

IEEE P2600 Hardcopy Device and System Security comments

Cl All P SC 10.1 P 18 L 4 # 7
 Smithson, Brian Ricoh

Comment Type E Comment Status X

The app note is unclear.

SuggestedRemedy

Change the completed assignment statement to:
 ""for each Relevant SFR in Table 14, (1) information as defined by its Audit Level (if one is specified) and (2) all Additional Information (if any is required)""

Proposed Response Response Status O

Cl All P SC 10.4 P 19 L 8 # 13
 Smithson, Brian Ricoh

Comment Type T Comment Status X

When referring to ""ownership"" in relation to D.FUNC, it should refer to ""jobs"" not ""documents"".

SuggestedRemedy

Change ""Denied, except for his/her own documents"" to ""Denied, except for his/her own jobs"". Similar modifications are needed in other access control SFP tables.

Add a second app note (similar to the first):
 PP APPLICATION NOTE: A job is downed by a User if that job was created or submitted to the TOE by that User, unless indicated otherwise in one of the named SFR Packages in this Standard.

Add a definition of ""job"" to Annex A:
 Job: An object that represents the submission of work for the HCD which may contain descriptive and state information as well as other elements. Jobs contain one or more Documents.

(adapted from PWG semantic model for printers)

Proposed Response Response Status O

Cl All P SC 10.4 P 19 L 8 # 4
 Smithson, Brian Ricoh

Comment Type T Comment Status X

There are some configurations in which the rules in the common access control SFP might not be satisfied. For example, restricting ""D.FUNC / Modify, Delete"" may not apply in the case of the FAX package because another user may be granted permission by an administrator to delete or modify a FAX job.

SuggestedRemedy

Perform the changes identified in the external document ""ProposedDataACSFPs.doc"".

Proposed Response Response Status O

Cl All P SC 10.4 P 19 L 20 # 8
 Smithson, Brian Ricoh

Comment Type E Comment Status X

The table referenced in the fourth app note after the Common AC SFP is incorrect. Also, for consistency, ""table"" should be capitalized.

SuggestedRemedy

Point to the correct table, and capitalize Table.

Proposed Response Response Status O

Cl All P SC 10.4 P 22 L 6 # 9
 Smithson, Brian Ricoh

Comment Type E Comment Status X

The app note after FDP_ACF.1.4(b) should refer to FDP_ACF.1(b)

SuggestedRemedy

Change ""FDP_ACF.1"" to ""FDP_ACF.1(b)"".

Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security comments

Cl All P SC 17.2 P 50 L 23 # 5
 Smithson, Brian Ricoh

Comment Type E Comment Status X

The extended component definitions should appear in the PP (clause 9), not in the SFR packages. This aligns the ECDs with the work packages required in the CEM for ECDs.

SuggestedRemedy

Move the ECDs from 17.2 and 18.2 into clause 9. Change the ""Common Criteria conformance"" statement in clause 3.2 to say ""Part 2 extended, Part 3 conformant"", and make the same change in 11.2 for the NVS and SMI packages.

Proposed Response Response Status O

Cl All P SC 17.2 P 50 L 48 # 12
 Smithson, Brian Ricoh

Comment Type T Comment Status X

The ECDs in the NVS and SMI packages recommend some management and audit functions. These should be consider by the WG to see if we want to require or recommend any of them. If we require or recommend, then we'll need to add FMT_SMF.1 and/or FAU_GEN.1 to those packages (FAU_GEN.1 is already in SMI).

SuggestedRemedy

Review the management and audit functions, and discuss and decide in the WG.

Proposed Response Response Status O

Cl All P SC 17.2 P 51 L 10 # 10
 Smithson, Brian Ricoh

Comment Type E Comment Status X

List item designation is incorrect.

SuggestedRemedy

Change the item designation from ""c"" to ""a"" (i.e., restart the list numbering).

Proposed Response Response Status O

Cl All P SC 17.2 P 51 L 15 # 11
 Smithson, Brian Ricoh

Comment Type T Comment Status X

Some kinds of data do not require confidentiality protection, and so the definition of FTP_CIP_EXP should allow selection and then the instantiation of the SFR should refine it.

SuggestedRemedy

Change ""ensures the confidentiality and integrity of"" to ""ensures the [selection: confidentiality, integrity] of"".

Then in 17.3, iterate the SFR. For O.DOC and O.CONF, specify ""confidentiality and integrity"", and for O.FUNC and O.PROT, specify ""integrity"".

Apply similarly to PP-B.

Proposed Response Response Status O

Cl All P SC 19 P 58 L 1 # 14
 Smithson, Brian Ricoh

Comment Type E Comment Status X

The SAR part of APE_REQ should appear in the common PP, after the SFR part of APE_REQ.

SuggestedRemedy

Move clause 19 to appear between 10 and 11. Similar move for the other PPs.

Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security comments

Cl All P SC 19 P 58 L 4 # 15
 Smithson, Brian Ricoh

Comment Type T Comment Status X

[NIAP] After consulting with some colleagues, a question came up about the Security Assurance Requirements (SAR)s in the P2600.1 PP. Has anyone in the working group looked at the Common Criteria Evaluation Methodology (CEM) to see how it would apply to the P2600.1 PP and the products that claim compliance to that PP? Would there be any application notes that you or the working group could/should add to the PP to ensure that the SARs associated with the evaluated product have met the intent of the PP as well as the assurance level. In addition, to ensure consistency among the different labs, there may be specific assurance items that you or the working group might want to emphasize or elaborate on in the PP that will be address when evaluating the products assurance.

SuggestedRemedy

Consider NIAP's request.

Proposed Response Response Status O

Cl All P SC 5.1 P 6 L 23 # 1
 Smithson, Brian Ricoh

Comment Type T Comment Status X

The definition of ""shared-medium interfaces"" on this line is different from the definition in 5.3.4. The definition in 5.3.4 is more correct because the intention is that shared-medium interfaces can be shared_simultaneously_ by multiple users.

SuggestedRemedy

Change: ""that are or can be shared by other users""

To: ""which, in conventional practice, is or can be simultaneously accessed by multiple Users""

Applies to 5.1, 11.2, 11.3, and similar sections in PP-B/C/D.

Proposed Response Response Status O

Cl All P SC 7.3 P 12 L 1 # 2
 Smithson, Brian Ricoh

Comment Type T Comment Status X

References to the TOE's ""operational environment"" (unless referring to the IEEE 2600 operational environments, e.g. A B C or D) should be changed to specify the IT environment or the non-IT environment. This will help disambiguate what has become an overloaded term, and will clarify whether the IT or non-IT environment is expected.

SuggestedRemedy

In 7.3 P12 L1, 8.3 P14 L10, and 10.5 P23 L10 and L23 : change ""operational environment"" to ""IT environment"".

In 17.1 P50 L7, L14 and L16: change ""operational environment"" to ""non-IT environment"".

Also change similar sections in PP-B/C/D.

Proposed Response Response Status O

Cl All P SC 8.2 P 14 L 5 # 3
 Smithson, Brian Ricoh

Comment Type E Comment Status X

""Security objectives for the development environment"" is not part of CCv3.1. It was part of 3.0. We have no such objectives anyway.

SuggestedRemedy

Remove clause 8.2. Similar change is needed in PP-B/C/D.

Proposed Response Response Status O

Cl All P SC 8.3 P 14 L 10 # 6
 Smithson, Brian Ricoh

Comment Type E Comment Status X

In the definition of OE.AUDIT_ACCESS.AUTHORIZED, the word ""analyzed"" could be misinterpreted to imply some analysis functions (like FAU_SAA.*) that are not actually intended as requirements.

SuggestedRemedy

Change ""analyzed"" to ""accessed"".

Proposed Response Response Status O

IEEE P2600 Hardcopy Device and System Security comments

Cl Guide SC 0 P iv L 9 # 16
 Smithson, Brian Ricoh
Comment Type E **Comment Status** X
 Alan, you are the lead editor!
SuggestedRemedy
 Change ""Brian Smithson, Secretary and Lead Editor"" to ""Brian Smithson, Secretary
 <newline> Alan Sukert, Lead Editor"", and remove line 23.
Proposed Response **Response Status** O

Cl Guide SC 1.2 P 3 L 21 # 18
 Smithson, Brian Ricoh
Comment Type E **Comment Status** X
 Use of the word ""consumer"" appears in the list heading and also in one of the list items.
SuggestedRemedy
 Change ""primary consumer groups"" to ""primary groups"".
Proposed Response **Response Status** O

Cl Guide SC 1.2 P 3 L 24 # 17
 Smithson, Brian Ricoh
Comment Type E **Comment Status** X
 For consistency and clarity, use ""compliance"" to refer to compliance with IEEE 2600, and
 use ""conformance"" to refer to STs that conform to the 2600-series PPs.
SuggestedRemedy
 Change ""are compliant with"" to ""conform to"". Similar change is suggested wherever
 these terms are used elsewhere in the document.
Proposed Response **Response Status** O

Cl Guide SC 1.2 P 3 L 26 # 19
 Smithson, Brian Ricoh
Comment Type E **Comment Status** X
 Sentence is a little convoluted.
SuggestedRemedy
 Change ""Vendors and HCD Developers: Providers (e.g., product vendors, integrators, and
 value-added
 27 resellers), product developers and security analysts of Hardcopy Devices.""
 To ""HCD developers, providers, and analysts: Hardcopy Device product developers,
 providers (e.g., product vendors, integrators, and value-added resellers), and security
 analysts.""
Proposed Response **Response Status** O

Cl Guide SC 2.1 P 5 L 17 # 20
 Smithson, Brian Ricoh
Comment Type E **Comment Status** X
 CCRA only works up to EAL4.
SuggestedRemedy
 Indicate the limitation (with some forward reference to whatever ""EAL"" means).
Proposed Response **Response Status** O

Cl Guide SC 2.1 P 5 L 36 # 21
 Smithson, Brian Ricoh
Comment Type E **Comment Status** X
 Should the annex in 2600.1/2/3/4 also be mentioned? They have terms that are specific to
 the 2600-series PPs. Or are we keeping the Guide Annex A in sync with the PP Annex A?
SuggestedRemedy
 Include PP terms in the Guide's Annex A, or make reference to the PP's Annex A on this
 line.
Proposed Response **Response Status** O

IEEE P2600 Hardcopy Device and System Security comments

Cl Guide SC 4 P 14 L 1 # 22
 Smithson, Brian Ricoh
Comment Type E **Comment Status** X
 Who is responsible for this section!? It's content-free!!
SuggestedRemedy
 Get that guy to work...
Proposed Response **Response Status** O

Cl Guide SC 5.2.1.1 P 15 L 6 # 27
 Smithson, Brian Ricoh
Comment Type E **Comment Status** X
 It seems to me that the discussions in this section go beyond describing how the PPs remain independent of implementation because they describe how the ST author might go about using the PP to describe their particular implementation. I think that the topics are good, but the discussion is too deep.
SuggestedRemedy
 Describe the topics more generally and provide pointers to the appropriate section under 5.2.2 in which the implementation discussion takes place. Otherwise, I think we'll have scattered, duplicated, or possibly conflicting advice.
Proposed Response **Response Status** O

Cl Guide SC 5.2.1.1.1 P 15 L 11 # 23
 Smithson, Brian Ricoh
Comment Type T **Comment Status** X
 It is not quite accurate to say that the equivalent or more restrictive solution is based on the requirements of those specific SFRs. The solution must fulfill objectives that are equivalent or more restrictive than the OE objectives (OE.AUDIT_STORAGE.PROTECTED and OE.AUDIT_ACCESS.AUTHORIZED). The SFRs listed in the app note are suggested, and would probably be used, but the real rule is that the ST author must add objectives and then fulfill them.
SuggestedRemedy
 Reword the paragraph accordingly...
Proposed Response **Response Status** O

Cl Guide SC 5.2.1.1.1 P 15 L 15 # 24
 Smithson, Brian Ricoh
Comment Type T **Comment Status** X
 This clause should also address the case in which audit data can be stored inside OR outside of the TOE, as an administrator option.
SuggestedRemedy
 In case both options are available, then the ST author must add objectives (see related comment about that), AND the ST author must define internal and external audit storage as separate modes of operation so that each mode is evaluated.

Other combinations are possible, including storage inside but access outside, or even storage outside but access inside (I think someone mentioned this case to me a little while ago). So it may be best to handle storage and access as individual items, each having the cases (1)inside, (2)outside, and (3) both.
Proposed Response **Response Status** O

Cl Guide SC 5.2.1.1.2 P 15 L 32 # 25
 Smithson, Brian Ricoh
Comment Type T **Comment Status** X
 There is another option: a third-party product that itself is CC certified. In this case, the HCD vendor would need to compose the TOE's certification and the third-party product's certification.
SuggestedRemedy
 Composition is tricky and not well documented. I'm not sure what to suggest...
Proposed Response **Response Status** O

Cl Guide SC 5.2.1.1.3 P 16 L 13 # 26
 Smithson, Brian Ricoh
Comment Type T **Comment Status** X
 It should be mentioned that if the trusted path is implemented entirely in a third-party network interface device, then the certification options are similar to those previously stated in 5.2.1.1.2: (1) certify the third-party product, which requires some cooperation with the third-party vendor, (2) compose the TOE with an already certified third-party product, or (3) you can't claim conformance.
SuggestedRemedy
 Add some discussion of these options.
Proposed Response **Response Status** O

IEEE P2600 Hardcopy Device and System Security comments

Cl Guide SC 5.2.1.1.4 P 16 L 14 # 28
 Smithson, Brian Ricoh
Comment Type T **Comment Status** X
 There is an additional topic to discuss for I&A in an enterprise environment: internal I&A vs. external I&A versus both.
SuggestedRemedy
 Add to this section, or create a separate section, that describes the choice of internal, external, or both. The issues are similar to those found in internal versus external audit data storage/access.
Proposed Response **Response Status** O

Cl Guide SC 5.2.2.2.1 P 18 L 37 # 29
 Smithson, Brian Ricoh
Comment Type E **Comment Status** X
 This clause seems out of place.
SuggestedRemedy
 Figure out where it belongs and put it there.
Proposed Response **Response Status** O

Cl Guide SC 5.2.2.2.1 P 19 L 2 # 30
 Smithson, Brian Ricoh
Comment Type T **Comment Status** X
 Testing for an external timestamp source would not be part of FPT_TST, it would be part of FPT_TEE.
SuggestedRemedy
 Replace ""either locally or from an outside source"" with ""from a local time source"".
Proposed Response **Response Status** O

Cl Guide SC 5.2.2.2.1 P 19 L 4 # 31
 Smithson, Brian Ricoh
Comment Type T **Comment Status** X
 I don't think that a random file would be a good example of testing encryption/decryption. A random file could be used to test if a file can be encrypted and then decrypted to the same data, but specific files would be needed to test encryption and decryption to and from known plaintext and ciphertext files.
SuggestedRemedy
 Remove ""using a random file"" or give better examples.
Proposed Response **Response Status** O

Cl Guide SC 5.2.2.2.1 P 19 L 8 # 32
 Smithson, Brian Ricoh
Comment Type T **Comment Status** X
 This (integrity checking of code) is the REQUIRED part of the SFR in the PPs. The other examples are optional.
SuggestedRemedy
 Modify the preceding paragraph to describe what is required by the SFR, and then give the other five items as examples of optional tests that could be included in FPT_TST.
Proposed Response **Response Status** O

Cl Guide SC 5.2.2.3 P 19 L 22 # 33
 Smithson, Brian Ricoh
Comment Type T **Comment Status** X
 I think that there could be a more clear-cut relevant example of protected versus confidential. For example, a user's password is clearly something that should be confidential, but a user's email address only needs to be protected. Outside of the TOE, an email address is necessarily public information, so confidentiality isn't useful, but inside the TOE, changing someone's email address could cause a security breach.
SuggestedRemedy
 Consider using a different example for protected versus confidential.
Proposed Response **Response Status** O

IEEE P2600 Hardcopy Device and System Security comments

Cl Guide SC 5.2.2.7 P 29 L 15 # 38
 Smithson, Brian Ricoh
Comment Type E **Comment Status** X
 This is a HUGE section with no subheadings.
SuggestedRemedy
 Consider restructuring. So as not to make it too deep (five or more levels becomes unwieldy), maybe there needs to be some higher-level restructuring as well.
Proposed Response **Response Status** O

Cl Guide SC 5.2.2.7 P 30 L 10 # 36
 Smithson, Brian Ricoh
Comment Type T **Comment Status** X
 An ST Author may increase the EAL and/or augment with additional SARs if they wish.
SuggestedRemedy
 Restate this section as a minimum conformance requirement.
Proposed Response **Response Status** O

Cl Guide SC 5.2.2.7 P 29 L 34 # 34
 Smithson, Brian Ricoh
Comment Type E **Comment Status** X
 Basic contents and format requirements of an ST are better described in CC part 1 and CEM and the ISO TR15446 ""Guide to PPs and STs"". Should we really try to replicate that information in the guide?
SuggestedRemedy
 Consider referring the ST author to other documents for general information about ST construction.
Proposed Response **Response Status** O

Cl Guide SC 5.2.2.7 P 30 L 14 # 37
 Smithson, Brian Ricoh
Comment Type T **Comment Status** X
 Additional discussion of when an ST must conform to each package would be very useful here (or elsewhere, referred to from here)
SuggestedRemedy
 Add sections describing the rules for package conformance requirements, with examples?
Proposed Response **Response Status** O

Cl Guide SC 5.2.2.7 P 30 L 5 # 35
 Smithson, Brian Ricoh
Comment Type T **Comment Status** X
 I am not sure if this is exactly correct. If we put the ECDs in the Common PP (as is suggested in a comment against the PPs), then the PP would be Part 2 Extended, and I think a conforming ST would might also be Part 2 Extended even if it only defines the ECDs but does not use them. This is a question for a lab...
SuggestedRemedy
 Check on this issue, it may be more simple to say that all conforming STs are Part 2 Extended (if the ECDs are moved into the Common PP).
Proposed Response **Response Status** O

Cl Guide SC 5.2.2.7 P 34 L 14 # 39
 Smithson, Brian Ricoh
Comment Type E **Comment Status** X
 There is an ""if"" (if the audit records are exported...), but there is no ""else"". It does appear on line 33, but it would be more clear if these cases were described in closer proximity.
SuggestedRemedy
 Discuss audit detail first, then internal/external second.
Proposed Response **Response Status** O

IEEE P2600 Hardcopy Device and System Security comments

Cl Guide SC 5.2.2.7 P 34 L 20 # 40
 Smithson, Brian Ricoh

Comment Type T **Comment Status** X

The audit level can be specified as ""not specified"". This is likely the case for most HCDs, because we found that even the ""minimal"" level as defined in the CC requires more audit event capture than is really useful or relevant for HCDs.

SuggestedRemedy

Allow ""not specified"", and give some discussion about why that is an acceptable specification. It gets confusing because our ""minimum"" requirement is not the same as the CC-defined ""minimal"" requirement.

Proposed Response **Response Status** O

Cl Guide SC 5.2.2.7 P 35 L 18 # 43
 Smithson, Brian Ricoh

Comment Type E **Comment Status** X

It may be worth giving some explanation or examples to clarify the composition of FDP_ACF rules. For example, if an ST conforms to the PRT then the product must perform the access controls specified by both the Common PP and the PRT package.

SuggestedRemedy

Consider adding explanation and examples of access control composition for PP and packages. Also note that a comment has been submitted against the PPs that would remove the rules from the common PP and place all rules in the packages.

Proposed Response **Response Status** O

Cl Guide SC 5.2.2.7 P 34 L 20 # 41
 Smithson, Brian Ricoh

Comment Type T **Comment Status** X

The CC-defined audit level is called ""minimal"", not ""minimum"".

SuggestedRemedy

Change references to ""minimum"" audit level to ""minimal"".

Proposed Response **Response Status** O

Cl Guide SC 5.2.2.7 P 35 L 41 # 44
 Smithson, Brian Ricoh

Comment Type T **Comment Status** X

There should be a section describing the access control rules for HCD functions.

SuggestedRemedy

Add a section for the HCD function access control rules.

Proposed Response **Response Status** O

Cl Guide SC 5.2.2.7 P 34 L 28 # 42
 Smithson, Brian Ricoh

Comment Type T **Comment Status** X

There are three parts to the audit requirement: (1) whatever the ST author specifies in FAU_GEN.1.1 by choosing an audit level and optionally adding additional events; (2) the events listed in the Audit Data Requirement table, and (3) the optional events listed in the Audit Data Recommendations table. These need a lot of explanation...

SuggestedRemedy

Explain that the ultimate requirement is composed of (1) and (2). If the ST puts ""not specified"" in (1) and does not add any events, then they will only need to fulfill the items in (2). If the ST author chooses ""minimal"" or one of the other CC-defined audit levels in (1), or if they add events, then they will need to reconcile that choice with the items in (2). Note that even if the ST author chooses ""minimal"", if an audit item in (2) specifies ""basic"" then the ST will still need to fulfill the ""basic"" audit requirement for that item. Some examples would probably be pretty helpful.

Proposed Response **Response Status** O

Cl Guide SC 6.1 P 40 L 40 # 46
 Smithson, Brian Ricoh

Comment Type T **Comment Status** X

I am not sure that this is the escalation path for questions. I think that the certifying scheme gets the question first. I do not think that the lab gets involved. If the scheme needs to contact someone, I think that they contact the PP sponsor (that is a CC-type sponsor, in this case it would be the IEEE P2600 WG).

SuggestedRemedy

Ask NIAP or atsec for clarification.

Proposed Response **Response Status** O

IEEE P2600 Hardcopy Device and System Security comments

CI **Guide** SC **6.1** P **41** L **11** # **47**
 Smithson, Brian Ricoh

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

Does this question mean ALL certified products, or just those that are certified against 2600-series PPs? If the latter, then the answer is still valid but I thought we had plans to list certified products on an IEEE web site.

SuggestedRemedy

Clarify if this question means ALL products or just 2600-certified products (maybe handle both in separate questions), and for 2600-certified products consider adding some placeholder to point to the IEEE site.

Proposed Response Response Status **O**

CI **Guide** SC **6.2** P **41** L **30** # **45**
 Smithson, Brian Ricoh

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

This is not quite accurate. Any HCD that has PRT, FAX, or DSR functions, must provide some method of authentication before releasing jobs to hardcopy output (in environments A and B). "PIN printing" is one implementation that should satisfy the authentication requirement. Note also that if, for example, someone prints from a local source like a USB flash memory device, they would have authenticated first to initiate the printing function and would not be required to re-authenticate to release output (unless for some reason their session is no longer active).

SuggestedRemedy

Clarify this FAQ item.

Proposed Response Response Status **O**

CI **Guide** SC **6.2** P **42** L **14** # **48**
 Smithson, Brian Ricoh

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

I think that items (d) through (h) would be better described in other sections, not in the FAQ. They are good questions and answers, but they overlap with topics in other sections.

SuggestedRemedy

Consider moving these Qs and As to earlier sections.

Proposed Response Response Status **O**

CI **PP-A** SC **10.1** P **18** L **9** # **49**
 Smithson, Brian Ricoh

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

The audit data requirements "unsuccessful use of..." and "successful use of..." for FIA_UAU and FIA_UID are redundant, because the Basic level of audit requires "all use of...". There is no need to specify these as separate auditable event requirements.

SuggestedRemedy

Change "Unsuccessful use of the authentication mechanism" to "Use of the authentication mechanism".

Remove the row "Successful use of the authentication mechanism".

Change "Unsuccessful use of the identification mechanism" to "Use of the identification mechanism".

Remove the row "Successful use of the identification mechanism".

Proposed Response Response Status **O**

CI **PP-A** SC **10.12** P **29** L **18** # **51**
 Chen, Nancy Oki Data

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

Table 18 completeness of Security Requirements.

FDP_ACC.1(b), FDP_ACF.1(b), FMT_MSA.1(b), and FMT_MSA.3(b) enforce TOE

Function Access Control SFP, therefore indirectly enforce access control to D.DOC that described in individual SFR packages later.

SuggestedRemedy

Add FDP_ACC.1(b), FDP_ACF.1(b), FMT_MSA.1(b), and FMT_MSA.3(b) as secondary support for O.DOC.NO_DIS & O.DOC.NO_ALT.

Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-A** SC **10.12** P **30** L **1** # **52**
 Chen, Nancy Oki Data

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

Table 19 Sufficiency of Security Requirements. FDP_ACC.1(b), FDP_ACF.1(b), FMT_MSA.1(b), and FMT_MSA.3(b) enforce TOE Function Access Control SFP, therefore indirectly enforce access control to D.DOC that described in individual SFR packages later.

SuggestedRemedy

- (1) Add FDP_ACC.1(b), FDP_ACF.1(b), FMT_MSA.1(b), and FMT_MSA.3(b) to sufficiency rationales for O.DOC.NO_DIS & O.DOC.NO_ALT.
- (2) Clarify the description of rationale as such.

Proposed Response Response Status **O**

Cl **PP-A** SC **10.4** P **19** L **33** # **62**
 Sukert, Alan Xerox

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

The App Note for FDP_ACC.1(a) indicates that FDP_ACC.1 is a dependency of both FDP_ACF.1 and FMT_MSA.1. Since there are FDP_ACF.1(a) and FDP_ACF.1(b) as well as FMT_MSA.1(a) and FMT_MSA.1(b) it is confusing whether this dependency only applies to one or both of the SFRs in each case.

A similar comment applies to the APP Note for FDP_ACC.1(b) in subclause 10.4, page 20, line 19.

SuggestedRemedy

Clarify these two App Notes to indicate exactly which specific SFRs FDP_ACC.1(a) and FDP_ACC.1(b) are a dependency of.

Proposed Response Response Status **O**

Cl **PP-A** SC **10.4** P **22** L **9** # **59**
 Sukert, Alan Xerox

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

Grammatical error -- says "...allowing all functions for all user authorized to use the TOE..."

SuggestedRemedy

Change to either "...allowing all functions for all users authorized to use the TOE..." or "...allowing all functions for a user authorized to use the TOE..."

Proposed Response Response Status **O**

Cl **PP-A** SC **10.6** P**27** L**14** # **70**
 Farrell, Lee

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

Since pseudo role "Nobody" may not exist if no selection is made in other SFR's "selection", FMR_SMR.1.1 should not mandate pseudo role "Nobody".

SuggestedRemedy

Remove "Nobody" from mandatory assignment and leave it to ST author, or place "Nobody" within assignment.

Proposed Response Response Status **O**

Cl **PP-A** SC **10.6** P**27** L**14** # **69**
 Farrell, Lee

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

Since both "APPLICATION NOTE"s and "Annex A Glossary (Informative)" are *NOT* normative parts of the standard, the pseudo role "Nobody" should be defined somewhere in the normative part.

SuggestedRemedy

Define "Nobody" in normative part instead of explaining it in informative annex or application notes that are not part of the formal specification statement.

Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security comments

CI **PP-A** SC 11.2 P 34 L 27 # 60
 Sukert, Alan Xerox

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

In the description of the P2600.1-NVS SFR package, there is a statement that if the protection is supplied by the TOE environment and not the TOE itself, the package cannot be claimed. Although this may seem repetitive, the way the statement is phrased it could be interpreted that if the protection involved is done by both the TOE environment and the TOE then the SFR package can not be claimed, which I believe is not the intent here - the package cannot be claimed only in the case where the protection is only provided by the TOE environment.

A similar comment applies to the corresponding statement for the P2600.1-SMI SFR package in subclause 11.2, page 34, line 40.

SuggestedRemedy

Suggest the two indicated sentences read "...If such protection is supplied by only the TOE environment and not the TOE itself, this package cannot be claimed."

Proposed Response Response Status **O**

CI **PP-A** SC 12.2 P 36 L 15 # 63
 Sukert, Alan Xerox

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

Possible grammatical error - This sentence says that "...If the User authenticated using Operator Panel when submitting a print job...". Authenticated in this context is a verb so the sentence as stated is not grammatically correct.

SuggestedRemedy

Suggest restating as either "...If the User was authenticated using the Operator Panel when submitting a print job..." or "...If the User authenticated and submitted the print job using the Operator Panel ..." (as is done later in this statement).

Proposed Response Response Status **O**

CI **PP-A** SC 15.2 P 44 L 28 # 64
 Sukert, Alan Xerox

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

The APP Note on this line has a couple of grammatical errors that need correction. Currently it states "...to manage the transmission of or delete outgoing fax documents, ... that permit the administrator to Read or Delete..."

In the first case the tenses of the two verbs are not consistent; in the second case permit is a verb associated with rule so it should be singular.

SuggestedRemedy

Suggest changing this note to read "...to manage the transmission or deletion of outgoing fax documents, ... that permits the administrator to Read or Delete..."

Proposed Response Response Status **O**

CI **PP-A** SC 15.2 P 44 L 32 # 65
 Sukert, Alan Xerox

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

Grammatical error -- This APP Note states "...before creating hardcopy output or transmission, then the ST Author..." I believe the sentence as currently written doesn't indicate what is being transmitted here.

SuggestedRemedy

Suggest revising to read "...before creating hardcopy output or transmitting outgoing fax documents, then the ST Author..."

Proposed Response Response Status **O**

CI **PP-A** SC 17.2 P 50 L 30 # 66
 Sukert, Alan Xerox

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

Here and elsewhere with subclause 17.2 user data is not capitalized. I believe our convention elsewhere in the document has been that when referring to the entity described in subclause 5.3 the term user data is capitalized.

SuggestedRemedy

capitalize 'User Data' here and elsewhere with subclause 17.2 when used as the entity described in subclause 5.3.

Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-A** SC **18.2** P **54** L **14** # **67**
 Sukert, Alan Xerox

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

The discussion of the FMT_FDI_EXP.1 extended SFR is focused around forwarding of data from one external interface to another. I checked both IEEE Std 2600-2008 and Annex A of this document and there is no definition of "external interface". I know we had decided to delete it from IEEE Std 2600 previously but since the concept of what an external interface is becomes critical to understanding this new extended SFR, I believe we should add a definition of external interface to Annex A so the discussion of FMT_FDI_EXP.1 becomes clear to an ST author.

SuggestedRemedy

Add a definition of external interface to Annex A that is something like:

External Interface: An interface where either the input is being received from outside the HCD or the output is being delivered outside the HCD.

Proposed Response Response Status **O**

Cl **PP-A** SC **18.2** P **55** L **14** # **68**
 Sukert, Alan Xerox

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

Grammatical error -- Sentence states "Quite often a TOE is supposed to perform specific checks process data received on one external interface...". This sentence as stated is incorrect.

SuggestedRemedy

Revise the sentence to read something like "Quite often a TOE is supposed to perform specific checks on process data received on one external interface...".

Proposed Response Response Status **O**

Cl **PP-A** SC **5.1** P **6** L **19** # **61**
 Sukert, Alan Xerox

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

Grammatical error - says "...on a nonvolatile storage devices that..."

SuggestedRemedy

Change to either "...on a nonvolatile storage device that..." or "...on nonvolatile storage devices that..."

Proposed Response Response Status **O**

Cl **PP-A** SC **50** P**17.1** L **6** # **53**
 Chen, Nancy Oki Data

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

In NVS package Introduction: "protection for User Data and TSF Data that is stored on Removable Nonvolatile Storage devices when such devices are removed from the operational environment".
 Shouldn't this be "when such devices are removed from the TOE" instead of the operational environment?

The same needs to be fixed in PP-B

SuggestedRemedy

Change "operational environment" to "TOE".

Proposed Response Response Status **O**

Cl **PP-A** SC **8.5** P **16** L **0** # **50**
 Chen, Nancy Oki Data

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

Table 13 Security Objective Rationale.
 OE.INTERFACE.MANAGED is mapped to P.INTERFACE.MANAGED. But in PP-B, PP-C, and PP-D it is mapped to both P.INTERFACE.MANAGED and A.ACCESS.MANAGED.

SuggestedRemedy

Please make sure it's consistent among all PPs.

Proposed Response Response Status **O**

Cl **PP-B** SC **10.12** P **28** L **17** # **55**
 Chen, Nancy Oki Data

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

Table 18 completeness of Security Requirements.
 FDP_ACC.1(b), FDP_ACF.1(b), FMT_MSA.1(b), and FMT_MSA.3(b) enforce TOE Function Access Control SFP, therefore indirectly enforce access control to D.DOC that described in individual SFR packages later.

SuggestedRemedy

Add FDP_ACC.1(b), FDP_ACF.1(b), FMT_MSA.1(b), and FMT_MSA.3(b) as secondary support for O.DOC.NO_DIS & O.DOC.NO_ALT.

Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-B** SC **10.12** P **29** L **1** # **56**
 Chen, Nancy Oki Data

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

Table 19 Sufficiency of Security Requirements.
 FDP_ACC.1(b), FDP_ACF.1(b), FMT_MSA.1(b), and FMT_MSA.3(b) enforce TOE
 Function Access Control SFP, therefore indirectly enforce access control to D.DOC that
 described in individual SFR packages later.

SuggestedRemedy

- (1) Add FDP_ACC.1(b), FDP_ACF.1(b), FMT_MSA.1(b), and FMT_MSA.3(b) to sufficiency
 rationales for O.DOC.NO_DIS & O.DOC.NO_ALT.
- (2) Clarify the description of rationale as such.

Proposed Response Response Status **O**

Cl **PP-B** SC **8.5** P **14** L **1** # **54**
 Chen, Nancy Oki Data

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

Table 13 Security Objective Rationale.
 OE.INTERFACE.MANAGED is mapped to P.INTERFACE.MANAGED and
 A.ACCESS.MANAGED. In PP-A, OE.INTERFACE.MANAGED is only mapped to
 P.INTERFACE.MANAGED.

SuggestedRemedy

Please make sure it's consistent among all PPs.

Proposed Response Response Status **O**

Cl **PP-C** SC **8.5** P **14** L **16** # **57**
 Chen, Nancy Oki Data

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

Table 13 Security Objective Rationale.
 OE.INTERFACE.MANAGED is mapped to P.INTERFACE.MANAGED and
 A.ACCESS.MANAGED. In PP-A, OE.INTERFACE.MANAGED is only mapped to
 P.INTERFACE.MANAGED.

SuggestedRemedy

Please make sure it's consistent among all PPs.

Proposed Response Response Status **O**

Cl **PP-D** SC **8.5** P **14** L **4** # **58**
 Chen, Nancy Oki Data

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

Table 11 Security Objective Rationale.
 OE.INTERFACE.MANAGED is mapped to P.INTERFACE.MANAGED and
 A.ACCESS.MANAGED. In PP-A, OE.INTERFACE.MANAGED is only mapped to
 P.INTERFACE.MANAGED.

SuggestedRemedy

Please make sure it's consistent among all PPs.

Proposed Response Response Status **O**