

IEEE P2600 Hardcopy Device and System Security comments

Cl **All** SC P L # 3
 Wright, Don Lexmark

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

There are many places in the Guide where long blocks of text from Std 2600 have been duplicated. Since this Guide will not be an IEEE document, we need to respect the IEEE copyright and not copy this text into the document

SuggestedRemedy

Replace duplication of text from Std 2600 with references to the appropriate clauses within Std 2600

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **Guide** SC ??? P ??? L # 2
 Farrell, Lee Canon

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

Two interpretations can be possible with audit objective (O.AUDIT.LOGGED) and SFR (FAU_GEN) because these are not consistent with each other. O.AUDIT.LOGGED specifies maintaining a log and preventing its disclosure or alteration. SFR (FAU_GEN) specifies generation of a log. (i.e., SFR partially fulfills the objective.) Interpretation a): O.AUDIT.LOGGED has an error and the SFR is correct. Interpretation b): SFR (FAU_GEN) has an error and O.AUDIT.LOGGED is correct.

An explanation that addresses and clarifies this issue should be added to the Guide.

SuggestedRemedy

The following explanatory text should be added to the Guide document (somewhere): It is understood that the Working Group's intent is that an external log server can be used to maintain the log generated by the TOE, and in this case, the external server maintains the log and prevents its disclosure or alteration. Thus the TOE does not need to maintain and prevent the log's disclosure or alteration. (i.e., Interpretation a) -- no additional SFR is required.)

If an external server is not used (i.e., the TOE maintains the log by itself), an appropriate SFR (e.g., FAU_STG.1) needs to be added to ST.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

The final text will be close to but perhaps not identical to the suggested remedy.

Cl **Guide** SC ??? P ??? L # 1
 Farrell, Lee Canon

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

There is a Problem with Protection Profile A that should be noted and explained in the Guide somewhere ... wherever most appropriate.

The problem is that external authentication cannot be used because there exists an SFR for authentication.

O.USER.AUTHORIZED requires authentication. FIA_UAU addresses the authentication.

Above is fine if authentication *internal* to the TOE is used. However, if external authentication is used, there is no authentication in the TOE, and thus the TOE cannot fulfill O.USER.AUTHORIZED.

It is understood that the working group intended to accommodate *external* authentication as an acceptable method for addressing this security requirement. Ideally, both FIA_UAU.1 and .2 should be removed from the Protection Profile and the definition of O.USER.AUTHORIZED would be changed from:

""The TOE shall require identification and authentication of Users, and shall ensure that Users are authorized in accordance with security policies before allowing them to use the TOE.""

... to the following:

""The TOE shall require identification of Users, and shall ensure that Users are authorized in accordance with security policies before allowing them to use the TOE.""

However, because the Working Group is no longer accepting changes to the Protection Profile, explanatory text should be added to the Guide document to clarify the intent.

SuggestedRemedy

The following explanatory text should be added to the Guide document (somewhere):

"It is the Working Group's intent that an external authentication server can be used as an acceptable method of addressing the requirement for authentication. When an external authentication server is used, FIA_UAU.1 and .2 can be removed from the ST. If an external server is not used (i.e. the TOE authenticates), then FIA_UAU needs to be included in the ST."

Proposed Response Response Status **W**

PROPOSED REJECT.

We don't read FIA_UAU as requiring internal authentication and @tsec agrees with that interpretation.

App notes 35-37 and 40-42 already explain how identification and authentication work in conjunction with an external server.

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP Gu** SC 5.2.1.1 P 31 L 10 # 5
Sukert, Alan Xerox

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

The sentence on the indicated line has a typographical error that needs to be corrected.

SuggestedRemedy

Revise the line to read ""The assets the product must protect. Table x compares the assets that must be protected...""

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **PP Gu** SC 5.2.1.1 P 31 L 10 # 4
Sukert, Alan Xerox

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

For some reason the Table titles and numbers for the two tables in subclause 5.2.1.1 (Items #c and d) on page 31 were accidentally deleted. This caused the Table number references on lines 10 and 21 for these two tables to be removed also.

Note that this same comment applies to the tables and table number references in subclause 5.2.1.1, pages 32 (line 24), 33 (lines 9 and 34) and 34 (line 30)

SuggestedRemedy

Add the applicable Table titles and numbers for the tables on the indicated pages above and fix the associated table references on the indicated pages.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **PP Gu** SC 5.2.2.5.7.6 P 54 L 7 # 7
Sukert, Alan Xerox

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

It looks like all the table titles and numbers in the document somehow got corrupted in this version and need to be fixed.

SuggestedRemedy

Correct all of the table title and number references in the document.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **PP Gu** SC 5.2.2.5.7.6 P 54 L 7 # 6
Sukert, Alan Xerox

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

The two references in the Common Access Control table somehow got corrupted.

SuggestedRemedy

Fix the two references in the Common Access Control table.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **PP Gu** SC 5.2.2.7.1 P 63 L 19 # 8
Sukert, Alan Xerox

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

The two references in the table on page 63 somehow got corrupted.

SuggestedRemedy

Fix the two references in the table on page 63.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

IEEE P2600 Hardcopy Device and System Security comments

Cl **PP Gu** SC **5.2.2.7.7** P **79** L **1** # **10**
Chen, Nancy Oki Data

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

The first three paragraphs of this page provide guidance to ST authors what other SFRs should be used to implement FTP_CIP_EXP.1. In other words, it interpretes FTP_CIP_EXP.1 as an SFR that requires TOE to also meets other SFRs such as FPT_ITC, FPT_IIT, FDP_ITC, FDP_ETC, FTP_TRP, and others that may be recommended by ST evaluators. I would like to confirm whether this is the intention for this FTP_CIP_EXP.1. I thought the reason we defined FTP_CIP_EXP.1 is because if we don't have this ECD, we would have to use so many separate sets of SFRs for User Data and TSF Data as recommended here. To avoid the complexity and provide flexibility, we defined FTP_CIP_EXP.1 to encompasses these other SFRS. But ST authors only have to describe how the TOE's TSF code actually implement this ECD.

SuggestedRemedy

Please discuss and confirm the intention of FTP_CIP_EXP.1.1.

If ST author does not to use other SFRs recommended here to fulfill FTP_CIP_EXP.1.1, only need to describe TOE TSF's actually implementation, then Delete these three paragraphs, or use these three paragraphs as detailed rationales for why we needed to define FTP_CIP_EXP.1 for NVS package.

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

We will delete lines 1 through 22 on page 79.

Cl **PP Gu** SC **6.1** P **87** L **4** # **9**
Sukert, Alan Xerox

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

Typographical errors -- ""NEAP"" should be ""NIAP"" in subclause 6.1, page 87, line 4 and ""CLEVES"" should be ""CCEVS"" in subclause 6.1, page 87, line 4.

SuggestedRemedy

Change 'NEAP' to 'NIAP' in subclause 6.1, page 87, line 4 and 'CLEVES' to '-CCEVS' in subclause 6.1, page 87, line 5.

Proposed Response Response Status **W**

PROPOSED ACCEPT.