

[US<sup>1</sup>] comments on ISO/IEC 3<sup>rd</sup> WD 15446 (revision)

Date: 2007-MM-DD	Document: <b>SC27 N5792</b>
------------------	-----------------------------

1	2	(3)	4	5	(6)	(7)
NB <sup>1</sup>	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment <sup>2</sup>	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
[US] 1	6.3.2.4	3	ed	The paragraph explains how an ST conforms to a PP but does not explain or reference the concept of strict and/or demonstrable conformance.	Mention that the two types of conformance exist here Note that these are explained in 6.5.6 of the document.	
[US] 2	6.5.3	4	ed	There is a typographical error in the sentence "You should briefly examine this list to see if you see anything odd <b>on</b> it that you would not expect,"...	There is a typographical error in the sentence "You should briefly examine this list to see if you see anything odd <b>in</b> it that you would not expect,"...	
[US] 3	6.5.3	5	ed	The reference to the TOE overview section of ISO/IEC 15408-1 2008 as A.4.3 is incorrect.	The section is numbered A.4.2.	
[US] 4	6.5.5	3 bulleted text	ed	The construct of the bullets might lead the reader to suppose that the guidance text e.g. "This represents the version of ISO/IEC 15408 that is used" is part of the form that will be seen n the PP or ST. Which is not the case.	Use some means to clarify. Perhaps a new line after 'ISO/IEC 15408:2008' So that the guidance text is clearly separated.	
[US] 5	6.5.7	2	Te	The use of the word "better" is misleading the reader into a poor understanding of assurance. Increased assurance will not make the card "better" (i.e. stronger or more robust) it increases the confidence that the claims are true, but it does not change the claims. Similarly in the first example assurance is not related to a "low quality" smart card.  It is possible to evaluate a TOE against an ST that has specifications that are not related to the use of the TOE to a high assurance level. One ends up with high assurance that the TOE does the wrong thing!	"In the first case if a hacker manages to brek the bus ticket, he may be able to get free bus rides until the card parameters change, which in this example represents a relatively small financial loss to the operator, who can therefore afford to be less sure that the security functionality is implemented correctly. In the second, and certainly the third case, you want to be very sure that the smart card is meeting the security claims made, as the consequences of breaking these cards may be much more expensive."	
[US] 6	9.2.3	1	Te	The enumeration of a risk is made with a specific audience in mind. Typically the organization making the risk assessment. What is determined to be an insignificant consequence of loss to one audience may	The results of a security risk assessment should be assessed with cogniscence of this issue. A brief explanation or warning should be added	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by \*\*)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

**NOTE** Columns 1, 2, 4, 5 are compulsory.

[US<sup>1</sup>] comments on ISO/IEC 3<sup>rd</sup> WD 15446 (revision)

Date: 2007-MM-DD	Document: <b>SC27 N5792</b>
------------------	-----------------------------

1	2	(3)	4	5	(6)	(7)
NB <sup>1</sup>	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment <sup>2</sup>	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
				not be determined identically by another audience.	to this guidance text. For example add after "... the consequence of a loss are not significant."  "However, risk assessments determine the risk with a particular audience in mind. The reader of a risk assessment prepared by a third party should consider the assessment of acceptable risk with reference to their own needs"	
[US] 7	9.3.3.1	1	ed	The meaning of the sentence would be clearer if the use of the word "asset" were highlighted as an object,	Suggest modifying the sentence to.. " – The interpretation that the term "asset" is understood to include" ...	
[US] 8	9.3.3.2	1	ed	The use of the word "merely" implies that the definition in ISO/IEC 15408 is not sufficient.	Remove the word "merely"	
[US] 9	9.3.3.2	8	ed	The terms "acts of god" has incorrect capitalisation	Change to "acts of God"	
[US] 10	11	7 (not including editors note)	ed	The sentence "This makes it easier for other ST or PP writer to pick up the extended component and instantiate it in a way that fits their requirements." Does not agree.	Change to  This makes it easier for other ST or PP writers to pick up the extended component and instantiate it in a way that fits their requirements."  Or  This makes it easier for another ST or PP writer to pick up the extended component and instantiate it in a way that fits their requirements."	
[US] 11	15.2	1	te	There are no national schemes that use ISO/IEC 15408. In truth interpretations are in the domain of the CCMB	Explain the relationship between CC and ISO/IEC 15408	
[US] 12	15		ed	There are several references to "ISO 15408"	Change to "ISO/IEC 15408"	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by \*\*)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

**NOTE** Columns 1, 2, 4, 5 are compulsory.

[US<sup>1</sup>] comments on ISO/IEC 3<sup>rd</sup> WD 15446 (revision)

Date: 2007-MM-DD	Document: <b>SC27 N5792</b>
------------------	-----------------------------

1	2	(3)	4	5	(6)	(7)
NB <sup>1</sup>	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment <sup>2</sup>	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
[US] 13	16	1	ed	The word “extend” is used instead of “extent” in the sentence “The structured nature of ISO/IEC 15408, and the ruled content of an PP/ST, have raised the question of to what extent the usage of automated tools to develop PPs/STs can help in the production and evaluation of such key documents in an ISO/IEC 15408 evaluation.”	Change “extend” to “extent”	
[US] 14	16	final	ed	This paragraph seems to be constructional	Remove the paragraph.	
[US] 15	New Annex		ge	We suggest the addition of a glossary of acronyms used in CC for reference as an aid to the audience. This could be an informative annex.	See contribution attached.	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by \*\*)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

**NOTE** Columns 1, 2, 4, 5 are compulsory.