



ISO/IEC JTC 1/SC 27 **N 7799**

ISO/IEC JTC 1/SC 27/WG 3 **N 999**

REPLACES: N

**ISO/IEC JTC 1/SC 27**

**Information technology - Security techniques**

**Secretariat: DIN, Germany**

**DOC. TYPE:** Dispositions of Comments

**TITLE:** Dispositions of comments on ISO/IEC 2nd WD 29147 (SC 27 N 7267)  
Information technology – Security techniques – Responsible  
vulnerability disclosure

**SOURCE:** 38<sup>th</sup> SC 27/WG 3 meeting

**DATE:** 2009-05-07

**PROJECT:** 29147

**STATUS:** Output document of the editing session for 2nd WD 29147 (SC 27 N 7267) held during the 38<sup>th</sup> SC 27/WG 3 meeting Beijing, China, May 4 – 8, 2009.

This document was available at the above-mentioned meeting. It is being circulated for information.

**ACTION:** FYI

**DUE DATE:**

**DISTRIBUTION:** P-, O-, and L- Members  
W. Fumy, SC 27 Chairman, M. De Soete, SC 27 Vice Chair  
E. Humphreys, K. Naemura, M. Ohlin, M.C. Kang, K. Rannenberg,  
WG-Conveners

**MEDIUM:** Server

**NO. OF PAGES:** 1 + 43

[All NBs<sup>1</sup>] comments on ISO/IEC 2nd WD 29147

Date: 2009-05-07	Document: <b>SC27 N7799</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

BE 1	Overall	N/A	ge	It was agreed to replace “receiving party” with “vendor”, see N7227, resolution to FI-7	Replace all references to “receiving party” with “vendor”	Duplicate Refer to UK 2
BE 2	3		Ge	Can editor explain why agreed change, as per N7227 FI-1, were not carried out in the WD2?		Duplicate Refer to UK 4.
BE 3	Overall	N/A	ge	Document lacks internal cohesion. It is just a set of paragraphs and sentences that are only loosely tied together.	Introduce structure into the document.	Duplicate Refer to UK 11
BE 4	Overall					Not accepted due to lack of detail
BE 5	6	paragraph 2 sentence 1	te	Description of vulnerability is not consistent with the definition given in 3.	Either remove the sentence or make it consistent with the vulnerability definition.	Duplicate Refer to UK 13 and FI 10
BE 6	6	paragraph 2 sentence 2	te	What is “observation”?	Either remove the word “observation” or explain what it was supposed to mean.	Duplicate Refer to UK 14
BE 7	6	paragraph 2 sentence 2	te	Vulnerability can be demonstrated only theoretically. This is usually present in crypto algorithms where theoretical break can be made several years before practical implementation of an attack.	Add “theoretical proof” in the list.	Duplicate Refer to UK 15
BE 8	6	paragraph 2 sentence 3	ge	The sentence express subjective views. Vulnerability in elevator’s breaking system can be more important than ability	Remove the sentence	Duplicate Refer to UK 16

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.

[All NBs<sup>1</sup>] comments on ISO/IEC 2nd WD 29147

Date: 2009-05-07	Document: <b>SC27 N7799</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

				to authenticate against entry door.		
BE 9	6	paragraph 3	te	Vulnerability is defined in a way that is not consistent with its definition in 3	Make the text consistent with the definition of the vulnerability	Duplicate refer to UK 17
BE 10	6	paragraph 5 sentence 2	ge	What is significance of this subdivision? Why it is important to further divide finders into various categories?	Remove the sentence or expand on the significance of this subdivision.	Duplicate refer to UK 18
BE 11	6	paragraph 6 sentence 2	te	What is relationship between researchers from this sentence from ones in 6, para 5, sent 2?	Explain relationship between these two groups.	Duplicate refer to UK 19
BE 12	6	paragraph 6 sentence 2	te	Who are “operators”?	Expand the term “operators”	Duplicate refer to UK 20
BE 13	6	paragraph 6 sentence 2	ge	What is significance of this subdivision?	Remove the sentence or expand on the significance of this subdivision.	Duplicate refer to UK 21
BE 14	6	paragraph 7 sentence 1	te	What is sub-component? This term is used but not defined.	Remove the references to “sub-component” or define the term.	Duplicate refer to UK 22
BE 15	6	paragraph 7 sentence 1	te	As written there is no difference between a vendor and sub-component owner (compare with 6, para 6, sent 1)	Explain difference between a vendor and sub-component owner or remove all reference s to sub-component owner	Duplicate refer to UK 23

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.

[All NBs<sup>1</sup>] comments on ISO/IEC 2nd WD 29147

Date: 2009-05-07	Document: <b>SC27 N7799</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

BE 16	6	Life Cycle... bullet 1 sentence 1	ge	“Discovering vulnerability is usually accomplished by research....” is subjective statement. It is also based on assumptions. There are many examples where vulnerabilities were discovered by chance.	Reword the sentence to remove subjectivity and assumptions.	Duplicate refer to UK 26
BE 17	6	Life Cycle... bullet 1 sentence 3	ge	Attacks are based on actual vulnerabilities and not the other way around as the current text suggests. It is possible to discover additional vulnerabilities while examining existing attacks.	Remove the sentence	Duplicate refer to UK 27
BE 18	6	Life Cycle... bullet 5 sentence 1	te	Vendor is asked to “...., cooperate in further research....” but is not clear what is the scope of this cooperation.	Explain the cooperation or remove this part of the sentence.	Duplicate refer to UK 28
BE 19	6	Phases of Vulnerability Disclosure	ge	How these phases fit into the lifecycle of the disclosure? We have two models (lifecycle and phases) that overlap in places but diverge otherwise.	Either provide explanation how these phases fit into the lifecycle or remove this text.	Duplicate refer to UK 29
BE 20	6.1	title	ge	Title is misleading	Change title to “vulnerability handling policy”	Duplicate refer to UK 30
BE 21	6.1	bullet 2	ge	Turn around times and responses are out of scope	Change into “expected acknowledge time”. How long should take for vendor to acknowledge receipt of the information.	Duplicate refer to UK 31 and US 30
	6.1.1	“process	ge	According to N7227, FI-14 the “process overview” should be	Move the “process overview” into an	Duplicate refer to UK 32

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.

[All NBs<sup>1</sup>] comments on ISO/IEC 2nd WD 29147

Date: 2009-05-07	Document: <b>SC27 N7799</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

BE 22		overview"		moved into an annex	annex	
BE 23	6.1.2	all	te	This information is out of place. According to N7227, FI-15 this section is to be removed from the main body and move into an annex.	Move the text into an annex	Duplicate refer to UK 33
BE 24	6.1.2	N/A	ge	Can the author explain why the section 6.1.2 is retained in the main text?		Duplicate refer to UK 34
BE 25	6.1.3	all	ge	Missing examples as per N7227, FI-16	Add examples as per Japanese contribution	Duplicate refer to UK 36
BE 26	6.1.3	all	ge	Can author explain why no examples were added as agreed per N7227, FI-16		Duplicate refer to UK 37
BE 27	6.1.3	all	te	It is unclear are we talking here about new, previously unknown vulnerabilities, or old ones. Text must clarify to which scenario 6.1.3 is applicable.	Clarify what vulnerabilities (old or new) text is talking about	Duplicate refer to UK 38
BE 28	6.1.3	all	te	If text pertains to newly discovered vulnerabilities it is unclear who is supposed to obtain CVE number. Is that incumbent upon finder or vendor?	Clarify who is to provide CVE numbers	Duplicate refer to UK 39
	6.1.3	bulleted list	te	Listed information is incomplete (even as an example).	Add the following items:	Duplicate refer to UK 40

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.

[All NBs<sup>1</sup>] comments on ISO/IEC 2nd WD 29147

Date: 2009-05-07	Document: <b>SC27 N7799</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
BE 29					<ul style="list-style-type: none"> <li>• software configuration</li> <li>• hardware model</li> <li>• hardware revision number</li> </ul> <input type="checkbox"/> relevant information about connected devices if vulnerability arises during interaction	
BE 30	6.1.3	bulleted list	te	The list must be prioritized. Some items (e.g., threat/risk assessment) are superficial when receiving information about a vulnerability.	Prioritize the list so it delineate items that must be provided (e.g., all factual information like configurations, versions, etc.) and one that is optional.	Duplicate refer to UK 41
BE 31	6.2.1	paragraph 1 sentence 2	te	The sentence suggests for vendor to have "...web forms or portal site to receive and track vulnerability reports". This is out of scope as it asks that vendor provide means for finders to track reports on vendor's web site.	Remove the sentence.	Duplicate refer to UK 42
BE 32	6.2.2	title	ge	Title is misleading. If a vendor is not affected why it should be notified at all?	Reword the title to match the text	Duplicate refer to UK 43
BE 33	6.2.2	paragraph 1 sentence 2	te	This is out of scope of the document. This touches upon global vendor coordination which is not part of this IS.	Remove the sentence.	Duplicate refer to UK 44
	6.2.3	paragraph 1	ge	It should be clarified if this acknowledgement is automatic	Clarify what constitutes	Duplicate refer to UK 45

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.

[All NBs<sup>1</sup>] comments on ISO/IEC 2nd WD 29147

Date: 2009-05-07	Document: <b>SC27 N7799</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
BE 34		sentence 1		(e.g., mail autoresponder) or by a person.	acknowledgement.	
BE 36	6.2.4	bullet c)	ge	Provide details how RSS can be used to support communication between finder and a vendor	Provide example how RSS can be use to communicate or remove the reference to RSS	Duplicate refer to UK 47
BE 37	6.2.5	paragraph 1	ge	It is unclear what kind of dispute can arise that coordinator can resolve.	Explain the nature of disputes that should be resolved by a coordinator	Duplicate refer to UK 48
BE 38	6.3	paragraph 2	ge	This paragraph is out of place. It is not connected with what 6.3 is about	Remove the paragraph	Duplicate refer to UK 50
BE 39	6.3	“Overview” and onwards	ge	This text, while seems to belong here, is not connected to the first paragraph. It is not clear from the text what this section of text describes.	Add text to link first paragraph to the rest of the text	Duplicate refer to UK 51
BE 40	6.3	“Threats” paragraph 1 sentence 2	ge	It is unclear to what “...the level of risk...” refers to. Risk to what?	Explain the nature of the risk	Duplicate refer to UK 52
BE 41	6.3	“Threats” paragraph 1 sentence 2	ge	“...probability of attack” is not possible to predict. Vendor can not state how probable is that someone will be attacked using a particular exploit/vulnerability.	Remove the reference to “probability of attack.”	Duplicate refer to UK 53
	6.3.1	title	ge	Title is not correct. Dissemination is a process so it can not be	Change the title to “Machine readable	Duplicate refer to UK 54

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.

[All NBs<sup>1</sup>] comments on ISO/IEC 2nd WD 29147

Date: 2009-05-07	Document: <b>SC27 N7799</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
BE 42				'formatted'. What is being disseminated can have a format.	advisory format" or similar.	
BE 43	6.3.1	all	ge	The purpose of this section is not clear. Several schemes are listed but it is not clear what is being suggested. What vendors and finders have to do if anything.	Clarify the purpose of this section. If it serves only to provide a snapshot of currently proposed and/or used schemas then it should be placed in an appendix and labelled as such.	Duplicate refer to UK 55
FI 1	All		ge	Every company will instantiate this standard according to its existing <b>internal</b> issue management process. This implies that this standard shall be a set of <b>guidelines and templates</b> with no fixed time-limit and fixed control-point mandates.	Taken into account in detailed changes below.	Accept in principle
FI 2	All		ge	This standard shall not mandate guidelines that mean duplicating or reinventing the <b>existing issue response networks</b> e.g. FIRST and the various CERTs	As above.	Accept in principle
FI 3	All		ge	This standard shall take into account the already existing multi-vendor vulnerability response initiatives such as ICASI ( <a href="http://www.icaso.org/">http://www.icaso.org/</a> ) and synchronise its guidelines with how that already functioning vendor-wide initiative generally functions in practice.	As above.	Accept in principle  Editor would ask that specific reference or alignment be sighted in comments.
FI 4	All		ed	The chapter numbering is wrong. E.g. Clause 4 does not exist	Correct the numbering	Accept
FI 5	Contents		ed	When this document matures (it is still quite under-developed), the Contents should ideally have headers	- Foreword - Introduction - Scope & audience	Accept in principle Will update table of contents according

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.

[All NBs<sup>1</sup>] comments on ISO/IEC 2nd WD 29147

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

				something like proposed here	<ul style="list-style-type: none"> <li>- Normative references</li> <li>- Terms and definitions</li> <li>- Symbols</li> <li>- Responsible vulnerability disclosure</li> <li>- Discovery</li> <li>- <i>Detection</i></li> <li>- <i>Reporting</i></li> <li>- <i>Acknowledgement</i></li> <li>- Information collecting</li> <li>- <i>Initial investigation &amp; intial report</i></li> <li>- <i>Verification</i></li> <li>- Resolution</li> <li>- <i>Containment</i></li> <li>- <i>Forensic deep investigation &amp; forensic report</i></li> <li>- <i>Resolution</i></li> <li>- <i>Patch / fix &amp; advisory review and approval</i></li> <li>- <i>Patch / fix &amp; advisory release</i></li> <li>- <i>Advisory</i></li> <li>- Feedback</li> <li>- Closure</li> <li>- Learning lessons</li> <li>- Security Policy implications</li> <li>- Utilisation of security networks</li> <li>- CERTs, etc.</li> <li>- Addendum</li> <li>- Template examples</li> <li>- Investigation report</li> <li>- Advisory</li> </ul>	to changes agreed upon during ad-hoc editing sessions.
--	--	--	--	------------------------------	---	--

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.

[All NBs<sup>1</sup>] comments on ISO/IEC 2nd WD 29147

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
FI 6	Introduction		ge	Introduction should attempt to mention what are the <u>benefits</u> of ISO-RVD for adopters. For example: gaining a structured vulnerability response framework, corporate RVD awareness, etc. Benefits must be communicated to "sell" the standard.		Accept in principle FI to provide editor with suggested text.
FI 7	Introduction		te	Introduction should already define not only "vulnerability" but also what "responsible disclosure" means.	Add the following text between current chapters of introduction: "Responsible Disclosure implies that the vulnerability finder and receiving party (for example a company, organisation, or vendor) work together diligently and ethically to produce a timely resolution to reduce any vulnerability-associated risks as much as possible and as soon as possible."	Accept in principle  Changed to the following: Responsible Disclosure implies that the vulnerability finder and vendor work together diligently to produce a timely resolution to reduce users' risks associated with the vulnerability.
FI 8	Introduction		Te	The Finder's objective may or may not be the same as the other participants	"The key stakeholders in this process; finders, vendors, sub-component owners and coordinators should have the same objective: reduce or eliminate vulnerabilities to ensure continued delivery of critical services and timely secure flow of information"	Not accepted  Decided to remove this sentence based on US 7
FI 9	3 Terms and Definitions	4.1 Receiving party	Te	According to Cyprus resolution on US comment 11, receiving party was supposed to be changed to vendor. Refer to N7227.	Remove definition for "Receiving Party"	Accept
	3 Terms	Definition for	te	The definition for "Vulnerability" explains what can cause	Change the definition for vulnerability to:	Accept

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.

[All NBs<sup>1</sup>] comments on ISO/IEC 2nd WD 29147

Date: 2009-05-07	Document: <b>SC27 N7799</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

FI 10	and Definitions	Vulnerability		<p>it and some consequences, but it does not define what it is, so the existing definitive should be preceded by a proper vuln definition.</p> <p>Section 6 goes on to actually define it to some extent, but a de facto definition belongs in the preceding Terms &amp; definitions section.</p>	<p>“A vulnerability is a weakness in a system which, if exploited, allows the exploiter to violate the security policy for that system. Examples of weaknesses in a system are software and hardware design flaws, poor administrative processes, lack of awareness and education, and advancements in the state of the art or improvements to current practices. Regardless of cause, an exploitation of such vulnerabilities may result in real threats to mission-critical information systems.”</p>	
-------	-----------------	---------------	--	---	---	--

FI 11	Section 6	Lifecycle of Vulnerability Disclosure	ed	<p>This section is rather convoluted - there are apparently two sort of duplicate sections - the Lifecycle should reflect the headers given in FI 5</p>	<p>Change the structure of the section as follows. Move current text under the new subsection titles.</p> <ul style="list-style-type: none"> <li>-Responsible vulnerability disclosure</li> <li>-Discovery</li> <li>-Detection</li> <li>-Reporting</li> <li>-Acknowledgement</li> <li>-Information collecting</li> <li>-Initial investigation &amp; intial report</li> <li>-Verification</li> <li>-Resolution</li> <li>-Containment</li> <li>-Forensic deep investigation &amp; forensic report</li> <li>-Resolution</li> <li>-Patch / fix &amp; advisory review and approval</li> </ul>	<p>Accept in principle</p> <p>Phases and steps will be integrated into a single lifecycle model including a new diagram</p> <p>Working progress titles are as follows:</p> <p>1. <b>Discovery Phase</b></p> <ol style="list-style-type: none"> <li>a. Discovery: A finder discovers a potential security vulnerability</li> <li>b. Notification: The finder notifies the vendor(s) of the potential vulnerability</li> <li>c. Acknowledgement: Vendors acknowledge receipt of the report,</li> </ol>
-------	-----------	---------------------------------------	----	---	--	--

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.

[All NBs<sup>1</sup>] comments on ISO/IEC 2nd WD 29147

Date: 2009-05-07	Document: <b>SC27 N7799</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

					-Patch / fix & advisory release -Advisory -Feedback -Closure -Learning lessons	<b>2. Verification Phase</b> <ol style="list-style-type: none"> <li>Initial Investigation: The vendor attempts to reproduce the vulnerability</li> <li>Root Cause Analysis: The vendor attempts to determine underlying causes of the vulnerability and attempts to identify the affected products including all possible methods of exploitation as it relates to the instance of the vulnerability.</li> <li>Further Investigation: Attempt to find other instances of the same type of vulnerability</li> <li>Triage: Determine severity of the vulnerability</li> </ol> <b>3. Resolution Phase</b> <ol style="list-style-type: none"> <li>Action Point: Vendor determines how they will deal with the vulnerability</li> <li>Produce Update: &lt; copy def. of update here &gt;</li> <li>Test Update: .....</li> </ol> <b>4. Advisory Phase</b> <b>Update Release:</b> Once the vendor is satisfied that the patch is effective and not harmful to most customer software
--	--	--	--	--	--	--

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.

[All NBs<sup>1</sup>] comments on ISO/IEC 2nd WD 29147

Date: 2009-05-07	Document: <b>SC27 N7799</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

						<p>environments, it notifies customers and the general public via an advisory.</p> <p>Post Release Phase  <b>Case Closure: After advisory has been released further updates to the advisory my continue</b> The vendor updates advisories as appropriate, generally until further updates are no longer relevant.</p> <p><b>Feedback:</b> Any new collateral effects, modifications of the malicious exploit, or new discoveries of the vulnerability or patch's effects on customer installations are fed back to the vendor that issued the patch. The reason could be that the vendor has confirmed with a high percentage of customers that affected software is patched; the affected software is obsolete; or the vulnerability and its solution are known for a long time. At this point, the case is considered closed</p>
FI 12	Section 6	Phases of Vulnerability Disclosure, last chapter before 6.1,	ed	Typo: Remainer	Remainder	<p>Accept</p> <p>Located in section just before 6.1</p>

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.

[All NBs<sup>1</sup>] comments on ISO/IEC 2nd WD 29147

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

		last sentence				
FI 13	Section 6.1	Responsible Vulnerability Policy	te	<p>Refer to N7227, FI 13: If the company has a security policy, it could be expanded to include a reference to vulnerability management.</p> <p>It is difficult to imagine all companies having a separate Responsible Vulnerability Policy. What would make more sense is that the ISO-RVD would be referred to in a company's Product Security Policy. This is why a new ISO-RVD section titled Security Policy Implications is being proposed (see FI 5).</p>	<p>Add reference to security policy.</p> <p>Create new Clause "Security Policy Implications" (Refer to FI 5).</p>	Accept
FI 14	Section 6.1	Responsible Vulnerability Disclosure, first chapter, last two sentences	Ed	Rewrite two last sentences.	"It can be as open as the vendor is willing to operate. Several examples are listed in Appendix B1: Sample Responsible Vulnerability Policies."	<p>Accept in principle</p> <p>Will correct sentence</p>
FI 15	Section 6.1	2 <sup>nd</sup> chapter	Ed	Typo: "should ,as a minimum"	Fix: "should, as minimum..."	<p>Accept in principle</p> <p>Will correct sentence</p>
FI 16	Section 6.1	Third bullet	ed	Typo: "depending"	...depend...	<p>Accept in principle</p> <p>Will correct sentence</p>
	Section	First	Ed	Last sentence does not make sense ("An individual ...")	Rewrite last sentence	Accept in principle

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.

[All NBs<sup>1</sup>] comments on ISO/IEC 2nd WD 29147

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
FI 17	6.1.1	paragraphs				Will correct sentence
FI 18	Section 6.1.1	2 <sup>nd</sup> paragraph	Ed	"May" should be used instead of "might"	Replace "may" with "might"	Accept in principle Will correct sentence
FI 19	Section 6.1.3	Bullet point list	Ed	The first bullet should be the title of the list	Change the intention of the first bullet	Accept in principle Will correct sentence
FI 20	6.2	2 <sup>nd</sup> paragraph	Ed	One sentence ends with two dots	Remove 2 <sup>nd</sup> dot	Accept in principle Will correct sentence
FI 21	Section 6.2.3	1 <sup>st</sup> paragraph	Ed	Typo: "should respond with a ..."	"...should respond within a period..."	Accept in principle Will correct sentence
FI 22	Section 6.2.4	3 <sup>rd</sup> paragraph, last sentence	Ed	Rewrite the last sentence starting with "Currently several technologies"	Rewrite (cut the sentence into two)	Accept in principle Will correct sentence
FI 23	Section 6.2.5	1 <sup>st</sup> paragraph	Ed	Typo: "is" is lacking	"It is hoped that both..."	Accept in principle Will correct sentence

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.

[All NBs<sup>1</sup>] comments on ISO/IEC 2nd WD 29147

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
FI 24	Section 6.2.5	2 <sup>nd</sup> paragraph	Ed	Typo: "The coordinator should be vendor neutral and willing to worth with..."	Replace "worth" with "work"	Accept in principle Will correct sentence
FI 25	Section 6.3	"Solution"	Te	Are the listed solutions the only possible ones?	Change the sentence to "Provide information on for example how to install the fixed product or update, or on how to apply a security patch.	Not accepted Refer to US 46
FI 26	Section 6.3.1	Dissemination Formatting	Te	It is good that this section mentions already existing vuln info exchange formats e.g. CVE and environmental impact scoring e.g. CVSS.  These should be kept as examples.		Accepted in principle Moved to annex during ad-hoc editing session.
JP 1	1	Last paragraph	Te	In order to reduce vulnerability-related risks, the parties whom the vulnerability resolution information is disseminated to should be decided carefully on case-by case basis instead of always "all interested parties."	This IS aims to ensure that vendors have the capability for receiving information about a potential vulnerability and disseminating vulnerability information to <u>appropriate parties</u> so that the risk for attackers to exploit the vulnerability is minimized.	Accept in principle  Updated changes to Intro based on FI 7 are acceptable to address the changes requested.
JP 2	3	2 <sup>nd</sup> line	Ed	There is an editorial error, and the fourth clause is missing.	The second line "4.1" in the third clause should be deleted.  The clause numbers after five should be reassigned from four.	Accept in principle Will realign numbering
	6	Paragraphs 1 -- 8	Ed	The nature of description in these paragraphs seems to be definition of terms, which are those of vulnerability,	These paragraphs should be relocated into clause 3 (Terms and definitions)	Accept in principle

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.

**[All NBs<sup>1</sup>] comments on ISO/IEC 2nd WD 29147**

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

JP 3				proof-of-concept code, incident activity, finder, vendor, sub-component owner, distribution.	and be polished as description of definitions.	Will update the terms and definitions
JP 4	6	5 <sup>th</sup> paragraph	Te	While most of vulnerabilities of products, or a fairly large amount of them, at least, are found by vendor themselves, vendors are not included in the enumeration of finder subgroups.	Vendors should be added to the finder subgroup enumeration.	Accept in principle Will update sentence
JP 5	6	Sub-clause structure	Ed	The essential part of this IS consists of only one clause – the sixth clause, which consists of complex sub-clauses. The clause structure should be reconsidered.	The following is a proposed clause structure (Sub-clauses are omitted for simplification):  6. Vulnerability Handling Framework, whose contents should be the part of 6 through 6.1.2 of 2nd WD,  7. Receiving Vulnerability Information, whose contents should be the part of 6.2 through 6.2.5 of 2nd WD,  8. Disseminating Vulnerability Information, whose contents should be the part of 6.3 through 6.3.1 of 2nd WD.	Accept in principle Will seek to realign the body of the document  Will renumber sub-sections accordingly.
JP 6	6 Disclosure	Figure	Ed	The number and title of the figure should be given. Some description referring this figure should be created.	The figure title should be something like “Figure 1. Stakeholders in vulnerability handling by a vendor.”	Accept in principle Add title to figure
JP 7	6	Section title of “Life Cycle of Vulnerability	Ed	The section title of “Life Cycle of Vulnerability Disclosure” is not appropriate, since disclosure is an action but not an object which has its life time.	Alternative section title is:  ☺ Life Cycle of Vulnerability	Accept in principle

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.

[All NBs<sup>1</sup>] comments on ISO/IEC 2nd WD 29147

Date: 2009-05-07	Document: <b>SC27 N7799</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

		Disclosure			or ⌚ Vulnerability Reporting Process	Will update to reflect "Life Cycle of a Vulnerability"
JP 8	6	Section of "Phases of Vulnerability Disclosure"	Ed	<p>⌚ The section title "Phases of Vulnerability Disclosure" is not appropriate, since "discovery" phase and "validation" phase, which are listed in this section, are not elements of the disclosure process.</p> <p>⌚ The description in this section seems to be the same as one of the followed section entitled "Life Cycle of Vulnerability" in essence</p>	The two sections, "Life Cycle of Vulnerability Disclosure" and "Phases of Vulnerability Disclosure" should be merged into one section and refined to get rid of the redundancy.	<p>Accept in principle</p> <p>Will update to eliminate the redundancy and better align the content of these sections.</p>
JP 9	6	Purpose or benefits of RVD	Ge	The 2 <sup>nd</sup> WD includes little description about benefits of the RVD and the vulnerability handling.	<p>Some description such as the following, which is cited from the guideline by Organization for Internet Safety (<a href="http://www.oisafety.org">http://www.oisafety.org</a>), should be included in clause 6 or 1:</p> <p>⌚ It can minimize the risk posed by security vulnerabilities, by enabling them to be identified, investigated, and resolved in a way that produces a timely, high –quality remedy that will have high uptake among the affected systems.</p> <p>⌚ It can also contribute to improving</p>	Accept will add these statements

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.

[All NBs<sup>1</sup>] comments on ISO/IEC 2nd WD 29147

Date: 2009-05-07	Document: <b>SC27 N7799</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
					the engineering quality of software products, by supporting the academic and research communities' ongoing efforts to identify common security vulnerabilities, the conditions under which they occur, and methods to avoid them.	
JP 10	6.1.1	"Process Overview"	Ed	Apparently "Process Overview" is beyond the subject of "Contact Gateway."	The part following the tile "Process Overview" should be raised in to a new clause. The new clause may possibly be merged with the current clause 6.1.1 entitled "Anticipated Response Times and Actions."	Accept in principle Refer to JP 5 for section realignment.
JP 11	6.1.2	Anticipated Response Times	Te	It is very controversial to specify exact number as anticipated response times, which should not be included in our IS. For example, Hasan Cavusoglu's paper "Efficiency of Vulnerability Disclosure Mechanisms to Disseminate Vulnerability Knowledge" (IEEE Tr. on Software Engineering, Vol. 33, No. 3, March 2007) theoretically shows that inappropriate deadline for vulnerability information release may fail to motivate vendors to release patches. In the case, specifying anticipated response times a priori increases social security risks in the end.	All the description about anticipated response times should be deleted.  Or, we should list up items which should be considered in order to decide a best response timeline for each case instead of specifying certain response times a priori.	Accept in principle  Table to be removed based on US 34
JP 12	6.1.3		Ge	This clause seems to be described for those who find and report vulnerabilities, but not for vendors for whom this IS targets.	This clause should be deleted or should be moved into 6.2 (Receiving Vulnerability Information) as a list of items which vendors should inspect on	Accept

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.

[All NBs<sup>1</sup>] comments on ISO/IEC 2nd WD 29147

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

					reception. In the latter case, "multi-vendor or not" should be added as an item of the list.	
JP 13	6.2.1 and 6.2.4		Te	Some dissemination of vulnerability information should be also done through a secure channel to keep its confidentiality. So a secure communication model should be applied not only for receiving but also for disseminating.  There seems to be overlap between 6.2.1 and 6.2.4	These clauses should be moved to a framework section after merging.	Accept
JP 14	6.2.2	1 <sup>st</sup> paragraph	Te	Since it is very difficult for finders and vendors to notify all the affected vendors comprehensively in case of multi-vendor issues, they should ask a coordinator to do so instead of doing by themselves.	The 2 <sup>nd</sup> sentence should be:  In the case, finders and vendors should notify all the affected vendors through coordinators. They may also directly do it if they can do comprehensively,	Accept
JP 15	6.2.3	3 <sup>rd</sup> paragraph	Te	Since those standard contact e-mail addresses tend to be targets of spam in these day, we had better not mention them.	It should be deleted.	Accept in principle  Remove list of sample addresses and replace with a sentence that states use standard vendor policy for creating a e-mail address that reflects a contact point for disclosure.
JP 16	6.2.3		Ge	Vendors have to investigate the received vulnerability information and make some decisions about it before acknowledging it. Description about investigation is missing in 2 <sup>nd</sup> WD.	Summarized version of Clause 6 with Figure 4 in the guideline by Organization for Internet Safety ( <a href="http://www.oisafety.org">http://www.oisafety.org</a> ) should be	Accept in principle

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.

[All NBs<sup>1</sup>] comments on ISO/IEC 2nd WD 29147

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

					introduced somewhere in clause 6.2.	
JP 17	6.2.3	3 <sup>rd</sup> and 4 <sup>th</sup> paragraphs	Ed	These paragraphs should not be in this context, since neither e-mail alias nor on-line helpdesk is matters to be considered in the acknowledgement phase.	These paragraphs should be moved into a framework section.	Accept in principle  Updated 4 <sup>th</sup> paragraph sentence 1 to be "In some instances a vendor can leverage a case or on-line helpdesk function."
JP 18	6.3		Ge	The document structure of this clause should reflect our consensus (N6763) in the Kyoto meeting.	The sub-clause structure should be as follows: 6.3.1 Introduction 6.3.2 Terminology (might be skipped) 6.3.3 Lifecycle (diagram) 6.3.4 Minimum content requirement 6.3.5 Single owner dissemination of vulnerability information 6.3.6 Multi owner dissemination of vulnerability information	Not Accepted  A new lifecycle outline was developed in ad-hoc editing sessions that were acceptable changes to the current sub-clause mapping.
JP 19	6.3		Te	Not only the format but also the channel or communication media for dissemination should be addressed in this IS.	Some description such as the 4 <sup>th</sup> clause of N6880 (Vulnerability Disclosure Guideline for Software Developers) should be included	Accept in principle  Will add the subclause.
LU 1	All	All	Ge	According to Roadmap WG4 (N6907) :  Section 4, (a) : <i>In addition, new standards in the area of</i>	Suggestion to reconsider the integration of the project 29147 - Responsible vulnerability disclosure within WG4	Not accepted

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.

[All NBs<sup>1</sup>] comments on ISO/IEC 2nd WD 29147

Date: 2009-05-07	Document: <b>SC27 N7799</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

				<p><i>vulnerability and updates management [...] Note that WG 3 is also developing a standard relating to vulnerability reporting. There may be overlaps in this requirement for vulnerability and updates management in WG 4 Roadmap, to be resolved with WG 3 in future meetings</i></p> <p>Annex F : <i>There is a potential overlap in the scope of WG 4 Roadmap in the area of "Vulnerabilities and Updates Management" with WG 3's currently being developed standard on "Responsible Disclosure and Vulnerability Reporting". See Section 4 (a) in main text of Roadmap document</i></p>	instead of WG3	Please refer to N6763 for the identified scope of work. We believe that this project is fully within the scope of WG3.
UK 1	-	-	ge	This has the makings of a good outline of the Vulnerability Disclosure process but the document is obviously not finished yet. A number of areas of this document need fleshing out before it can progress to CD status.	Complete document as a matter of urgency.	Accept
UK 2	Overall	-	ge	It was agreed to replace "receiving party" with "vendor", see N7227, resolution to FI-7	Replace all references to "receiving party" with "vendor"	Accept
UK 3	2	Normative references	ed	The list is currently empty. Given the nature of this standard, the UK would wish to review the references that are regarded as normative.	Complete clause as a matter of urgency.	Accept
UK 4	3		ge	Can editor explain why agreed change, as per N7227 FI-1, were not carried out in the WD2?	Please provide justification or implement previously agreed change.	Accept will implement changes as previously agreed
UK 5	4	Title	ed	No clause title. Probably continuation of clause 3.	Provide clause title or remove/renumber.	Accept
UK 6	4.1	Software	te	This definition is marked for alignment with SC7. Should also cross-correlate with other activities in SC22 and SC27.	Make appropriate checks.	Accept

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.

[All NBs<sup>1</sup>] comments on ISO/IEC 2nd WD 29147

Date: 2009-05-07	Document: <b>SC27 N7799</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
UK 7	4.1	Application	te	This definition is marked for alignment with SC7. Should also cross-correlate with other activities in SC22 and SC27.	Make appropriate checks.	Accept
UK 8	4.1	Patch	te	This definition is marked for alignment with SC7. Should also cross-correlate with other activities in SC22 and SC27.	Make appropriate checks.	Accept
UK 9	4.1	Fix	te	This definition is marked for alignment with SC7. Should also cross-correlate with other activities in SC22 and SC27.	Make appropriate checks.	Accept
UK 10	4.1	Vendor	te	This definition is marked for alignment with SC7. Should also cross-correlate with other activities in SC22 and SC27.	Make appropriate checks.	Accept
UK 11	6 onwards	N/A	ge	Document lacks internal cohesion. It is just a set of paragraphs and sentences that are only loosely tied together.	Introduce structure into the document.	Accept in principle
UK 12	6	-	ed	This clause is not structured in accordance with ISO style. It contains unnumbered divisions and “hanging paragraphs”.	Follow rules of ISO Directives part 2.	Accept
UK 13	6	paragraph 2 sentence 1	te	Description of vulnerability is not consistent with the definition given in 3.	Either remove the sentence or make it consistent with the vulnerability definition.	Accept see FI 10
UK 14	6	paragraph 2 sentence 2	te	What is “observation”?	Either remove the word “observation” or explain what it was supposed to mean.	Accept will remove word
UK 15	6	paragraph 2 sentence 2	te	Vulnerability can be demonstrated only theoretically. This is usually present in crypto algorithms where theoretical break can be made several years before practical implementation of an attack.	Add “theoretical proof” in the list.	Accept will add to list
UK 16	6	paragraph 2	ge	The sentence express subjective views. Vulnerability in	Remove the sentence	Accept will remove sentence

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.

[All NBs<sup>1</sup>] comments on ISO/IEC 2nd WD 29147

Date: 2009-05-07	Document: <b>SC27 N7799</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

		sentence 3		elevator's breaking system can be more important than ability to authenticate against entry door.		
UK 17	6	paragraph 3	te	Vulnerability is defined in a way that is not consistent with its definition in 3	Make the text consistent with the definition of the vulnerability	Accept will align to def. used in terms
UK 18	6	paragraph 5 sentence 2	ge	What is significance of this subdivision? Why it is important to further divide finders into various categories?	Remove the sentence or expand on the significance of this subdivision.	Accept will remove sentence
UK 19	6	paragraph 6 sentence 2	te	What is relationship between researchers from this sentence from ones in 6, para 5, sent 2?	Explain relationship between these two groups.	Accept will remove the sentence
UK 20	6	paragraph 6 sentence 2	te	Who are "operators"?	Expand the term "operators"	Refer to UK 19
UK 21	6	paragraph 6 sentence 2	ge	What is significance of this subdivision?	Remove the sentence or expand on the significance of this subdivision.	Refer to UK 19
UK 22	6	paragraph 7 sentence 1	te	What is sub-component? This term is used but not defined.	Remove the references to "sub-component" or define the term.	Accept will remove the sentence
UK 23	6	paragraph 7 sentence 1	te	As written there is no difference between a vendor and sub-component owner (compare with 6, para 6, sent 1)	Explain difference between a vendor and sub-component owner or remove all reference s to sub-component owner	Refer to UK 22
UK 24	6	Paragraph 8 sentence 1	te	Use the term ISIRT not CERT to align with ISO/IEC 27035 (WD)	Change to ISIRT	Not accepted this term is not an industry accepted term
UK 25	6	Diagram	te	The diagram showing Life Cycle of Vulnerability disclosure is very high level	It should be expanded to reflect the role of ISIRTs as defined in ISO/IEC 27035 (WD), and other communities of interest e.g. WARPs ( <a href="http://www.warp.gov.uk">http://www.warp.gov.uk</a> )	Accept in principle Refer to US 24
UK 26	6	Life Cycle... bullet 1	ge	"Discovering vulnerability is usually accomplished by research..." is subjective statement. It is also based on	Reword the sentence to remove	Accept in principle

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.

[All NBs<sup>1</sup>] comments on ISO/IEC 2nd WD 29147

Date: 2009-05-07	Document: <b>SC27 N7799</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

		sentence 1		assumptions. There are many examples where vulnerabilities were discovered by chance.	subjectivity and assumptions.	Refer to FI 11
UK 27	6	Life Cycle... bullet 1	ge	Attacks are based on actual vulnerabilities and not the other way around as the current text suggests. It is possible to discover additional vulnerabilities while examining existing	Remove the sentence	Accept in principle Refer to FI 11
UK 28	6	Life Cycle... bullet 5 sentence 1	te	Vendor is asked to “...., cooperate in further research....” but is not clear what is the scope of this cooperation.	Explain the cooperation or remove this part of the sentence.	Accept in principle Refer to FI 11
UK 29	6	Phases of Vulnerability Disclosure	ge	How these phases fit into the lifecycle of the disclosure? We have two models (lifecycle and phases) that overlap in places but diverge otherwise.	Either provide explanation how these phases fit into the lifecycle or remove this text.	Accept in principle Refer to FI 11
UK 30	6.1	title	ge	Title is misleading	Change title to “vulnerability handling policy”	Accept Will change the title
UK 31	6.1	bullet 2	ge	Turn around times and responses are out of scope	Change into “expected acknowledge time”. How long should take for vendor to acknowledge receipt of the information.	Accept in principle Refer to US 30
UK 32	6.1.1	“process overview”	ge	According to N7227, FI-14 the “process overview” should be moved into an annex	Move the “process overview” into an annex	Not Accepted Moved this section to new section 7 of ad-hoc revision.
UK 33	6.1.2	all	te	This information is out of place. According to N7227, FI-15 this section is to be removed from the main body and move into an annex.	Move the text into an annex	Accepted Table was relocated to annex in this revision
UK 34	6.1.2	N/A	ge	Can the author explain why the section 6.1.2 is retained in the	Please provide justification or	Accept

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.

**[All NBs<sup>1</sup>] comments on ISO/IEC 2nd WD 29147**

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
				main text?	implement previously agreed change.	Refer to US 34 section to be replaced by single sentence
UK 35	6.1.2	Anticipated Response Times and Actions table	Te	Response Timeline Table incomplete	Although it is accepted this table is marked as incomplete, the column "Time to Respond" will need to be considered, possibly retitle as "Typical .." or "Best Practice ..."	Not accepted Refer to US 34
UK 36	6.1.3	all	ge	Missing examples as per N7227, FI-16	Add examples as per Japanese contribution	Accept Will include JP contributions as per N7227, FI 16.
UK 37	6.1.3	all	ge	Can author explain why no examples were added as agreed per N7227, FI-16	Please provide justification or implement previously agreed change.	Accept Will add sections agreed and realign to ad-hoc version
UK 38	6.1.3	all	te	It is unclear are we talking here about new, previously unknown vulnerabilities, or old ones. Text must clarify to which scenario 6.1.3 is applicable.	Clarify what vulnerabilities (old or new) text is talking about	Accept in principle will attempt to realign in document
UK 39	6.1.3	all	te	If text pertains to newly discovered vulnerabilities it is unclear who is supposed to obtain CVE number. Is that incumbent upon finder or vendor?	Clarify who is to provide CVE numbers	Accept in principle Add sentences that identify the two methods that include getting a CVE from Mitre or vendors that have large block of CVEs assigned  < Finder will not typically obtain the CVE number when they first report the

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.

**[All NBs<sup>1</sup>] comments on ISO/IEC 2nd WD 29147**

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

						vulnerability to the vendor>
UK 40	6.1.3	bulleted list	te	Listed information is incomplete (even as an example).	Add the following items: <ul style="list-style-type: none"> <li>• software configuration</li> <li>• hardware model</li> <li>• hardware revision number</li> <li>• relevant information about connected devices if vulnerability arises during - interaction</li> </ul>	Accept Add to the current list
UK 41	6.1.3	bulleted list	te	The list must be prioritized. Some items (e.g., threat/risk assessment) are superficial when receiving information about a vulnerability.	Prioritize the list so it delineate items that must be provided (e.g., all factual information like configurations, versions, etc.) and one that is optional.	Accept in principle Change the first bullet to become “useful information might include” ---- align to title Remove the bullet in front of this statement
UK 42	6.2.1	paragraph 1 sentence 2	te	The sentence suggests for vendor to have “...web forms or portal site to receive and track vulnerability reports”. This is out of scope as it asks that vendor provide means for finders to track reports on vendor’s web site.	Remove the sentence.	Accept in principle  We agreed that we would indicate that vendors “can” offer this
UK 43	6.2.2	title	ge	Title is misleading. If a vendor is not affected why it should be notified at all?	Reword the title to match the text	Accept Changed to “Issues that Affect Multiple

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.

[All NBs<sup>1</sup>] comments on ISO/IEC 2nd WD 29147

Date: 2009-05-07	Document: <b>SC27 N7799</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
						Vendors”
UK 44	6.2.2	paragraph 1 sentence 2	te	This is out of scope of the document. This touches upon global vendor coordination which is not part of this IS.	Remove the sentence.	Accept in principle Move bullet to new advisory section and expand discussion on multi-vendor release
UK 45	6.2.3	paragraph 1 sentence 1	ge	It should be clarified if this acknowledgement is automatic (e.g., mail autoresponder) or by a person.	Clarify what constitutes acknowledgement.	Accept Will add statement to clarify
UK 46	6.2.3	paragraph 1 sentence 4	ge	Acknowledgement can be in any agreed form and not only electronic.	Remove the word “electronic”	Not Accept In principle however electronic is mean to reference a audit mechanism. A sentence should be added to reflect this concept.
UK 47	6.2.4	bullet c)	ge	Provide details how RSS can be used to support communication between finder and a vendor	Provide example how RSS can be use to communicate or remove the reference to RSS	Accept Will add statement for RSS
UK 48	6.2.5	paragraph 1	ge	It is unclear what kind of dispute can arise that coordinator can resolve.	Explain the nature of disputes that should be resolved by a coordinator	Accept in principle Will add list of disputes that might result
UK 49	6.2.5	paragraph 1		Rather than naming specific ISIRTs (see UK comment 24), it would be preferable to name “umbrella” bodies would could act as the way to contact such ISIRTs. The main such umbrella organisations would be: • FIRST • Trusted Introducer (for Europe)	Change technical recommendation.	Not accepted The is subjective statement based on organizations.

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.

[All NBs<sup>1</sup>] comments on ISO/IEC 2nd WD 29147

Date: 2009-05-07	Document: <b>SC27 N7799</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

				• APCERT (for Asia / Pacific)		
UK 50	6.3	paragraph 2	ge	This paragraph is out of place. It is not connected with what 6.3 is about	Remove the paragraph	Accept in principle the title should be changed to reflect this discusses coordinated releases Refer to US 46
UK 51	6.3	“Overview” and onwards	ge	This text, while seems to belong here, is not connected to the first paragraph. It is not clear from the text what this section of text describes.	Add text to link first paragraph to the rest of the text	Accept in principle Refer to US 46
UK 52	6.3	“Threats” paragraph 1 sentence 2	ge	It is unclear to what “...the level of risk...” refers to. Risk to what?	Explain the nature of the risk	Accept in principle will update to list possible risks to vulnerability. Most vendors to have risk levels that such as critical, informational, etc.
UK 53	6.3	“Threats” paragraph 1 sentence 2	ge	“...probability of attack” is not possible to predict. Vendor can not state how probable is that someone will be attacked using a particular exploit/vulnerability.	Remove the reference to “probability of attack.”	Accept in principle Refer to US 47
UK 54	6.3.1	title	ge	Title is not correct. Dissemination is a process so it can not be ‘formatted’. What is being disseminated can have a format.	Change the title to “Machine readable advisory format” or similar.	Not accepted Refer to US 48
UK 55	6.3.1	all	ge	The purpose of this section is not clear. Several schemes are listed but it is not clear what is being suggested. What vendors and finders have to do if anything.	Clarify the purpose of this section. If it serves only to provide a snapshot of currently proposed and/or used schemas then it should be placed in an appendix and labelled as such.	Accept in principle Refer to US 48
UK 56	A.2	Vulnerability Resolution	Ed	Partial diagram at top of page 12	Remove or expand.	Accept in principle

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.

[All NBs<sup>1</sup>] comments on ISO/IEC 2nd WD 29147

Date: 2009-05-07	Document: <b>SC27 N7799</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

		Process Life Cycle				Will provide a better diagram
UK 57	A.3	-	Ge	Unable to comment as no content	Remove or expand.	Accept Remove A.3
UK 58	Annex B	(informative)	Ge	Unable to comment as no content	Remove or expand.	Accept in principle Currently just a placeholder
US 1	Overall	N/A	Te	The document has pieces of the NIAC Vulnerability Disclosure Framework and other prior vulnerability disclosure policies cut and pasted together in a piecemeal patchwork of incomplete and sometimes contradictory elements.	Review the entire document with the strict scope in mind, in order to eliminate duplicate or contradictory sections and sections that do not apply to this document due to scope restrictions.  This document needs to be written from the perspective of Vendors.	Accept in principle  Will seek to align to vendors perspective
US 2	Overall	N/A	Ed	The document is full of typos and grammatical errors.	Proofread and edit the entire document for spelling and grammar.	Accept in principle  Will correct issues the next edition is developed
US 3	Entire document	N/A	Te	Organization is indecipherable. Topics are duplicated, terms are mixed, there is little logical flow.	Clarify scope, develop outline/table of contents, and rebuild document.	Accept in principle  See FI 5 and JP 5 Will rebuild document to align to scope

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.

[All NBs<sup>1</sup>] comments on ISO/IEC 2nd WD 29147

Date: 2009-05-07	Document: <b>SC27 N7799</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 4	Entire document	Para 1	Te	Various terms are used, causing confusion, e.g. patch/fix, finder/discoverer, vendor/sub-component owner, customer/user, notification/report, evaluation/validation, repair/resolution	Select and define terms then use terms consistently throughout.	Accept in principle Will update and align as next edition is created
US 5	Introduction	Para 1	Te	Vulnerability disclosure concerns more narrowly information about vulnerabilities, not broadly any “information security problem.”	Suggest something more specific to vulnerabilities, for example: “Vulnerability disclosure is the practice of reporting, coordinating, and publishing information about a vulnerability.”	Accept
US 6	Introduction	Para 1	Te	“Vulnerabilities in technology vital to operations represent a threat.” Vulnerabilities are not threats. A threat is usually the action of an attacker or force that exploits a vulnerability.	Replace “Vulnerabilities in technology vital to operations represent a threat.” with “Vulnerabilities in technology vital to operations represent an increased risk.”	Accept
US 7	Introduction	Para 1, last sent	Ge	The last sentence of the first paragraph makes assumptions about the goals of all parties in disclosure. Not all of them share the same goal.	Remove last sentence of first paragraph “The key stakeholders in this process; finders, vendors, sub-component owner and coordinators have the same objective: reduce or eliminate vulnerabilities to ensure continued delivery of critical services and timely secure flow of information.”	Accept
US 8	4	Terms	Te	Add term to describe incidents/attacks/exploit activity	Use the term “Incident Activity” defined as evidence of attacks that attempt to exploit a vulnerability, whether successful or not.	Accept in principle Will update to ensure consistency in next edition.

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.

[All NBs<sup>1</sup>] comments on ISO/IEC 2nd WD 29147

Date: 2009-05-07	Document: <b>SC27 N7799</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

					Use consistently throughout.	
US 9	4.1	Definition of Finder	Te	The definition of Finder should be generalized to “person or organization”. “Security researcher” and “customer” are two examples of a “person”.	Replace “The security researcher, customer, or other interested person or organization who identifies the vulnerability.”  With “The person or organization who identifies the vulnerability.”	Accept
US 10	4.1	Term Receiving Party	Te	In Limassol, Cyprus, all National Body representatives agreed to replace all instances of “Receiving Party” with “Vendor”. See SC27N7227_WG3N967_Doc_27147 :Comment US 11.	Remove the term “Receiving Party” throughout the document and replace it with “Vendor”.	Accept
US 11	4.1	Term Patch	Te	“Patch” implies something quickly thrown together, whereas “Update” usually implies the code has been tested.  “Fix” and “Patch” are somewhat redundant. The term should define a change to software/component that ideally resolves (or at least lessens) the vulnerability.	Replace “Patch” with “Update”.  Choose one term - “Update” - and define that “Update” covers patch, fix, possibly upgrade (list commonly used terms).  Use “Update” consistently throughout.	Accept in principle  Will update to use term update and add definition. SC7 will have to provide a ruling to the term being used.
US 12	4.1	Term Update	Te	Definition proposed.	A software change intended to resolve or mitigate a vulnerability. An update typically takes the form of a configuration change, binary file replacement, hardware change, or source code patch, etc. Updates are usually provided by vendors. Vendors use different terms including patch, fix, and upgrade.	Accept in principle  Will update to use term update and add definition. SC7 will have to provide a ruling to the term being used.

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.

[All NBs<sup>1</sup>] comments on ISO/IEC 2nd WD 29147

Date: 2009-05-07	Document: <b>SC27 N7799</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	4.1	Term Coordinator	Te	Definition proposed.	An optional participant that can serve as a proxy for the Finder, assists with technical evaluations, coordinates among multiple vendors, or performs other functions to promote the effectiveness of the vulnerability response process.	Accept in principle Will update to use term update and add definition. SC7 will have to provide a ruling to the term being used.
US 14	4.1	Term Vulnerability	Te	New definition proposed.	Vulnerabilities can be A set of conditions, often a coding defect or insecure design, that permits the violation of a security policy. A vulnerability can also be caused by insecure administration, changing environmental conditions, or complex interactions between systems.	Accept in principle  Refer to FI 10 Will update to use term update and add definition. SC7 will have to provide a ruling to the term being used.
US 15	4.1	Term Fix	Te	Synonymous with "Update".	Delete "Fix"	Accept
US 16	4.1	Definition Vendor	Te	"Receiving Party" definition is now "Vendor" definition. See SC27N7227_WG3N967_Doc_27147 : Comment US 11.	Definition of Vendor should be: "The person, organization, or company that developed the software, application, web service, or is responsible for maintaining it."	Accept
US 17	4.1	Term Vendor	Te	Definition proposed.	Person or organization responsible for developing updates.	Not accepted duplicate of US 16
US 18	4.1	Term Responsible Disclosure	Te	Title term must be defined.	Private advance disclosure of a vulnerability to a Vendor or Coordinator where Vendor is allowed time to produce a fix prior to public disclosure.	Accept

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.

[All NBs<sup>1</sup>] comments on ISO/IEC 2nd WD 29147

Date: 2009-05-07	Document: <b>SC27 N7799</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 19	4.1	Term Vulnerability Information Service (VIS)	Te	New definition proposed.	Replace existing definition with “A Vulnerability Information Service is an organization that acts as an aggregator or distributor for vulnerability information. Finders and Vendors can provide information to these services or add references to them when publishing vulnerability information. “	Accept  Will update to use term update and add definition. SC7 will have to provide a ruling to the term being used.
US 20	4.1	Term Advisory	Te	Definition proposed.	A document that describes a vulnerability. An advisory may be published by a Vendor, Finder, or Coordinator. An Advisory typically contains a description of the vulnerability including a list of vulnerable software, potential impact, resolution and mitigation information, and references.	Accept in principle  Will update to use term update and add definition. SC7 will have to provide a ruling to the term being used..
US 21	6	Para 1	Te	A new definition on vulnerability is used in this section than was defined in section 4.1. There is no need to define vulnerability again in this section.	Delete Paragraph 1.	Accept
US 22	6	Para 2	Te	Demonstration of a vulnerability is irrelevant to this document’s scope. Vulnerabilities in different types of systems is irrelevant for purposes of this document.	Delete Paragraph 2.	Accept
US 23	6	Para 3 - 8	Te	These paragraphs are irrelevant to the purpose of this document.	Delete Paragraphs 3-8. Rewrite to reflect the Vulnerability Resolution Process Lifecycle correlating to the	Accept

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.

[All NBs<sup>1</sup>] comments on ISO/IEC 2nd WD 29147

Date: 2009-05-07	Document: <b>SC27 N7799</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

					diagram (see next comment).	
US 24	6	Diagram	Te	This diagram is unclear as to process, information flow, and roles.	Replace this diagram with the NIAC Framework page 15 Vulnerability Resolution Process Lifecycle diagram.	<p>Accept in principle</p> <p>Submitted from US during Kyoto meeting.</p> <p>Will create a new diagram that reflects the combination of phases and steps agreed upon during ad-hoc editing sessions.</p>
US 25	6	Figure on page 3	Ge	<p>There's an inconsistency between this figure and the text immediately above it, which uses the terms "sub-component owner", and section 6.2.4 which uses the term "component owner"</p> <p>See SC27N7227_WG3N967_Doc_27147 : Comment US 11</p> <p>Distinction between vendor and sub-component owner is not useful and distracting. "Vendor" is the term for the party responsible for the vulnerable software.</p> <p>OK to note software relationships/dependencies, e.g. vendor A uses a component from vendor B.</p>	Replace all instances of "component owner" and "sub-component owner" with "Vendor" throughout the document.	Accept
US 26	6	Lifecycle of Vulnerability Disclosure and Phases of Vulnerability Disclosure	Te	These sections are each cut and pasted from the NIAC framework and other prior vulnerability disclosure guides and describe the same process in slightly different ways.	Use The Phases of Vulnerability disclosure.	<p>Accept in principle</p> <p>Will update to aligned to phases and steps as created during ad-hoc editing sessions.</p> <p>Refer to FI 11</p>

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.

[All NBs<sup>1</sup>] comments on ISO/IEC 2nd WD 29147

Date: 2009-05-07	Document: <b>SC27 N7799</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 27	6	Last Para	Te	Scope is unclear. See SC27N7227_WG3N967_Doc_27147 : Comment FI 5.	This paragraph should be rewritten from a vendor's perspective.	Accept in principle Update to reflect vendor perspective
US 28	6: Phases of Vulnerability Disclosure	1	Te	Suggestion for clarification	Change "recovering aspect" and "dissemination aspect" to "recovering element" and "dissemination element" – or add verbiage in this paragraph to describe what these two areas are aspects of.	Accept in principle US NB will provide the paragraph updates.
US 29	6.1 Responsible Vulnerability Policy	Section Title	Te	Title is confusing.	Suggestion: Change to "Vulnerability Handling Policy" or similar.	Accept Refer to UK 30
US 30	6.1	Entire	Te	As discussed in Limassol, Cyprus, all timeline discussion and suggestions should be placed in an Annex. See SC27N7227_WG3N967_Doc_27147 : Comment US 25 and FI 15.	Move any references to timelines to an Annex.	Accept  Will move to annex
US 31	6.1.1 Contact Gateway	Title	Te	Title is unclear	Suggestion: Change to "Avenues of Communication", "Communication Channels," or like	Accept in principle  I prefer Avenues of Communications
US 32	6.1.1	Fax number	Te	Fax is an insecure mechanism of communication and is outdated. . See SC27N7227_WG3N967_Doc_27147 : Comment US 31.	Remove Fax number from this list.	Accept

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.

[All NBs<sup>1</sup>] comments on ISO/IEC 2nd WD 29147

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 33	6.1.1	Process Overview	Te	This looks like the first part of a process outline for Vulnerability Disclosure, but it stops with Vendor acknowledgement of receipt of the vulnerability report.	Move this to an appropriate section (section 6, above) and continue outlining the entire process through the Resolution Phase.	Accept
US 34	6.1.2	Anticipated Response Times and Actions	Te	<p>The only response times that are appropriate and in scope are for the Vendor's acknowledgement of receipt of the vulnerability report.</p> <p>Timelines vary between vendors and depending on the depth of the issue, number of versions/builds, etc. Some vendors have a set release schedule (such as MS or Oracle) while others do as required updates and releases (such as Symantec). But timelines are by the very nature of the issue going to vary. The OIS guidelines and the NIAC documents did not include fixed timescales in this area.</p> <p>Large vendors are often faced with significant code-base modifications, with numerous builds and regression testing, with several concurrent development versions in process.</p> <p>A single issue may impact a number of versions/platforms/etc thus multiplying the engineering and SQA time to ensure a reliable fix is released. As a result, in the event of a critical severity issue, the initial release may be just for the more heavily deployed product versions and legacy versions flow out as finalized. Or, some form of mitigation is released initially (e.g. a workaround, restriction or signature) as a temporary solution until a full solution can be determined</p>	<p>Replace this entire section and table with the following:</p> <p>"Vendors should acknowledge receipt of the vulnerability report from the Finder within 14 days."</p>	<p>Accept</p> <p>Update to reflect the sentence change.</p>

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.

[All NBs<sup>1</sup>] comments on ISO/IEC 2nd WD 29147

Date: 2009-05-07	Document: <b>SC27 N7799</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
				and adequately tested. See SC27N7227_WG3N967_Doc_27147 : Comment US 25 and FI 15.		
US 35	6.1	2. Expected turn around times for responses and action	Te	Numbers are probably only useful for the initial acknowledgement (e.g. "We will make every effort to complete an initial assessment and contact you within 3 business days."). Otherwise, vendor should set expectations, but numbers are unenforceable for every business.  Regression testing is often the longest part of the resolution phase, although understanding/reproducing the vulnerability can also take time.	Suggested language: "Vendors should explain/set expectations for communication, including initial acknowledgement of receipt of report and status updates.	Accept
US 36	6.1	3. Information that would be useful...	Te	Reference real-world examples in an appendix, similar to B1.  While more/good information is of course better, any information is better than none.	Include examples such as the following in an appendix:  <a href="https://forms.cert.org/VulReport/">https://forms.cert.org/VulReport/</a>  Rewrite this section from a Vendor perspective/scope. Rewrite section to encourage the incorporation of thorough information but also don't dissuade reporting due to lack of information.	Accept
US 37	6.1.2.	Para 5	Te	Identify additional standards relevant to identifying & managing risk in systems. Place in an Annex.	In an Annex, reference: 1) ISO/IEC 16085:2006 Systems and software engineering -- Life cycle processes -- Risk management 2) ISO/IEC 27005:2008 Information	Accept

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.

[All NBs<sup>1</sup>] comments on ISO/IEC 2nd WD 29147

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
					technology — Security techniques — Information security risk management	
US 38	6.1.3	Entire section	Te	This is out of scope for this document, as it gives direction to Finders who are not governed by this standard. See SC27N7227_WG3N967_Doc_27147 : Comment FI 5.	Move this section to an Annex with example vulnerability reports.	Accept
US 39	6.1.3	Entire section	Te	This was written from the perspective of the Finder, and is therefore out of scope.	Reword section in terms of useful information a vendor would want (vendor perspective). Provide examples in an annex.	Accept
US 40	6.2	Paras 1, 2	Te	This section goes out of scope in describing the Finder's responsibilities. Only the Vendor's actions are in scope of this standard. See SC27N7227_WG3N967_Doc_27147 : Comment FI 5.	Rewrite this section to reflect only Vendor actions.	Accept
US 41	6.2.2 Multi-vendor or issues where the discovered issue does not affect component owner (NIAC section 6)	Title	Ge	Title is unintelligible.	Strike this section.	Not accepted See JP 14
US 42	6.2.3, 6.2.4	Both	Te	These sections are redundant. "Component Owner" and	Condense this down to one section, and	Accept

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.

[All NBs<sup>1</sup>] comments on ISO/IEC 2nd WD 29147

Date: 2009-05-07	Document: <b>SC27 N7799</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

		sections		“Vendor” are synonymous. See SC27N7227_WG3N967_Doc_27147 : Comment US 11.	describe the infrastructure and procedures a Vendor must have to be able to securely exchange information with Finders and Coordinators.	
US 43	6.2.3	Para 1	Te	This section should be clarified to state that the acknowledgement merely acknowledges receipt of the notification from the finder, and provides an internal tracking number to the finder. With this clarification a period of 3-5 business days from receipt is appropriate	The receiving party once notified of the issue from a finder should issue a receipt to the finder, indicating only receipt of the notification, and assigning an internal tracking number. This acknowledgment should respond with a period as specified by the receiving party vulnerability disclosure policy. However, it is recommended that a response be provided within 3-5 days of notification of the issue	Accept
US 44	6.2.5		Te	Coordinators can provide various services, one of which is conflict resolution.	From a vendor perspective (scope), describe coordinators and their services.  Reference FIRST Vendor SIG <i>Guidelines for Vendor – Coordination Centers Relationship</i>  <a href="http://www.first.org/vendor-sig/vendor-coordinators-guidelines-public-v1.0.pdf">http://www.first.org/vendor-sig/vendor-coordinators-guidelines-public-v1.0.pdf</a>	Accept in principle  Will add section to identify coordinators and services provided
US 45	6.2.5		Te	Coordinators are out of scope, but this can be placed in an annex. A neutral coordinator does not function on behalf of Vendor or Finder but seeks to make a neutral judgement based on available information.	Place this section in an annex. Remove “They would function on behalf of the vendor...”  Remove “and nations will have at least	Accept  Move this section to the annex

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.

[All NBs<sup>1</sup>] comments on ISO/IEC 2nd WD 29147

Date: 2009-05-07	Document: <b>SC27 N7799</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
					one” Suggested list of example coordinators: CERT Coordination Center US-CERT JPCERT/CC CERT-FI AusCERT oCERT	Update to reflect the changes provided.
US 46	6.3	Entire Section	Te	As discussed in Limassol, Cyprus, Vendors should have a mechanism to disseminate vulnerability resolution information, but the exact formatting and content is out of scope of this document. See SC27N7227_WG3N967_Doc_27147 : Comment US 38.	Move this section to the Annex with sample Vendor vulnerability advisories/bulletins containing vulnerability resolution information.	Accept
US 47	6.3	Threats	Te	Threats are actions (by an attacker or some force). Fineto include a Threats section, but what is currently described is Impact.  Threat includes probability of attack, Impact is consequence of successful attack.	Reword Threats section, such as:  Threats  Provide information about known threats that relate to the vulnerability, for example the existence of exploit or proof-of-concept code, discussion or evidence of incident activity.  Add Impact section, such as:	Accept in principle Update to reflect the content provided

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.

[All NBs<sup>1</sup>] comments on ISO/IEC 2nd WD 29147

Date: 2009-05-07	Document: <b>SC27 N7799</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
					<p>Impact</p> <p>Describe potential/expected consequences of attacks against the vulnerability. Attacks can have multiple impacts (e.g., an attack against a buffer overflow vulnerability could cause a crash or execute code). Where possible, describe secondary impacts (e.g., a cross-site scripting vulnerability directly allows an attacker to inject content into a web page, however the secondary impact may be the exposure of cookies or other authentication credentials).</p> <p>Use existing ISO terms if applicable.</p>	
US 48	6.3.1 Dissemination Formatting	1	Te	Move this section to an appendix.	<p>Move to appendix</p> <p>Any party producing and distributing vulnerability information as an Advisory or any other format should consider the needs of the intended audience both in terms of content and format. Consumers of vulnerability information need to decide if and to what extent they are affected and how best to respond to a vulnerability. An Advisory should contain:</p> <p>relevant dates</p>	<p>Accept in principle</p> <p>Move current section to annex and update to reflect the changes during ad-hoc editing session</p>

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.

[All NBs<sup>1</sup>] comments on ISO/IEC 2nd WD 29147

Date: 2009-05-07	Document: <b>SC27 N7799</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

					<p>how to identify vulnerable software</p> <p>a high level description</p> <p>sufficient technical detail about the vulnerability, but not enough to empower attackers</p> <p>impact/consequence</p> <p>how to obtain and install/deploy updates</p> <p>workaround or mitigation information</p> <p>threat information</p> <p>Advisory producers should consider both human and machine-readable formats. A selection of Advisories and formats is provided in Appendix X.</p> <p>Appendix X</p> <p>CERT Advisory</p> <p>Cisco Advisory</p> <p>Microsoft Security Bulletin</p> <p>US SCAP, including</p> <p>CVE</p> <p>CVSS</p>	
--	--	--	--	--	---	--

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.

[All NBs<sup>1</sup>] comments on ISO/IEC 2nd WD 29147

Date: 2009-05-07	Document: <b>SC27 N7799</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
					CPE CAIF (.de) VulDef (.jp) VuXML	
US 49	6.3.1		Te	Section is hastily written, lists a set of existing formats without much guidance.	Discuss/note that various formats exist, suggest that vendors provide information in human-readable and machine-parseable formats, suggest vendors consider existing common formats in annex.  Put list of formats and brief description in annex	Accept in principle  Create a advisory annex and relocate this information to the annex.
US 50	A.2.1	Table	Te	Providing numbers of days is misleading.  Characteristics of the Risk Level are somewhat arbitrary. Availability of <b>exploit</b> (not source) code is certainly a factor, as is incident activity, but there are many other factors which are not adequately represented (out of scope) and many subjective factors. It is out of scope to address all the factors that could lead to a reasonable severity chart.  Discussion of significant risk factors is appropriate.	Remove chart entirely.	Accept  Chart to be removed

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.