

IEEE P2600 Hardcopy Device and System Security comments

Cl Main SC 10.1.1.4 P 143 L 36 # 5  
Sukert, Alan Xerox

Comment Type G Comment Status D

The term 'Protected Data' is used here and elsewhere in the main clause. Since it may not be clear what this term means in the context of the P2600 standard (for example, the Google definition is ""Protected data can be accessed by the methods of the class in which it is defined as well as by the subclasses""), this term should be defined in Clause 3.

SuggestedRemedy

Include a definition for 'Protected Data' in Clause 3 - like Confidential data I don't have a good definition yet, but the Goggle definition isn't it.

Proposed Response Response Status W

PROPOSED ACCEPT IN PRINCIPLE.

Same response as comment 5.

Cl Main SC 10.1.1.4.1 P 144 L 3 # 11  
Sukert, Alan Xerox

Comment Type T Comment Status D

Given that the threats in Clause 7 have now been differentiating between those threats associated with data stored during performance of a job and data stored after performance of a job, I think the requirements in Clause 10 associated with storing data should also differentiate whether they apply to data stored on the HCD during performance of a job, after performance of a job, or both. In this case I think it's both but I certainly could be wrong.

SuggestedRemedy

Clarify in Clause 10 for any requirement dealing with storage of data on the HCD whether it applies during performance of a job, after performance of a job, or both.

Proposed Response Response Status W

PROPOSED ACCEPT IN PRINCIPLE.

This will have to be solved for the PPs first and can then be reflected back into the compliance clause of P2600.

Cl Main SC 10.1.1.7 P 145 L 3 # 9  
Sukert, Alan Xerox

Comment Type T Comment Status D

I think there needs to be some clarification here if what is meant by ""usage-related"" event - does this involve counting copies and prints, recording job starts and completions, etc. Important from a requirements per that it is clear to the manufacturer what specific events are to be monitored so there can be no question pr confusion as to what manufacturers are to comply with.

SuggestedRemedy

Clarify by examples if necessary what usage-related events are to be monitored.

Proposed Response Response Status W

PROPOSED ACCEPT IN PRINCIPLE.

This will have to be solved for the PPs first and can then be reflected back into the compliance clause of P2600.

Cl Main SC 10.1.1.9 P 145 L 14 # 10  
Sukert, Alan Xerox

Comment Type T Comment Status D

The requirement here is not correct as stated. The requirement should be that the HCD shall not permit users to establish a malicious connection to not only the external IT environment but also to the internal network. You do not want attackers being able to access anything internal to the HCD using the Fax and the PSTN as well as using the HCD as a bridge to access the external network and thus attack other nodes.

SuggestedRemedy

Restate the requirement as ""The HCD shall not permit users to establish a malicious connection to either the internal network or to the external IT environment from the HCDs fax interface"".

Proposed Response Response Status W

PROPOSED ACCEPT IN PRINCIPLE.

The HCD shall not permit users to establish a malicious connection to the external IT environment and should not permit an unauthorized non-fax data connection to the HCD via the fax interface.

IEEE P2600 Hardcopy Device and System Security comments

Cl Main SC 7.2 P 27 L 45 # 1  
Sukert, Alan Xerox

Comment Type E Comment Status D

The rows for T.HCD.AVAIL.COPY and T.HCD.AVAIL.PEER in Table 3 indicate that these threats are covered in Subclause 7.3.2.2; they are actually covered in Subclause 7.3.2.1. Note - this also has to be corrected in Table 53, Page 70.

SuggestedRemedy

Correct the Clause reference for T.HCD.AVAIL.COPY T.HCD.AVAIL.PEER and in Table 3.

Proposed Response Response Status W

PROPOSED ACCEPT.

Cl Main SC 7.2 P 42 L 27 # 6  
Sukert, Alan Xerox

Comment Type T Comment Status D

In the revised Clause 7, the following threat included in the latest draft for the Protection Profile for Operational Environment A (P2600.1/D28a) is not included in the updated Clause 7 -- T.FUNC.TRANSIT.DIS (Table 78 - SMI Threats)

SuggestedRemedy

Add discussion of T.FUNC.TRANSIT.DIS to Clause 7.

Proposed Response Response Status W

PROPOSED ACCEPT.

Cl Main SC 7.3.2.4 P 62 L 5 # 7  
Sukert, Alan Xerox

Comment Type T Comment Status D

The threat description in Table 39 for T.CONF.CAMERA.DIS does not match the corresponding threat description for this threat in Table 3, page 42.

SuggestedRemedy

Make the threat descriptions for T.CONF.CAMERA.DIS in Tables 3 and 39 match.

Proposed Response Response Status W

PROPOSED ACCEPT.

Cl Main SC 7.4.2 P 69 L 10 # 8  
Sukert, Alan Xerox

Comment Type T Comment Status D

The following threat shown in Table 3, page 42 is not included in Table 53 -- T.CONF.CAMERA.DIS

SuggestedRemedy

Include T.CONF.CAMERA.DIS in Table 53

Proposed Response Response Status W

PROPOSED ACCEPT.

Cl Main SC 8.3.12.2 P 94 L 27 # 3  
Sukert, Alan Xerox

Comment Type G Comment Status D

Document has been inconsistently using 'nonvolatile' and 'non-volatile'. In this instance, 'non-volatile' is used; two lines earlier 'nonvolatile' is used. Note that Clause 3.1.56, Page 8 defines terms as 'non-volatile'.

SuggestedRemedy

Be consistent in using 'nonvolatile' or 'non-volatile' throughout the document.

Proposed Response Response Status W

PROPOSED ACCEPT.

Use nonvolatile throughout.

Cl Main SC 8.3.13.2 P 95 L 34 # 4  
Sukert, Alan Xerox

Comment Type G Comment Status D

Clauses 7, 8 and 10 are now using the term ""confidential data"". Given that this term may have a clear meaning (for example, a Google search had this definition -- data that can be connected at some point, no matter how brief, to the person providing them) we should provide one for the context we are using this term in Clause 3.

SuggestedRemedy

Provide a definition of ""confidential data"" in Clause 3. I'll look for a good proposed definition, but what Google states isn't it.

Proposed Response Response Status W

PROPOSED ACCEPT IN PRINCIPLE.

Add a definition in clause in 3 that points to the appropriate place in clause 6.

IEEE P2600 Hardcopy Device and System Security comments

Cl Main SC 8.4.8.1 P 106 L 3 # 2  
Sukert, Alan Xerox

Comment Type E Comment Status D

The definition here appears to be the one for T.PROT.TRANSIT.ALT or not the required one for T.PROT.STORED.ALT. Similarly the definition in Subclause 8.4.9.1 appears to be the one for T.PROT.STORED.ALT and not the one required for T.PROT.TEANSIT.ALT

*SuggestedRemedy*

Include the proper threat definition for T.PROT.STORED.ALT in Subclause 8.4.8.1 and for T.PROT.TRANSIT.ALT in 8.4.9.1

Proposed Response Response Status W

PROPOSED ACCEPT.