

IEEE P2600 Hardcopy Device and System Security comments

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

Comment Type **G** Comment Status **D**

[Overall]
 The comments we made for assets, threats, OSPs, assumes or objective policies have not been accepted until now. So, this time we make comments from the security function point of view so as to realize objective policies. In short, we focus on the issues when we implement the security functions.

Please note that we need to complement the contents that are required in work units APE_SPD.1-2, APE_SPD.1-3, APE_SPD.1-4 and APE_OBJ.2-* since the threat descriptions, OSPs, assumes and objective policies in P2600.1-30a.pdf do not satisfy the work units.

Since we have not yet confirmed the contents regarding the work units APE_INT.* and APE_CCL.*, we will make comments from time to time if description is not proper.

SuggestedRemedy

Proposed Response Response Status **W**

PROPOSED REJECT.

APE_SPD.1-2 threats are described in terms of agent (unauth person), asset (e.g. user doc data), and adverse action (disclosed)

APE_SPD.1-3 OSPs are clearly understandable and traceable to objectives that are derived from OSPs

APE_SPD.1-4 assumptions are clearly described

Cannot act on this without specifics: how does the current draft not fulfill the work unit, and what is your suggested remedy?

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

Comment Type **T** Comment Status **R**

P.ADMIN.AUTHORIZATION and O.ADMIN.AUTHORIZED are not necessary. P.ADMIN.AUTHORIZATION requires administrator authorization, and O.ADMIN.AUTHORIZATION counters it. Normally, administrator has an ability to operate TOE security management function. Since the security management function needs to be specified in association with security function, administrator authorization is inevitably required.

SuggestedRemedy

Delete P.ADMIN.AUTHORIZATION and O.ADMIN.AUTHORIZED

Response Response Status **C**

REJECT.

Solution to comment #18 addresses this problem without adopting the suggested remedy.

CI **PP-A** SC P **71** L # 1
 aubry, carmen oce

Comment Type **E** Comment Status **A**

Table 47 CPY Audit data requirements Unsuccessful attempt to use trusted path

There is no trusted path requirement for the copy TOE!

SuggestedRemedy

Remove this item.

Response Response Status **C**

ACCEPT.

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-A** SC P 105 L # 4
 aubry, carmen oce

Comment Type **E** Comment Status **R**

Table 102 Assets not applicable to the SMI TOE:

I don't know if we still need to include it (we said that the TOE will protect data with a given security attribute, like D.DOC(+OTHERTOE).TRANSIT). In any case, with the current names (D.DOC.REST, ..) it might be unclear.

SuggestedRemedy

Remove the table.

Response Response Status **C**

REJECT.

For consistency purposes, any asset.state in the general model that is not considered in each TOE is listed as "not applicable" in that TOE. We could consider removing that table from all TOEs, but I would prefer to leave it up to an evaluator to consider.

Cl **PP-A** SC P 109 L # 2
 aubry, carmen oce

Comment Type **E** Comment Status **A**

Table 70 Assets not applicable to the DSR TOE
 "D.DOC.JOB There is no User access to User Document Data after the job has been submitted"

I'm not comfortable with this explanation because the DSR model says: "The Originator or an authorized Delegate retrieves User Document Data from the TOE". Consequently, there is user access to User Document Data.

SuggestedRemedy

In my opinion, this asset is not applicable to this model because the DSR model by its definition does not include this state. The DSR model considers only documents stored by a job that are retrieved by a subsequent job, the are no "User Document Data in the TOE awaiting or processing a job"

Response Response Status **C**

ACCEPT IN PRINCIPLE.

In the DSR case, a "job" either (1) submits a document for later retrieval or (2) retrieves a document that was previously submitted. In case (1), user doesn't have access to the document (D.DOC.JOB) unless they submit another job to retrieve it. In case (2), I suppose they do have access (according to the definition of D.DOC.JOB, anyway).

Maybe the definition needs to change?

Cl **PP-A** SC P 128 L 4 # 3
 aubry, carmen oce

Comment Type **E** Comment Status **A**

The Nonvolatile Storage TOE is composed of the essential processing elements required to prevent the recovery of deleted Document data from nonvolatile storage devices which might be removed and analyzed by unauthorized persons.

I don't think that this definition is complete because it only speaks about "recovery of deleted data".

SuggestedRemedy

Remove "deleted" part and say:

"The Nonvolatile Storage TOE is composed of the essential processing elements required to prevent the recovery of Document data from nonvolatile storage devices which might be removed and analyzed by unauthorized persons"

Response Response Status **C**

ACCEPT.

Cl **PP-A** SC P 129 L 4 # 8
 aubry, carmen oce

Comment Type **T** Comment Status **A**

Major security features of NVS:
 "User Document Data are protected from offline salvage by unauthorized persons"

I think that NVS is somehow similar with SMI when it comes to protecting other TOE's s User Document Data. NVS by itself doesn't know what User Document Data is! NVS acts on behalf of other Subjects to protect data flagged with a given security attribute by another subject (it will do an overwrite or it will encrypt data flagged with a given security attribute).

SuggestedRemedy

For consistency, I would suggest using something similar with SMI when defining the security feature of NVS:

"The NVS TOE can protect User Data of the Subject of another TOE from offline salvage by unauthorized persons."

This would generate only asset name changes (Table 84 User Data assets of NVS TOE, Table 87 Threats to User Data for the NVS TOE, Table 91 NVS Security objectives, Table 93 NVS objectives rationale), the SRRs are the same.

Response Response Status **C**

ACCEPT.

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-A** SC P 152 L # 6 [REDACTED]
 aubry, carmen oce

Comment Type **E** Comment Status **A**

In Table 107 Security objectives for the SMI TOE:
 the names for the security objectives are changed but they are not changed in Table 110
 uSMI objectives rationale.

SuggestedRemedy

Either change the security objectives in all the tables where security objectives are
 mentioned, or keep the same name everywhere.

Response Response Status **C**

ACCEPT.

Cl **PP-A** SC P 152 L # 5 [REDACTED]
 aubry, carmen oce

Comment Type **E** Comment Status **A**

Table 10 Security objectives for the SMI TOE,

I think that O.FUNC(+OTHERTOE) .TRANSIT.NO_DIS is missing.
 Same for Table 110 SMI objectives rationale.

SuggestedRemedy

Include
 O.FUNC(+OTHERTOE) .TRANSIT.NO_DIS

Response Response Status **C**

ACCEPT IN PRINCIPLE.

We decided that D.FUNC.TRANSIT would only be protected from alteration, not from
 disclosure, so the proposed remedy would not be appropriate.

However, T.FUNC(+OTHERTOE).TRANSIT.DIS should be removed from Table 103
 because we don't have a DIS threat for FUNC data.

Cl **PP-A** SC P 156 L # 7 [REDACTED]
 aubry, carmen oce

Comment Type **E** Comment Status **A**

Table 112 SMI Information Flow Control SFP

D.DOC.TRANSIT should be D.DOC(+OTHERTOE).TRANSIT

D.FUNC.TRANSIT should be D.FUNC(+OTHERTOE).TRANSIT

SuggestedRemedy

Use D.DOC(+OTHERTOE).TRANSIT and D.FUNC(+OTHERTOE).TRANSIT.

Response Response Status **C**

ACCEPT.

Cl **PP-A** SC P 168 L # 9 [REDACTED]
 aubry, carmen oce

Comment Type **T** Comment Status **A**

Table 116 Completeness of SMI security requirements

I don't understand why both FTP_TRP.1 and FDP_IFC.1 are used for
 O.DOC(+OTHERTOE).TRANSIT, O.FUNC(+OTHERTOE).TRANSIT,
 O.PROT(+OTHERTOE).TRANSIT, O.CONF(+OTHERTOE)?

From what I have understood, FTP_TRP is used only to protect the SMI administration
 (O.CONF.TRANSIT and O.PROT.TRANSIT) and FDP_IFC.1 is used for
 O.DOC(+OTHERTOE).TRANSIT, O.FUNC(+OTHERTOE).TRANSIT,
 O.PROT(+OTHERTOE).TRANSIT, O.CONF(+OTHERTOE).TRANSIT.
 In any case, this was the approach taken in VPN PP.

SuggestedRemedy

Use FTP_TRP.1 for O.CONF.TRANSIT and O.PROT.TRANSIT.
 Use FDP_IFC.1 for O.DOC(+OTHERTOE).TRANSIT, O.FUNC(+OTHERTOE).TRANSIT,
 O.PROT(+OTHERTOE).TRANSIT, O.CONF(+OTHERTOE).TRANSIT.

Response Response Status **C**

ACCEPT.

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-A** SC **10.2.1** P **82** L **4** # **25**
 Sukert, Alan Xerox

Comment Type **E** Comment Status **A**

Table 54 does not include D.DOC.REST that is listed in Table 3 but not discussed as a User Data asset of the FAX TOE in Tables 52 and 53.

SuggestedRemedy

Include D.DOC.REST in Table 54.

Response Response Status **C**

ACCEPT IN PRINCIPLE.

Add an APP note to table 3 (and 54) that explains this.

Cl **PP-A** SC **10.3 table 59** P L # **18**
 Nevo, Ron Sharp

Comment Type **T** Comment Status **A**

O.DOC.OUTPUT.NO_DIS is for retrieval of received FAX. Who do you define is able to retrieve it? Administrator? All users? Or user who is granted for retrieving received FAX?

SuggestedRemedy

??

Response Response Status **C**

ACCEPT IN PRINCIPLE.

The specifics as to who can access what is defined by SFPs in the STs. We will add O.USER.AUTHORIZED and O.ADMIN.AUTHORIZED to the rationale tables for all access control threats for all PPs.

Cl **PP-A** SC **10.5.5** P **90** L **10** # **26**
 Sukert, Alan Xerox

Comment Type **E** Comment Status **A**

The PP application note for the FDP_ACC.1 SFR references objective O.FUNC.JOB.NO_ALT that is not described in subclause 10.3.1.

SuggestedRemedy

Resolve the inconsistency between subclauses 10 and 10.3.1 with respect to objective O.FUNC.JOB.NO_ALT.

Response Response Status **C**

ACCEPT.

Cl **PP-A** SC **11.2.1** P **104** L **1** # **27**
 Sukert, Alan Xerox

Comment Type **E** Comment Status **A**

Table 70 does not include D.DOC.REST that is listed in Table 3 but not discussed as a User Data asset of the DSR TOE in Tables 68 and 69.

SuggestedRemedy

Include D.DOC.REST in Table 70.

Response Response Status **C**

ACCEPT IN PRINCIPLE.

See comment #25.

Cl **PP-A** SC **11.2.1 table 68,71** P L # **19**
 Nevo, Ron Sharp

Comment Type **T** Comment Status **A**

From the threats T.DOC.RETRIEVE.DIS and T.DOC.RETRIEVE.ALT, we cannot read whether only owner is granted to retrieve or plural users (group) are granted to retrieve as HCD function, etc.

Description about the asset D.DOC.RETRIEVE, the threats T.DOC.RETRIEVE.DIS and T.DOC.RETRIEVE.ALT should be clarified.

This comes from whether FDP_ACC and FDP_ADF are necessary or not is not clear to realize O.DOC.RETRIEVE.NO_DIS and O.DOC.RETRIEVE.NO_ALT for countering T.DOC.RETRIEVE.DIS and T.DOC.RETRIEVE.ALT.

SuggestedRemedy

?

Response Response Status **C**

ACCEPT IN PRINCIPLE.

See comment #18

IEEE P2600 Hardcopy Device and System Security comments

CI **PP-A** SC 12.2.1 P 125 L 1 # 29
 Sukert, Alan Xerox

Comment Type **E** Comment Status **A**

Table 86 does not include the following assets that are listed in Table 3 but not discussed as a User Data asset of the NVS TOE in Tables 84 and 85: D.DOC.JOB, D.DOC.RETRIEVE, D.DOC.OUTPUT & D.FUNC.REST.

SuggestedRemedy

Add the missing assets to Table 86.

Response Response Status **C**

ACCEPT IN PRINCIPLE.

D.FUNC.REST -- should be added

Other: see comment #25

CI **PP-A** SC 12.2.1 P 125 L 1 # 28
 Sukert, Alan Xerox

Comment Type **E** Comment Status **A**

Table 86 lists the D.DOC.REST asset as being not applicable to the NVS TOE. However, D.DOC.REST is listed as an User Data asset for the NVS TOE in Table 84.

SuggestedRemedy

Resolve the inconsistency between tables 84 and 86.

Response Response Status **C**

ACCEPT IN PRINCIPLE.

One of them will be +OTHERTOE

CI **PP-A** SC 12.2.2 P 125 L 4 # 47
 Sukert, Alan Xerox

Comment Type **T** Comment Status **R**

The definition of T.DOC.REST.SAL and T.DOC.DELETED.SAL were modified so the threat now only covers salvaging on NVS that has been removed from the TOE. Although these are important threats, they don't cover the threat that an unauthorized person may attempt to access User Document Data stored in NVS while the NVS is still in the TOE. That threat and the associated security objective have to be addressed in the NVS TOE or it is incomplete in my view. Let's discuss this at the meeting next week.

SuggestedRemedy

Add a threat and associated security objective to the NVS TOE addressing unauthorized persons attempting to access User Document Data stored in NVS while the NVS is still in the TOE.

Response Response Status **C**

REJECT.

The NVS TOE does not provide any access to D.DOC. There is no user defined in NVS except for an Administrator. Those threats are handled by other TOEs, as indicated in table 86. Abnormal access to data in the OTE should be covered by AVA.

CI **PP-A** SC 12.5.4.3 P 132 L 28 # 48
 Sukert, Alan Xerox

Comment Type **T** Comment Status **A**

The FCS_COP.1.1 SFR requirement states that encryption should be performed on the asset D.DOC.JOB. However, D.DOC.JOB is not listed as one of the User Data assets for the NVS TOE in Tables 84 & 85.

SuggestedRemedy

Resolve whether D.DOC.JOB is or isn't an asset for the NVS TOE and update the PP accordingly.

Response Response Status **C**

ACCEPT.

D.DOC.JOB should not have been specified in FCS_COP because it is a subclass of D.DOC.REST. It should be removed.

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-A** SC **12.5.4.3** P **132** L **32** # **30**
 Sukert, Alan Xerox

Comment Type **E** Comment Status **A**

The PP application note for the FCS_COP.1 SFR references objective O.DOC.JOB.NO_SAL that is not described in subclause 10.3.1.

SuggestedRemedy

Resolve whether O.DOC.JOB.NO_SAL is a security objective for the NVS TOE and update the PP accordingly.

Response Response Status **C**

ACCEPT.

See response to #48, O.DOC.JOB should be removed from the app note.

Cl **PP-A** SC **12.6** P **140** L **1** # **49**
 Sukert, Alan Xerox

Comment Type **T** Comment Status **A**

Table 98 indicates that SFR FMT_MSA.1 supports fulfillment of objectives O.PROT.REST.NO_ALT, O.CONF.REST.NO_DIS & O.CONF.REST.NO_ALT. However, this SFR is not discussed in Table 99 for either of the three objectives.

SuggestedRemedy

Resolve the inconsistency between Tables 98 & 99 with respect to whether FMT_MSA.1 supports fulfillment of objectives O.PROT.REST.NO_ALT, O.CONF.REST.NO_DIS & O.CONF.REST.NO_ALT.

Response Response Status **C**

ACCEPT IN PRINCIPLE.

I need to go through the FMT_MSAs in several PPs (and all environments). In this case, in 12.5.7, FMT_MSA.1 is said to be a dependency of MSA.3 (which is not present in the TOE) and performs management recommendations for FDP_ACF.1. If that is all true, then FMT_MSA.1 should remain in 12.5.7 but should not be listed in tables 98 and 99.

Cl **PP-A** SC **12.6 table 98,99** P L # **20**
 Nevo, Ron Sharp

Comment Type **T** Comment Status **A**

It is not clear why FIA_UID.1, FMT_MSA.1 and FMT_SMR.1 are necessary to realize O.DOC.REST.NO_SAL. They are not necessary.

SuggestedRemedy

Eliminate FIA_UID.1, FMT_MSA.1 and FMT_SMR.1.

Response Response Status **C**

ACCEPT IN PRINCIPLE.

This will be fixed as part of change to CC v3.1 release 2 "upgrade" of the documents where the dependency of these SFR's goes away.

If we don't go to release 2 then the following answer applies:

Please look at the SFR dependency tables. FCS_COP depends on CKM.4. CKM.4 depends on FMT_MSA.2. MSA.2 depends on MSA.1 and SMR.1 (and also FDP_ACC.1, which we do not fulfill, see app note under 12.5.5), and SMR.1 depends on FIA_UID.1.

Cl **PP-A** SC **13.1.1** P **143** L **19** # **50**
 Sukert, Alan Xerox

Comment Type **T** Comment Status **A**

The SMI TOE Model shown in Figure 18 doesn't correspond to the assets discussed in subclause 13.2. For example, Figure 18 only shows TSF Data that is not from another TOE that is at rest; however there are threats (e.g., T.CONF.TRANSIT.ALT) and objectives (e.g., O.CONF.TRANSIT.NO_ALT) that clearly apply to TSF data that is in transit.

SuggestedRemedy

Revise the SMI TOE Model in Figure 18 to be consist with the data assets discussed in subclause 13.2.

Response Response Status **C**

ACCEPT.

I will add TRANSIT state to TSF Data assets in that diagram.

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-A** SC **13.2.1** P **144** L **27** # **51**
 Sukert, Alan Xerox

Comment Type **T** Comment Status **R**

It is not clear why assets D.DOC.TRANSIT and D.FUNC.TRANSIT aren't listed as User Data assets of the SMIU TOE in Table 100. It is true that User Document and Function Data being transmitted over a SMI from an external TOE (such as an Internet FAX) has to be protected from alteration and disclosure, But the same should hold true for User Document and Function Data that is transmitted from the TOE to an external TOE; a good example would be a scan job that is transmitted to an external server or file. This comment ripples throughout the SMI TOE discussion.

SuggestedRemedy

Resolve whether assets D.DOC.TRANSIT and D.FUNC.TRANSIT along with their associated threats and security objectives should be included in the SMI TOE.

Response Response Status **C**

REJECT.

It is a matter of definition. From the SMI TOE's point of view, the TOE does not have D.DOC or D.FUNC assets. The SMI doesn't know what the data is, because its importance (as DOC or FUNC or PROT or CONF) is determined by the "OTHERTOE".

Cl **PP-A** SC **13.2.1** P **145** L **1** # **52**
 Sukert, Alan Xerox

Comment Type **T** Comment Status **A**

I was wondering why the various data assets indicated with a æ(+OTHERTOE)Æ are not included in Table 3 at the beginning of P2600.1 because the SMI TOE treats all of these assets as separate assets from the other assets listed in Table 3.

SuggestedRemedy

Include the various data assets indicated with a "(+OTHERTOE)" in Table 3.

Response Response Status **C**

ACCEPT IN PRINCIPLE.

I thought about putting +OTHERTOE assets in Table 3, and I will put in an app note to this effect. But from the general model doesn't really distinguish one TOE from another TOE so it didn't seem appropriate to distinguish TOE assets from OTHERTOE assets in the general model.

Cl **PP-A** SC **13.2.1** P **145** L **4** # **31**
 Sukert, Alan Xerox

Comment Type **E** Comment Status **A**

Table 102 does not include D.DOC.JOB that is listed in Table 3 but not discussed as a User Data asset of the SMI TOE in Tables 100 and 101.

SuggestedRemedy

Include D.DOC.JOB in Table 102.

Response Response Status **C**

ACCEPT IN PRINCIPLE.

There is something wrong with table 102 because it lists D.DOC.REST and its subclasses RETRIEVE and OUTPUT (but not JOB). So either I should only list REST, or I should remove REST and list OUTPUT. This should be done consistently throughout the FoPP -- either list the superclass (if all subclasses are included) or list the individual subclasses.

Cl **PP-A** SC **13.2.3, 13.6 table 105,1** P L # **21**
 Nevo, Ron Sharp

Comment Type **T** Comment Status **A**

The meaning of P.SMI.MEDIATION is not clear. Explanation is not sufficient for us to understand clearly. Following the policy "access to internal network" can be realized. In addition, explanation that FDP_IFC.1 and FDP_IFF_1, etc. are necessary to realize O.SMI.MEDIATED is not sufficient.

SuggestedRemedy

Explanation

Response Response Status **C**

ACCEPT IN PRINCIPLE.

I think that this OSP (and perhaps others) would benefit from some brief explanation of what the policy is intended to accomplish. In this case, it would be to mediate connections to/from SMIs to protect the network from attacks that use the TOE (I will make better wording). I will look at other OSPs in a similar light. The objectives derived from OSPs should then be more descriptive of how they fulfill the policy and its purpose. Then, SFRs like FDP_IFC should make more sense.

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-A** SC 13.3.4 P 149 L 8 # 32
 Sukert, Alan Xerox

Comment Type **E** Comment Status **A**

The threat T.FUNC(+OTHERTOE).TRANSIT.ALT is not included in Table 110.

SuggestedRemedy

Include the threat T.FUNC(+OTHERTOE).TRANSIT.ALT in Table 110.

Response Response Status **C**

ACCEPT.

(+OTHERTOE) should have been listed in the objective names (for those threats involving other TOEs).

Cl **PP-A** SC 13.3.4 P 149 L 8 # 33
 Sukert, Alan Xerox

Comment Type **E** Comment Status **A**

The following objectives listed in Table 107 are not included in Table 110:
 O.FUNC(+OTHERTOE).TRANSIT.NO_ALT, O.PROT(+OTHERTOE).TRANSIT.NO_ALT,
 O.CONF(+OTHERTOE).TRANSIT.NO_DIS, & O.CONF(+OTHERTOE).TRANSIT.NO_ALT.

SuggestedRemedy

Resolve the inconsistency between Table 107 and Table 110 with respect to objectives
 O.FUNC(+OTHERTOE).TRANSIT.NO_ALT, O.PROT(+OTHERTOE).TRANSIT.NO_ALT,
 O.CONF(+OTHERTOE).TRANSIT.NO_DIS, & O.CONF(+OTHERTOE).TRANSIT.NO_ALT.

Response Response Status **C**

ACCEPT.

See comment #32

Cl **PP-A** SC 13.3.4 P 149 L 8 # 34
 Sukert, Alan Xerox

Comment Type **E** Comment Status **A**

The following objectives listed in Table 110 are not included in Table 107:
 O.DOC.TRANSIT.NO_DIS, O.DOC.TRANSIT.NO_ALT, O.FUNC.TRANSIT.NO_ALT, &
 O.CONF(+OTHERTOE).TRANSIT.NO_ALT.

SuggestedRemedy

Resolve the inconsistency between Table 107 and Table 110 with respect to objectives
 O.DOC.TRANSIT.NO_DIS, O.DOC.TRANSIT.NO_ALT, O.FUNC.TRANSIT.NO_ALT, &
 O.CONF(+OTHERTOE).TRANSIT.NO_ALT.

Response Response Status **C**

ACCEPT.

See comment #32

Cl **PP-A** SC 13.5.1.2 P 151 L 4 # 53
 Sukert, Alan Xerox

Comment Type **T** Comment Status **A**

The entity U.OTHERSUBJECT discussed in Table 112 is not described anywhere in Table
 1 and the beginning of P2600.1.

SuggestedRemedy

Include entity U.OTHERSUBJECT in Table 1.

Response Response Status **C**

ACCEPT IN PRINCIPLE.

U.OTHERSUBJECT is a remnant and should be replaced by "the subject of another TOE"
 (or something like that, it appears elsewhere in the FoPP that way).

Cl **PP-A** SC 13.6 P 163 L 8 # 35
 Sukert, Alan Xerox

Comment Type **E** Comment Status **A**

Table 116 indicates that SFRs FIA_UID.1, FMT_MSA.1, FMT_MSA.3 and FMT_SMF.1
 support fulfillment of objectives O.CONF.REST.NO_DIS & O.CONF.REST.NO_ALT.
 However, these SFRs are not discussed in Table 117 for either of these two objectives.

SuggestedRemedy

Resolve the inconsistency between Tables 116 and 117 with respect to the SFRs that
 support objectives O.CONF.REST.NO_DIS & O.CONF.REST.NO_ALT.

Response Response Status **C**

ACCEPT.

Could be affected by CC V3.1 release 2

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-A** SC **13.6** P **163** L **8** # **36**
 Sukert, Alan Xerox

Comment Type **E** Comment Status **A**

Table 117 indicates that SFRs FIA_AFL.1 and FIA_SOS.1 support fulfillment of objective O.ADMIN.AUTHORIZED. However, these SFRs are not listed as supporting this objective in Table 116.

SuggestedRemedy

Resolve the inconsistency between Tables 116 and 117 with respect to the SFRs that support objective O.ADMIN.AUTHORIZED.

Response Response Status **C**

ACCEPT.

Cl **PP-A** SC **5.5.3** P **10** L **1** # **37**
 Sukert, Alan Xerox

Comment Type **T** Comment Status **A**

The definitions of User Document Data and User Function Data included in PP-A do not match the definitions for these two terms included in Clause 2, subclauses 2.1.78 & 2.1.79, respectively, of the P2600 main body.

Note that the same comment applies to the definitions of User Document Data and User Function Data in Annex A Glossary, page 169.

SuggestedRemedy

Make sure the definitions of User Document Data and User Function Data included in PP-A match the corresponding definitions in P2600 main body, Clause 2.

Response Response Status **C**

ACCEPT IN PRINCIPLE.

I think that the PP definition should be changed to match the P2600 definition, but the P2600 definition could also use a little tweak. "image data" should be expanded to include any form of temporary data while processing a job. "residually-stored data" should refer to data left over *after* processing.

Any changes to the P2600 definition will have to be submitted during sponsor ballot.

Cl **PP-A** SC **5.5.3** P **10** L **8** # **39**
 Sukert, Alan Xerox

Comment Type **T** Comment Status **A**

The definitions of TSF Protected Data and TSF Confidential Data both reference an entity called the ""owner"" of the indicated data. This entity isn't defined anywhere in Clause 5.5 so it's not clear whether the owner is a User or some other distinct entity.

SuggestedRemedy

Define in Subclause 5.5 what an ""owner"" is.

Response Response Status **C**

ACCEPT IN PRINCIPLE.

TOE Owner should be defined, but I am not sure exactly where. The owner is not a user or even an entity in the normal sense.

Add as a Special Term (aka definition) and it might also be appropriate in an early overview section (5.2?) talk briefly about this.

Cl **PP-A** SC **5.5.3** P **11** L **1** # **40**
 Sukert, Alan Xerox

Comment Type **T** Comment Status **A**

In Table 3 I noted that the definitions for D.DOC.TRANSIT and D.FUNC.TRANSIT have a very slight but important difference taking into account the different type of data being described in each case. D.DOC.TRANSIT is User Document Data in transit to or from the TOE ""over a shared communications media"" while D.FUNC.TRANSIT is Job instructions or job status in transit to or from the TOE ""over an Interface to a shared communications medium"". It's not clear to me User Function data would be transmitted over an interface to a shared communications media but User Document Data wouldn't be transmitted over an interface to a shared communications media. Shouldn't they both be the same in that respect?

SuggestedRemedy

Make the definitions of D.DOC.TRANSIT and D.FUNC.TRANSIT consistent in terms of what the data is transmitted over.

Response Response Status **C**

ACCEPT.

The second definition is preferred (because the interface is within the TOE, but the medium is not). Will make them consistent.

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-A** SC 7.1.1 P 15 L 26 # 22
 Sukert, Alan Xerox

Comment Type **E** Comment Status **A**

The sentence on this line doesn't read correctly; it appears to be missing an adjective between 'updated' and 'the performance'.

SuggestedRemedy

Revise the sentence to read something like ""Additional TSF Data (e.g., audit logs) may be created or updated during the performance...""

Response Response Status **C**

ACCEPT.

Cl **PP-A** SC 7.2.1 P 18 L 1 # 23
 Sukert, Alan Xerox

Comment Type **E** Comment Status **A**

Table 6 does not include D.DOC.REST that is listed in Table 3 but not discussed as a User Data asset of the PRT TOE in Tables 4 and 5.

SuggestedRemedy

Include D.DOC.REST in Table 6.

Response Response Status **C**

ACCEPT IN PRINCIPLE.

See comment #25

Cl **PP-A** SC 7.2.3 P 19 L 1 # 43
 Sukert, Alan Xerox

Comment Type **T** Comment Status **A**

Table 13 on page 21 maps the P.AUDIT.LOGGING OSP to both O.AUDIT.LOGGED and OE.AUDIT.REVIEWED. I believe the mapping is correct, but the definition of the P.AUDIT.LOGGING OSP only talks about maintaining and protecting the audit log which would map only to the O.AUDIT.LOGGED security objective; there is no mention of any required review of the audit log in the P.AUDIT.LOGGING OSP that would be needed for this OSP to map to the OE.AUDIT.REVIEWED security objective. Note that a similar comment applies to the SCN TOE (subclause 8.2.3, page 40, line 11), CPY TOE (subclause 9.2.3, page 61, line 10), FAX TOE (subclause 10.2.3, page 83, line 6), DSR TOE (subclause 11.2.3, page 105, line 1), NVS TOE (subclause 12.2.3, page 125, line 11), and SMI TOE (subclause 13.2.3, page 147, line 6).

SuggestedRemedy

Modify the definition of the P.AUDIT.LOGGING OSP to something like ""Records that provide an audit trail of TOE use and security-relevant events will be maintained, protected from unauthorized disclosure or alteration, and reviewed at appropriate intervals by authorized persons.""

Response Response Status **C**

ACCEPT.

Cl **PP-A** SC 7.2.3 P 19 L 1 # 41
 Sukert, Alan Xerox

Comment Type **T** Comment Status **A**

The definitions of the OSPs P.USER.AUTHORIZATION and P.ADMIN.AUTHORIZATION for the PRT, SCN, CPY, FAX, DSR, NVS and SMI TOEs seem somewhat circular in that you are defining an organizational security policy as authorizing users or administrators according to ""security policies"" (i.e., you are defining a security policy by saying it is a security policy). It is not clear to me what security policies you are referring to in the definitions themselves, and I suspect it wouldn't be clear to an ST author what you mean here also. You need to be more specific as to what policies will govern user and admin authorization and do it in a way that doesn't amount to a circular definition.

SuggestedRemedy

Redefine OSPs P.USER.AUTHORIZATION and P.ADMIN.AUTHORIZATION in the various PPs to be closer to their definitions in Version 29b (e.g., P.USER.AUTHORIZATION - Users shall be authorized prior to being granted permission to use the TOE).

Response Response Status **C**

ACCEPT IN PRINCIPLE.

See comment #21

IEEE P2600 Hardcopy Device and System Security comments

CI **PP-A** SC **7.3.1** P **19** L **10** # **42**
 Sukert, Alan Xerox

Comment Type **T** Comment Status **A**

The definition for O.DOC.OUTPUT.NO_DIS in Table 11 doesn't seem correct as stated. If I am interpreting it correctly, the objective as stated is to prevent User Document Data from being sent to an unauthorized persons; the threat (T.DOC.OUTPUT.DIS) however is that User Document Data will not be disclosed to unauthorized persons in the output handler which is different that User Document Data being sent to an unauthorized person. To match the associated threat, the objective here should be that the TOE ""protect User Document Data being sent to the hardcopy output handler from being disclosed to unauthorized persons."" Note that the same comment applies to the FAX TOE (subclause 10.3.1, page 83, line 15).

SuggestedRemedy

Revise the definition of O.DOC.OUTPUT.NO_DIS to read ""The TOE shall protect User Document Data being sent to the hardcopy output handler from being disclosed to unauthorized persons.""

Response Response Status **C**
 ACCEPT.

CI **PP-A** SC **7.5.2 Class security au** P **23** L **16** # **54**
 Shigeru, Ueda Canon

Comment Type **G** Comment Status **R**

Current Audit data requirements in Table 15 contains requirements not required in the CC. For example, Job initiation and Job completion is not described in the CC. I believe Audit data requirements in this PP should be as minimum as possible because it is referenced to many kind of ST of MFD. And I believe Current Audit data requirements requires too much cost to implementers.

SuggestedRemedy

Delete Audit data requirements in Table 15 not required in CC. It should be also applied to other tables in other individual PP in this PP. (P2600.1-SCN,P2600.1-CPY...)

Response Response Status **C**
 REJECT.

We decided on these audit requirements at a previous meeting, and most of them fall below the "minimal" class as defined by the CC because we determined that they do not apply to HCDs. However, "job initiation" is a recommended audit item -- see resolution of action item #418.

Something for discussion: should we include, perhaps as an annex, a rationale for not including "minimal" audit requirements for items that we do not include? -- Not at this time.

CI **PP-A** SC **7.6** P **34** L **1** # **44**
 Sukert, Alan Xerox

Comment Type **T** Comment Status **A**

Table 19 on page 35 indicates that SFRs FIA_UID.1 and FMT_SMR.1 support sufficiency of objectives O.CONF.REST.NO_DIS. O.PROT.REST.NO_ALT & O.CONF.REST.NO_ALT. However, this is not indicated in Table 18 (no 'S' in the applicable rows for FIA_UID.1 and FMT_SMR.1 for these objectives).

SuggestedRemedy

Resolve the inconsistency between Tables 18 and 19 as to whether FIA_UID.1 and FMT_SMR.1 support O.CONF.REST.NO_DIS. O.PROT.REST.NO_ALT & O.CONF.REST.NO_ALT.

Response Response Status **C**
 ACCEPT.

Table 18 is likely incorrect.

CI **PP-A** SC **7.6 table 18,19** P L # **15**
 Nevo, Ron Sharp

Comment Type **T** Comment Status **A**

Only FMT_MTD and FMT_SMF are not sufficient to realize O.PROT.REST.NO_ALT, O.CONF.REST.NO_DIS and O.CONF.REST.NO_ALT. Since FMT_MTD is a specification to manage TSF Protected data and TSF Confidential data, it cannot identify who (administrator or user) can operate the management.

SuggestedRemedy

We need to specify who can update or refer to TSF Protected data and TSF Confidential data, and make only them (their group) can update or refer to them. Normally, identification and authorization of user or administrator is necessary to update or refer to TSF Protected data and TSF Confidential data.

Response Response Status **C**
 ACCEPT IN PRINCIPLE.

Related to comment #44 and comment #18

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-A** SC **7.6 table 18,19** P L # **14**
 Nevo, Ron Sharp

Comment Type **T** Comment Status **A**

To realize O.DOC.OUTPUT.NO_DIS and O.FUNC.REST.NO_ALT, FIA_UID alone is not sufficient. Therefore FIA_UAU should be added.

SuggestedRemedy

Add FIA_UAU to realize O.DOC.OUTPUT.NO_DIS and O.FUNC.REST.NO_ALT.

Response Response Status **C**

ACCEPT IN PRINCIPLE.

The remedy is rejected but the intent will get fulfilled by comment #18

Cl **PP-A** SC **7.6 table 18,19** P L # **16**
 Nevo, Ron Sharp

Comment Type **T** Comment Status **A**

By P.ADMIN.AUTHORIZATION, the user is granted to use TOE management function after he is identified and authenticated as administrator. (We read that the user have to be identified and authenticated as administrator in order to use TOE management function.)

By P.USER.AUTHORIZATION, the user is granted to use TOE function after he is identified and authenticated as TOE user. (We read that the user have to be identified and authenticated as TOE user in order to use TOE.)

In order to operate O.ADMIN.AUTHORIZED and O.USER.AUTHORIZED for countering them, Subject-User Binding FIA_USB.1 is not necessary.

SuggestedRemedy

Eliminate FIA_USB.1.

Response Response Status **C**

ACCEPT.

Cl **PP-A** SC **7.6 table 18,19** P L # **17**
 Nevo, Ron Sharp

Comment Type **T** Comment Status **R**

FIA_UID.1 is not necessary to realize O.AUDIT.LOGGED.

Regarding FMT_SMF.1, contents that are required in "Management" described in every functional requirement in Part 2 are lacking.

For example, regarding Table 18, FMT_SMF.1 for O.USER.AUTHORIZED, O.ADMIN.AUTHORIZED, O.SOFTWARE.VERIFIED and O.AUDIT.LOGGED should be supported.

SuggestedRemedy

Modify as left column.

Response Response Status **C**

REJECT.

This comment was WITHDRAWN by the commenter.

Cl **PP-A** SC **7.6 table 19,18** P L # **13**
 Nevo, Ron Sharp

Comment Type **T** Comment Status **A**

It is not clear why FDP_ACC.1 and FDP_ACF.1 are necessary so as to realize O.DOC.OUTPUT.NO_DIS. We think they are not necessary.

FDP_ACC.1 and FDP_ACF.1 are the necessary security functions in the case, for example, regarding user A and B, A can use update function and B can only use read function.

Regarding O.DOC.OUTPUT.NO_DIS, output is granted only for the user that uses secure print. However, it can be realized by identification and authentication functions (FIA_UID and FIA_UAU). Therefore FDP_ACC.1 and FDP_ACF.1 are not necessary.

SuggestedRemedy

Eliminate FDP_ACC.1 and FDP_ACF.1.

Along with them, FMT_MSA is not necessary. So it should be deleted.

Response Response Status **C**

ACCEPT IN PRINCIPLE.

Solved by changes made as a part of #18.

IEEE P2600 Hardcopy Device and System Security comments

CI **PP-A** SC **8.2.1** P **39** L **27** # **45**
 Sukert, Alan Xerox

Comment Type **T** Comment Status **A**

Table 22 does not include D.DOC.REST and D.DOC.OUTPUT that are listed in Table 3 but are not discussed as a User Data asset of the SCN TOE in Tables 20 and 21.

SuggestedRemedy

Include D.DOC.REST and D.DOC.OUTPUT in Table 22.

Response Response Status **C**

ACCEPT IN PRINCIPLE.

D.DOC.REST is a superclass of OUTPUT, RETRIEVE, and JOB. None are considered in SCN, so either REST should be the only one in table 22, or OUTPUT should be added to table 22. See also #31.

CI **PP-A** SC **8.5.5** P **47** L **21** # **46**
 Sukert, Alan Xerox

Comment Type **T** Comment Status **A**

The PP application note for the FDP_ACC.1 SFR references objectives O.DOC.OUTPUT.NO_DIS & O.FUNC.JOB.NO_ALT that are not described in subclause 8.3.1. Same comment applies to the CPY TOE (subclause 9.5.5, page 68, line 21) and the DSR TOE (subclause 11.5.5, page 112, line 9).

SuggestedRemedy

Resolve the inconsistency between subclauses 8.5.5 and 8.3.1 with respect to objectives O.DOC.OUTPUT.NO_DIS & O.FUNC.JOB.NO_ALT.

Response Response Status **C**

ACCEPT.

the PP app note should be changed

CI **PP-A** SC **9.2.1** P **60** L **26** # **24**
 Sukert, Alan Xerox

Comment Type **E** Comment Status **R**

Table 38 does not include D.DOC.REST that is listed in Table 3 but not discussed as a User Data asset of the CPY TOE in Tables 36 and 37.

SuggestedRemedy

Include D.DOC.REST in Table 38.

Response Response Status **C**

REJECT.

See also #31

CI **PP-A** SC **Annex A** P **168** L **1** # **38**
 Sukert, Alan Xerox

Comment Type **T** Comment Status **A**

Annex A Glossary doesn't include definition of the terms TSF data, TSF protected data and TSF Confidential Data that are defined in subclause 5.5.3, page 10.

SuggestedRemedy

Include the definitions of TSF data, TSF protected data and TSF Confidential Data in Annex A.

Response Response Status **C**

ACCEPT.

Annex A needs a complete overhaul. Do I smell a volunteer? - Alan picked this up as an action item.