimal' auditable level. It is not clear why these auditable events are even defined here since they don't appear at all as either SMI SFR audit data requirements or recommendations.

More importantly, the definition as currently stated in subclause 9.2 indicates that the event ""should"" be collected. In terms of specifications ""should"" means that it is not a requirement which implies that this is a recommended auditable event to be collected rather than a required auditable event. The discussion in subclause 9.2 doesn't indicate either way whether this auditable event is required or recommended.

SuggestedRemedy

Clarify in subclause 9.2 whether the auditable event defined for the FMT_FDI_EXP.1 extended component is recommended or required, and show the relationship between these auditable events and the required auditable events for the SMI SFR Package shown in the indicated tables.

Proposed Response Response Status **O**

CI **PP-C** SC **11** P **30** L **4** # **40**
 Sukert, Alan Xerox

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

- In Table 19 the titles of the following SARs are incorrect:
1. ADV_FSP.2 -- It should be ""Security-enforcing functional specification""
 2. ALC_CMC.2 -- It should be ""Use of a CM system""
 3. ALC_CMS.2 -- It should be ""Parts of the TOE CM coverage""
 4. ALC_FLR.1 -- It should be ""Basic flaw remediation""
 4. ATE_COV.1 -- It should be ""Evidence of coverage""

SuggestedRemedy

Correct the titles of the SARs indicated above in Table 19.

Proposed Response Response Status **O**

CI **PP-C** SC **9.1** P **16** L **4** # **41**
 Sukert, Alan Xerox

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

The discussion of the FMT_FDI_EXP.1 extended component defines a proposed set of actions that should be auditable for this extended component. First of all it is not clear how these recommended auditable events relate to the required auditable event listed in Table 22, subclause 13.2, page 34, line 5 because (among other things) the event defined in subclause 9.2 is at the 'Basic' audit level while the auditable event in Table 22 is at the 'Minimal' auditable level. It is not clear why these auditable events are even defined here since they don't appear at all as either SMI SFR audit data requirements or recommendations.

More importantly, the definition as currently stated in subclause 9.1 indicates that the event ""should"" be collected. In terms of specifications ""should"" means that it is not a requirement which implies that this is a recommended auditable event to be collected rather than a required auditable event. The discussion in subclause 9.1 doesn't indicate either way whether this auditable event is required or recommended.

SuggestedRemedy

Clarify in subclause 9.1 whether the auditable event defined for the FMT_FDI_EXP.1 extended component is recommended or required, and show the relationship between these auditable events and the required auditable events for the SMI SFR Package shown in the indicated tables.

Proposed Response Response Status **O**

CI **PP-D** SC **9.1** P **15** L **16** # **42**
 Sukert, Alan Xerox

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

The discussion of the FMT_FDI_EXP.1 extended component defines a proposed set of actions that should be auditable for this extended component. The definition as currently stated in subclause 9.1 indicates that the event ""should"" be collected. In terms of specifications ""should"" means that it is not a requirement which implies that this is a recommended auditable event to be collected rather than a required auditable event. The discussion in subclause 9.1 doesn't indicate either way whether this auditable event is required or recommended.

SuggestedRemedy

Clarify in subclause 9.1 whether the auditable event defined for the FMT_FDI_EXP.1 extended component is recommended or required.

Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security comments

CI **PP-GUI** SC 5.2.1.1 P 21 L 18 # 18
Sukert, Alan Xerox

Comment Type T Comment Status X

In section 5.2.1.1.f, the Guide says that in a small accounting firm "there would be no real need for formal user policy", and that "it makes sense that for this type of business the P.ADMIN.AUTHORIZATION and P.AUDIT.LOGGING OSPs would not be needed, which is consistent with the OSPs for an Operational Environment D company." The error is that it says "P.ADMIN.AUTHORIZATION" where it should say "P.USER.AUTHORIZATION". (Page 26, line 18.) Correcting this error would make the argument sensible, & it would also make it consistent with the data in Table 5 (OSP's per Operational Environment).

SuggestedRemedy

Change P.ADMIN.AUTHORIZATION to P.USER.AUTHORIZATION

Proposed Response Response Status