

[FIRST¹] comments on ISO/IEC 4rd WD 29147

Date: 2009-MM-DD	Document: SC 27 N8126
------------------	------------------------------

1	2	(3)	4	5	(6)	(7)
FIRST ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
[FIRST] 1	Introduction	para 2	Te	Replace the first sentence with the following text to maintain consistency with the rest of the text.	A vulnerability is defined as a set of conditions that leads or may lead to an implicit or explicit failure of the confidentiality, integrity, or availability of an information system.	
[FIRST] 2	Introduction	para 5	Te	Remove the sentence “As defined by reference 15 in the bibliography, “The goals of responsible disclosure include:” and all seven bullets that follow it. Instead use the proposed text. Strictly speaking helping academia is not a goal. It is a fortunate consequence of the disclosure but not a goal.	<p>The goals of responsible disclosure include:</p> <ol style="list-style-type: none"> 1) Ensure that vulnerabilities can be identified and eliminated effectively and efficiently for all parties. 2) Minimize the risk to customers from vulnerabilities that could allow damage to their systems 3) Provide customers with sufficient information for them to assess the risk to their systems. 4) Minimise the amount of time and resources required to manage vulnerability information 5) Minimise the amount of antagonism that often exists between parties as a result of different assumptions and expectations, due to the lack of consistency and explicit disclosure process. 	

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.

[FIRST¹] comments on ISO/IEC 4rd WD 29147

Date: 2009-MM-DD	Document: SC 27 N8126
------------------	------------------------------

1	2	(3)	4	5	(6)	(7)
FIRST ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
[FIRST] 3	3 Terms and definitions	3.1	Te	The sentence “An advisory may be published by a vendor, finder, or coordinator.” Can imply that only one of them can publish an advisory while, in reality, any of them can and, occasionally, do.	Remove “a” from the sentence to read “An advisory may be published by vendor, finder, or coordinator”	
[FIRST] 4	3 Terms and definitions	3.3 finder	te	Use definition from NIAC document	Finders include individuals or organizations that find vulnerabilities. Subgroups include researchers, security companies, users, governments, and coordinators.	
[FIRST] 5 3	3 Terms and definitions	3.4 product	Te	Product does not have to be commercial. Also, according to the Scope services are also included in this IS.	Replace the existing text with this “Item or service developed, manufactured or refined be it commercial or not.”	
[FIRST] 6	3 Term and definitions	3.7	Te	Term “update” is overloaded and it not always clear are we talking about updated software of updating an advisory.	Use term “remedy” for software updates, fixes and configuration change. Make this change throughout the document.	
[FIRST] 7	4 Abbreviated terms	Title	Ed	remove ‘)’ from the title		
[FIRST] 8	4 Abbrevi		Te	The list of abbreviated terms is not consistent. IPA and JPCERT are present but not CERT/CC. We also feel that	Remove entries for IPA and	

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.

[FIRST¹] comments on ISO/IEC 4rd WD 29147

Date: 2009-MM-DD	Document: SC 27 N8126
------------------	------------------------------

1	2	(3)	4	5	(6)	(7)
FIRST ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
	ated terms			listing organization names is not required.	JPCERT	
[FIRST] 9	5 Responsible vuln disclosure	second para	Te	“vulnerability handling” can be viewed as insufficient broad definition	Use “vulnerability management” instead. Make change throughout the document.	
[FIRST] 10	5 Responsible vuln disclosure	second bullet	Te	The bullet contains subjective expressions	Replace with the following text “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 and effective remedy”	
[FIRST] 11	5 Responsible vuln disclosure	last para	Te	Current text implies that vendor cannot accept vulnerability report unless it has vulnerability policy. That is not correct.	Replace with the following text: “A vendor must create vulnerability management policy and it must be shared with vendor customer base. While optional, vendors are strongly encouraged to make this policy public. Having a vulnerability managing policy defined is not requirement for responsible vulnerability disclosure. However, the policy helps in setting right expectations.”	
[FIRST] 12	6 Life	first para	Te	It has to be noted that sub-phases in the life cycle are not	Replace the sentence with this “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.

[FIRST¹] comments on ISO/IEC 4rd WD 29147

Date: 2009-MM-DD	Document: SC 27 N8126
------------------	------------------------------

1	2	(3)	4	5	(6)	(7)
FIRST ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
	cycle			necessarily in chronological order.	following lifecycle aligns these common phases (sub-phases may not be in a chronological order)."	
[FIRST] 13	6 Life cycle	2 verification phase	Te	"reproduction" implies that vendor will always develop an exploit for a vulnerability which is not always the case	Replace word "reproduce" with "confirm"	
[FIRST] 14	6 Life cycle	3 resolution phase b)	Te	Replace "update" with "remedy" and remove the rest of the text as the remedy is already defined.	Produce remedy.	
[FIRST] 15	6 Life cycle	4 advisory phase a)	Te	A reference to extraordinary circumstances should be added	Add the following sentence "Under extraordinary circumstances a vendor can release an advisory even if a remedy is not available."	
[FIRST] 16	7 Vulnerability Handling policy	first para	Te	Remove the reference to IETF draft. Examples are given in Annex B so this one should be no exception.	Remove the second sentence from the paragraph.	
[FIRST] 17	7 Vulnerability Handling policy	bullet 1	Te	The number of co-ordinators can change and vendor may not even be aware of the existence of some of the co-ordinators. Vendors should give their contact information to co-ordinators but that is on the best effort basis.	Add sentence "Vendors will do their best effort to provide their contact information to the coordinators"	
[FIRST] 18	7 Vulnerability Handling policy	bullet 4	Te	The spirit of this bullet is good but it only protects finders and not vendors. Finders may be collecting information and provide it to its advantage against the vendor or give it to a competitor of the vendor. As long as this bullet provides only one way assurance it is not acceptable.	Remove the bullet 4	
[FIRST] 19	8.1 Simplifi	first sentence	Ed	Use affirmative voice.	Rewrite the sentence to read "The vulnerability handling policy should be	

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.

[FIRST¹] comments on ISO/IEC 4rd WD 29147

Date: 2009-MM-DD	Document: SC 27 N8126
------------------	------------------------------

1	2	(3)	4	5	(6)	(7)
FIRST ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
	ed Policy				simple and clear to enable easy reporting of product vulnerabilities to the vendor”	
[FIRST] 20	8.1 Simplified Policy		Te	Vendors should be encouraged to use intuitive place for this policy and other security-related information. Adoption of NIAC recommendation of /security page should be encouraged.	Add sentence “Vendors should consider intuitive placement of information related to product security management. Usage of /security web page for this purpose is recommended.”	
[FIRST] 21	8.3 Ack of receipt from finder	second para	Te	The last sentence talks about ‘pre-disclosure’. This term have specific, but different meaning, for different parties. To prevent confusion on what is exactly meant by pre-disclosure in this context we should use different term.	Rewrite the sentence as follows “When exchanging sensitive information in e-mail messages, they shall be protected by mutually agreed encryption mechanism like PGP.”	
[FIRST] 22	8.3 Ack of receipt from finder	Examples of exmail aliases	Ed	The example of e-mail aliases used for receiving vulnerability information feels a bit misplaced here.	Move this example into section 8.5 under e-mail bullet	
[FIRST] 23	8.4 Assign unique ID		Te	<p>CVEs are assigned in a sequential fashion and, as such, may reveal certain amount of information. CVEs should be protected in transit.</p> <p>It is also possible to encounter a situation that single CVE entry will be later split into multiple CVE entries during the subsequent review. Vendors and finds must be warned about that possibility to set the right expectations.</p> <p>Many vendors would also assign a case (tracking) number to the report. This will be done much sooner than</p>	<p>Add the following text “While every care is taken that CVE identifier is unique a situation may occur where an CVE candidate is split into a multiple CVE entries during the subsequent review. This is a rare situation but it can occur.</p> <p>CVE identifiers, by itself, reveal a certain amount of information and</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.

[FIRST¹] comments on ISO/IEC 4rd WD 29147

Date: 2009-MM-DD	Document: SC 27 N8126
------------------	------------------------------

1	2	(3)	4	5	(6)	(7)
FIRST ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
				assigning a CVE number. Distinction between these two IDs must be made.	they should be treated as any other sensitive information and not transmitted in cleartext. Vendors may also assign a case (tracking) number to the report. This can happen before CVE ID is assigned. Vendor tracking number is unique for that vendor and it does not replaces CVE identifier.”	
[FIRST] 24	8.7 Role of a Coordinator	whole section	Te	This section misrepresents the role of a coordinator. As the name suggest coordinator helps with coordination and is not an arbiter. In practice it is hard to imagine how a coordinator, with no jurisdiction, can perform arbitrage.	Remove completely section 8.7 and replace it with the following text “Coordinator can play multiple roles in vulnerability management process: <ul style="list-style-type: none"> • Act as trusted introducer between involved parties • Coordinate advisory public release date • Enabling communication between involved parties (vendors and finders) • Provide environment where experts from different organizations can work jointly on addressing the vulnerability Vendors and finders are encouraged to establish relationship with a	

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.

[FIRST¹] comments on ISO/IEC 4rd WD 29147

Date: 2009-MM-DD	Document: SC 27 N8126
------------------	------------------------------

1	2	(3)	4	5	(6)	(7)
FIRST ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
					coordinator (or more than one coordinator) before start working on a vulnerability. Which coordinator they choose to establish a relationship would depend on various factors as geographical proximity, language and acceptable operation model.”	
[FIRST] 25	8.7 Role of a Coordinator		Te	In addition to comment FIRST 24 add the following text at the end of the section.	“Implicitly, an assumption is that coordinators exchange some information among themselves and that certain level of cooperation within the group exists. Vendors and finders are encouraged to discuss this topic with their preferred coordinator. Document “ Guidelines for Vendor - Coordinators relationship ” (available at https://members.first.org/vendor-sig/vendor-coordinators-guidelines-public-v1.0.pdf) produced by FIRST Vendor SIG, can be used to set a basic level of expectations.”	
[FIRST] 26	9.0 Disseminating of vulnerability information		Te	To better help consumers of advisories to assess relative impact of different vulnerabilities to their systems vendors should consider using a vendor-neutral scoring system.	Add this sentence at the end of the paragraph “In order to help advisory consumers with assessing relative impact of different vulnerabilities, vendor should consider using a common vulnerability scoring system (CVSS).”	
[FIRST] 27	B.1	When to	Te	This text mixes vulnerability management with incident	Change the title to “When to contact	

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.

[FIRST¹] comments on ISO/IEC 4rd WD 29147

Date: 2009-MM-DD	Document: SC 27 N8126
------------------	------------------------------

1	2	(3)	4	5	(6)	(7)
FIRST ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
	Sample vulnerability disclosure	contact the security incident response team		management. They are not the same! In the text CSIRT is mentioned, these teams usually handle incidents and only rarely product vulnerabilities.	product vulnerability response team”	
[FIRST] 28	B.1 Sample vulnerability disclosure	When to contact the security incident response team, first para	Te	Remove the reference to CSIRT in the first sentence.	Use the following sentence “Contact the <company name> Product Vulnerability Response Team (PVRT).” By sending email to security-alert@<company domain name> in the following situations:”	
[FIRST] 29	B.1 Sample vulnerability disclosure	Responding to customer incidents	Te	This section talks about helping customers with computer incidents and is not about vulnerability handling. While it is true that some teams may have dual role (vulnerability and incident managing) that is not universally true. To make this example clear we should not mix these two roles.	Remove the section “Responding to customer incidents”	
[FIRST] 30	B.2 Identifying and managing risk in systems	Whole section	Te	This section does seem a bit out of place here and it could be moved to a separate annex. There are also other models that can be references.	Add references to CERT Resiliency Management Model http://www.cert.org/resiliency/rmm.html and Building Security in Maturity Model http://www.bsi-mm.com/	
[FIRST] 31	B.5 Samples of good and bad	whole section	Te	Referencing outside material is not optimal as it can change without notice, we removed or become unsuitable for the purpose. While using concrete organizations as bad examples is very tempting these organizations may object to that practice.	Remove the current text and produce generic examples without referencing concrete 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.

[FIRST¹] comments on ISO/IEC 4rd WD 29147

Date: 2009-MM-DD	Document: SC 27 N8126
------------------	------------------------------

1	2	(3)	4	5	(6)	(7)
FIRST ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
	disclosure					
[FIRST] 32	B.7 Coordinators recognized globally	Te	first sentence	The impression document gives right now is that there are only four global coordinators. That is not correct. CPNI from UK is an example of an organization that played coordination role and then scaled back but it may do it again. New coordinators may also appear. We must not give impression that this is a definitive list.	Replace the first sentence with the following text "The following, non-exhaustive, list of globally recognized coordinators is correct at the time this IS was last updated. Since then new coordinators may become active or an existing coordinators may scale back their capabilities."	
[FIRST] 33	Bibliography		Te	restore full bibliography from the previous WD	Use the bibliography from WD3	

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.