

IEEE P2600 Hardcopy Device and System Security comments

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

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

[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 **O**

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

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

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

Proposed Response Response Status **O**

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

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

Table 47 üCPY Audit data requirements Unsuccessful attempt to use trusted path
 There is no trusted path requirement for the copy TOE!

SuggestedRemedy

Remove this item.

Proposed Response Response Status **O**

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

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

Table 102 üAssets 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(+OTHER)TOE).TRANSIT). In any case, with the current names (D.DOC.REST, ..) it might be unclear.

SuggestedRemedy

Remove the table.

Proposed Response Response Status **O**

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

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

Table 70 üAssets 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, there are no "User Document Data in the TOE awaiting or processing a job."

Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security comments

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

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

ôThe 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 personsö.

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

SuggestedRemedy

Remove deleted part and say:
 ôThe 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 personsö

Proposed Response Response Status **O**

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

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

Major security features of NVS:
 ôUser Document Data are protected from offline salvage by unauthorized personsö
 I think that NVS is somehow similar with SMI when it comes to protecting other TOEs 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:
 ôThe NVS TOE can protect User Data of the Subject of another TOE from offline salvage by unauthorized personsö
 This would generate only asset name changes (Table 84 üUser Data assets of NVS TOE, Table 87 üThreats to User Data for the NVS TOE, Table 91 üNVN Security objectives, Table 93 üNVN objectives rationale), the SRRs are the same.

Proposed Response Response Status **O**

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

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

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

SuggestedRemedy

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

Proposed Response Response Status **O**

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

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

Table 107 ü Security objectives for the SMI TOE,
 I think that O.FUNC(+OTHERTOE).TRANSIT.NO_DIS is missing. Same for Table 110 üSMI objectives rationale.

SuggestedRemedy

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

Proposed Response Response Status **O**

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

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

Table 112 ü 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.

Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security comments

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

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

Table 116 üCompleteness 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.

Proposed Response Response Status **O**

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

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

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.

Proposed Response Response Status **O**

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

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

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

??

Proposed Response Response Status **O**

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

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

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.

Proposed Response Response Status **O**

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

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

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.

Proposed Response Response Status **O**

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

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

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

?

Proposed Response Response Status **O**

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 **X**

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.COC.OUTPUT & D.FUNC.REST.

SuggestedRemedy

Add the missing assets to Table 86.

Proposed Response Response Status **O**

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

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

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.

Proposed Response Response Status **O**

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

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

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.

Proposed Response Response Status **O**

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

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

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.

Proposed Response Response Status **O**

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

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

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.

Proposed Response Response Status **O**

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

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

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.

Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP-A** SC **12.6 table 98,99** P L # **20**
 Nevo, Ron Sharp
 Comment Type **T** Comment Status **X**
 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.
 Proposed Response Response Status **O**

Cl **PP-A** SC **13.2.1** P **145** L **1** # **52**
 Sukert, Alan Xerox
 Comment Type **T** Comment Status **X**
 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 æ(+OTHERTOE)Æ in Table 3.
 Proposed Response Response Status **O**

Cl **PP-A** SC **13.1.1** P **143** L **19** # **50**
 Sukert, Alan Xerox
 Comment Type **T** Comment Status **X**
 The SMI TOE Model shown in Figure 18 doesnÆt 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.
 Proposed Response Response Status **O**

Cl **PP-A** SC **13.2.1** P **145** L **4** # **31**
 Sukert, Alan Xerox
 Comment Type **E** Comment Status **X**
 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.
 Proposed Response Response Status **O**

Cl **PP-A** SC **13.2.1** P **144** L **27** # **51**
 Sukert, Alan Xerox
 Comment Type **T** Comment Status **X**
 It is not clear why assets D.DOC.TRANSIT and D.FUNC.TRANSIT arenÆt 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.
 Proposed Response Response Status **O**

Cl **PP-A** SC **13.2.3, 13.6 table 105,1** P L # **21**
 Nevo, Ron Sharp
 Comment Type **T** Comment Status **X**
 The meaning of P.SMI.MEDIATION is not clear. Explanation is not sufficient for us to understand clearly. Following the policy ðaccess to internal networkö 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
 Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security comments

CI **PP-A** SC 13.3.4 P 149 L 8 # 32
 Sukert, Alan Xerox
 Comment Type **E** Comment Status **X**
 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.
 Proposed Response Response Status **O**

CI **PP-A** SC 13.5.1.2 P 151 L 4 # 53
 Sukert, Alan Xerox
 Comment Type **T** Comment Status **X**
 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.
 Proposed Response Response Status **O**

CI **PP-A** SC 13.3.4 P 149 L 8 # 33
 Sukert, Alan Xerox
 Comment Type **E** Comment Status **X**
 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.
 Proposed Response Response Status **O**

CI **PP-A** SC 13.6 P 163 L 8 # 35
 Sukert, Alan Xerox
 Comment Type **E** Comment Status **X**
 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.
 Proposed Response Response Status **O**

CI **PP-A** SC 13.3.4 P 149 L 8 # 34
 Sukert, Alan Xerox
 Comment Type **E** Comment Status **X**
 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.
 Proposed Response Response Status **O**

CI **PP-A** SC 13.6 P 163 L 8 # 36
 Sukert, Alan Xerox
 Comment Type **E** Comment Status **X**
 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.
 Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security comments

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

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

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.

Proposed Response Response Status **O**

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

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

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.

Proposed Response Response Status **O**

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

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

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.

Proposed Response Response Status **O**

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

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

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...""

Proposed Response Response Status **O**

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

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

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.

Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security comments

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

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

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."

Proposed Response Response Status **O**

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

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

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).

Proposed Response Response Status **O**

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

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

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."

Proposed Response Response Status **O**

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

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

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...)

Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security comments

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

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

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.

Proposed Response Response Status **O**

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

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

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.

Proposed Response Response Status **O**

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

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

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.

Proposed Response Response Status **O**

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

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

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.

Proposed Response Response Status **O**

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

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

FIA_UID.1 is not necessary to realize O.AUDIT.LOGGED. Regarding FMT_SMF.1, contents that are required in Managementö 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 Supportö.

SuggestedRemedy

Modify as left column.

Proposed Response Response Status **O**

IEEE P2600 Hardcopy Device and System Security comments

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

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

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.

Proposed Response Response Status **O**

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

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

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.

Proposed Response Response Status **O**

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

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

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.

Proposed Response Response Status **O**

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

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

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.

Proposed Response Response Status **O**

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

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

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.

Proposed Response Response Status **O**