



ISO/IEC JTC 1/SC 27 **N8127**

ISO/IEC JTC 1/SC 27/WG 3 **N38127**

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 3rd WD 29147 (SC 27 N 7901)
Information technology – Security techniques – Responsible
vulnerability disclosure

SOURCE: 39th SC 27/WG 3 meeting

DATE: 2009-11-06

PROJECT: 1.27.65

STATUS: Output document of the editing session for 3rd WD 29147 (SC 27 N 7901) held during the 39th SC 27/WG 3 meeting Redmond, Washington, November 2 – 6, 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. Banon, M.C. Kang, K. Rannenber, WG-Conveners

MEDIUM: Server

NO. OF PAGES: 1 + 64

[All NBs¹] comments on ISO/IEC 3rd WD 29147

1	2	(3)	4	5	(6)	(7)
NB 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
BE 1			Ed	This document still contains several typos and confusing wordings	Make a quality review to have a removal of such events	Accept Will work towards fixing these. The editor asks that specific details to issues be indentified in the comments, such a general statement does not aid in the document editing process.
BE 2	Introduction	Par 1	Te	We think you cannot reduce vulnerabilities	Replace “reduce or eliminate vulnerabilities” by “eliminate vulnerabilities or reduce their impact”	Not Accepted. See JP 8 for replacement text for this paragraph.
BE 3	3.4		Te	Current definition is a bit vague.	“A vulnerability is a flaw in the design, development, implementation, operation of a system that can be exploited intentionally or deliberately to cause security incidents to occur	Not Accepted. A vulnerability may be exploited unintentionally as well.
BE 4	3.7		Te	Remediation is a more general term	Replace “update” with “remediation”	Not Accepted. The term "update" will remain in place for this draft. If a new term is proposed in the next round of comments, the editor asks that specific comments with proposed changes to sentences throughout the draft also be submitted.
BE 5	3.8		Ed	This is the same item as 3.2	remove	Accept will remove
BE 6	3.9		Te	“Responsible” is not related to “private” but means that the disclosure is done in agreement between different parties, as explained in other sections of this doc	Align with def in Introduction	Not Accepted. See JP 20.
BE 7	3.10		Ed	Same as 3.4	remove	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 NBs¹] comments on ISO/IEC 3rd WD 29147

1	2	(3)	4	5	(6)	(7)
NB 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
BE 8	3.13		Te	This does not define advisory	Use the NOTE as definition	Accepted. See JP 23 for replacement text.
BE 9	5	Par 2 1 st bullet	Ed		Timely and High quality	Accepted. See JP 25 for replacement text.
BE 10	5	Par 3	Te	A vulnerability management process does not begin each time with creating a disclosure policy	Replace with " Before responsible vulnerability disclosure between a finder and vendor can begin, the vendor first must ensure they have established and made publically available their vulnerability disclosure policy".	Accepted. See JP 23 for replacement text.
BE 11	6	Item 1	Te	The discovery phase should provide for the finder to receive status information	Add "Vendor motivates the confirmation or rejection of the vulnerability to the finder"	Not Accepted. Sentence does not belong in Section 6 Item 1, since the vendor cannot provide motivation for accepting or rejecting a potential vulnerability, since the vendor does not investigate the vulnerability until Phase 2 – Verification Phase.
BE 12	6	Item 1	Te	The discovery phase should provide for the finder to receive status information	Add "The vendor agrees with the finder if and how frequently status information is exchanged during the verification phase"	Not Accepted. The Vulnerability Handling Policy as determined by a particular vendor will cover the frequency of status updates.
BE 13	6	Item 2	Te	In the verification section it describes the process of the vendor attempting to identify the root cause of the vulnerability, and further investigating to attempt to find further instances of the same vulnerability, It should be noted that this process should include other vendor products (vendor whom vulnerability was reported to) which may share common operating platforms, or code	Further Investigation: Reword to include: Attempt to find other instances of the same type of vulnerability within the product, as well other vendor products which may share common operating	Not Accepted. Investigation of other vendor's products for the same or similar vulnerabilities is out of scope for this IS.

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 NBs¹] comments on ISO/IEC 3rd WD 29147

Date: 2009-11-02	Document: SC27 Nxxx
------------------	----------------------------

1	2	(3)	4	5	(6)	(7)
NB 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
				streams which may be reused internally within the organization. As alluded to, a single vulnerability report may cause a 1- many discovery of risks within the product which was reported, but as we know, a single vulnerability report may also cause a 1-many discovery of the same vulnerability across multiple products, within the same vendor, as well as across vendors.	platforms or code streams	
BE 14	6	Item 3b	Te	Remediation is a more general term	Replace "Produce update" with "Produce remediation"	Not Accepted. The term "update" is defined in section 3 and will be used throughout the IS.
BE 15	6	Item 4	Te	Informing customers is very important, but Wether an advisory is published can depend on several other criteria (e.g. customers may prohibit this)	Replace "... and the general public..." by "... and possibly the general public ..."	Accepted. Will update accordingly.
BE 16	6	Item 4	Te	A patch is only one possible action to remediate a vulnerability	"Once the vendor is satisfied that the remediation ..."	Accepted. Will update accordingly.
BE 17	6	Item 4	Te	Should the comment regarding extending further investigation to include other vendor products be incorporated, the advisory phase should add guidance regarding issuance of notification on a per product basis	Add "b. If multiple products are found to be affected, a public advisory is required per product"	Not Accepted. See BE13.
BE 18	7		TE	Guidance should include a statement regarding the development of the disclosure policy that it is not overly complicated in such a manner as to discourage disclosure because the established means for the finder to report to the vendor are too complex. i.e. keep it simple.	Add somewhere "disclosure policy should contain clearly stated responsibilities for the vendor and finder, provide an easy mechanism for the finder to report a vulnerability. The process should avoid complicated steps to avoid	Accepted. Text will be added to the end of the first paragraph as follows: "The vulnerability handling policy should avoid complicated steps to avoid discouraging the vulnerability reporting to the vendor."

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 NBs¹] comments on ISO/IEC 3rd WD 29147

1	2	(3)	4	5	(6)	(7)
NB 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

					discouraging the vulnerability reporting to the vendor.”	
BE 19	7.6	Line 1	Te	If a customer has to wait 14 days before he receives a receipt ack. I am afraid the vendor loses him	“within 2 days”	Not Accepted. See CA 16.
BE 20	Biblio		Gen	Website doesn't exist anymore	Remove [13]	Accepted. Will be removed
BE 21	Biblio		Gen	Standard documents should preferably not contain references to vendor specific documents	Remove [18]	Accepted. The editor will remove this reference unless any of the text from the body or annexes are found to have come from this source.
BE 22	All		gen	Regarding the responsibility, it is to note that 29100 standard should be taken into consideration		Accept will add the reference
CA 1	0		te	<p>The document does not state clearly what the problem is.</p> <p>Usually a standard tries to provide a solution to a problem, possibly stemming from the industry. The introduction says "This International Standard provides a guideline for vendors on receiving information about potential vulnerabilities in a uniform way. This document also provides guidance for vendors to distribute vulnerability resolution information". No background is provided as to why this is desirable.</p> <p>Although this is not mandatory information in an IS, it is a service to the reader.</p>	Add a context paragraph explaining what problem this IS is trying to solve.	<p>Accepted. The text "Vulnerability disclosure is the practice of reporting, coordinating, and publishing information about a</p> <p>vulnerability. Users, businesses, and governments have increased their reliance on networks, applications, and the Internet for core operations and critical infrastructure. Vulnerabilities in technology vital to operations</p> <p>represent an increased risk. The key stakeholders in this process; finders, vendor, sub-component owner and coordinators have the same objective:</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 NBs¹] comments on ISO/IEC 3rd WD 29147

1	2	(3)	4	5	(6)	(7)
NB 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

						<p>reduce or eliminate vulnerabilities to ensure continued delivery of critical services and timely secure flow of information. " will be replaced with "A vulnerability is a weakness in a system which, if exploited, allows the exploiter to violate the security policy for that system.</p> <p>As defined by reference X in the bibliography, "Vulnerabilities can be caused by software and hardware design flaws,</p> <p>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> <p>Users, including businesses and governments, rely heavily on hardware and software components used in operating systems, applications,</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 NBs¹] comments on ISO/IEC 3rd WD 29147

Date: 2009-11-02	Document: SC27 Nxxx
------------------	----------------------------

1	2	(3)	4	5	(6)	(7)
NB 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

						networks, and critical national infrastructure. Vulnerabilities in these components increase risk to users. Vulnerability disclosure is the practice of reporting, coordinating, and publishing information about a vulnerability and its resolution. "
CA 2	0, 3 and 5			RVD is not clearly explained. Introduction says "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". Does "responsible" mean "timely"? The definition for RVD says: "private advance disclosure of a vulnerability to a Vendor or coordinator, where Vendor is allowed time to produce a fix prior to public disclosure". So it seems "responsible" means the Finder gives the Vendor enough time to fix the problem, but still will eventually go public so that Finder gets the recognition for the find This seems like the core concept in this IS. If that is so, then it should be spelled out in introduction and in clause 5.	Clearly state this core concept in introduction and in clause 5.	Not Accepted. If Canada could please provide specific suggested text for the next draft, it will be reconsidered.
CA 3	2	Normative references	Te	Add references to the normative listing	Add the following: http://www.cert.org/kb/vul_disclosure.html http://cve.mitre.org/about/terminology.html http://secunia.com/advisories/about/ http://osvdb.org/about	Not Accepted. These are not normative references, see the directive. They belong in the bibliography, as some of them already appear.
CA 4	3.8		TE	Definition previously defined in 3.2	Remove 3.8	Accepted. In order to list the terms in alphabetical order, the term 3.8 should

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 NBs¹] comments on ISO/IEC 3rd WD 29147

1	2	(3)	4	5	(6)	(7)
NB 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
						remain and 3.2 should be deleted. See JP 11.
CA 5	3.9		TE	Section labelled as responsible vulnerability disclosure, but subtext describes a mutually agreeable private agreement on the terms for vulnerability reporting, validation, and remediation before public notifications are made. Perhaps a more descriptive heading is appropriate.	Perhaps "Confidential Assessment Period" is more descriptive.	Not Accepted. Term "Confidential Assessment Period" is never used in the draft, so the term does not need to be defined. See also JP 20 and US 13.
CA 6	3.10		TE	Definition previously defined in 3.4	Remove 3.10	Accepted. In order to list the terms in alphabetical order, the term 3.10 should remain and 3.4 should be deleted. See JP 11.
CA 7	5	3	TE	Responsible vulnerability disclosure does not begin with creating the disclosure policy, a disclosure policy is required as a facility for a finder and vendor to mutually agree and communicate the details of the vulnerability.	Change first sentence to " Before responsible vulnerability disclosure between a finder and vendor can begin, the vendor first must ensure they have established and made publically available their vulnerability disclosure policy".	Accepted. The following text will replace the first sentence of section 5 paragraph 1: "A vendor should develop and publish their vulnerability disclosure process."
CA 8	6	2	TE	In the verification section it describes the process of the vendor attempting to identify the root cause of the vulnerability, and further investigating to attempt to find further instances of the same vulnerability, It should it be noted that this process should include other vendor products (vendor whom vulnerability was reported to) which may share common operating platforms, or code streams which may be reused internally within the organization. As alluded to, a single vulnerability report may cause a 1- many discovery of risks within the product which was	Further Investigation: Reword to include: Attempt to find other instances of the same type of vulnerability within the product, as well other vendor products which may share common operating platforms or code streams.	Not Accepted. Investigation of other vendor's products for the same or similar vulnerabilities is out of scope for this IS.

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 NBs¹] comments on ISO/IEC 3rd WD 29147

Date: 2009-11-02	Document: SC27 Nxxx
------------------	----------------------------

1	2	(3)	4	5	(6)	(7)
NB 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
				reported, but as we know, a single vulnerability report may also cause a 1-many discovery of the same vulnerability across multiple products, within the same vendor, as well as across vendors.		
CA 9	6	4	TE	Should the comment regarding extending further investigation to include other vendor products be incorporated, the advisory phase should add guidance regarding issuance of notification on a per product basis	<p>a. Update Release: Once the vendor is satisfied that the patch is effective and not harmful to most customer software environments, it notifies customers and the general public via an advisory.</p> <p>b. If multiple products are found to be affected, a public advisory is required per product.</p>	Not Accepted. See BE13.
CA 10	6	4	TE	<p>Sentence "Once the vendor is satisfied that the patch is effective and not harmful to most customer software environments" – makes it sound like the only solution to a vulnerability is to issue a patch, this is something that the finder and vendor must agree upon. Consider changing</p>	<p>Maybe: "Once the vendor is satisfied that the vulnerability remediation is effective and not harmful to most customer software environments..."</p>	Accepted. Text will be replaced with "Once the vendor is satisfied that the update is effective, it notifies customers and possibly the general public via an advisory."
CA 11	7		TE	Guidance should include a statement regarding the development of the disclosure policy that it not be overly complicated in such a manner as to discourage disclosure because the established means for the finder to report to the vendor are too complex. i.e. keep it simple.	Add somewhere "disclosure policy should contain clearly stated responsibilities for the vendor and finder, and provide an easy mechanism for the finder to report a vulnerability, and not contain a process that over complicates the vulnerability disclosure process so as to discourage vulnerability reporting to the vendor.	Accepted. See BE 18.

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 NBs¹] comments on ISO/IEC 3rd WD 29147

Date: 2009-11-02	Document: SC27 Nxxx
------------------	----------------------------

1	2	(3)	4	5	(6)	(7)
NB 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
CA 12	7.7			Subclause 7.7 is about "conflict arbitration". It is not clear what conflict could possibly arise from applying this standard and why. You mention two cases that seem benign. Why should these be considered conflicts and why should they need arbitration?	Explain the concept, possibly relating to the core concept referred to in CA 2.	Not Accepted. See US 33.
CA 13	7.3	Acknowledgement of receipt from finder	Ed	In some situations organizations have turned to out sourcing companies to provide helpdesk frontline support. A reference should be made to this including some guidelines.	Add the following sentence: In situations when a 3 rd party is used to provide helpdesk or frontline contact to customers and end users; it is important to educate them on the disclosure policy and process. Especially aspects of the anticipated response times which could lead to a situation where a researcher publishes a vulnerability believing the company was not willing to follow the stated policy.	Not Accepted. Coverage of staffing or outsourcing for vendors is out of scope for this IS.
CA 14	7.4	Obtaining a CVE Number	Ed	Perhaps, indicate that vulns can be reported through Secunia, OSVDB, etc as well. I more often route vulns through Secunia given the delays in the CVE Mitre queue. For bigger issues Cert has been responsive but can be buried as well, and is often afraid to drive the vendor. Nonetheless, the draft could mention making use of disclosing vulns through Cert to ensure that government entities more quickly learn of the need to patch. https://forms.cert.org/VulReport/	Include CVE contact methodology.	Not Accepted. See US 29.
CA 15	7.4	Obtaining a CVE Number	Te	Identify the need to obtain a CVE number and use this as the subject for communication.	Add the following sentence: One of the two parties should request a CVE as soon as possible in the disclosure process, and attach that number to all future correspondance. This can help cut down on many problems in subsequent contact, cross-vendor disclosure, etc.	Accepted. The following text will replace the paragraph under section 7.4, as follows: "A unique identifier should be assigned to the vulnerability as soon as possible in the disclosure process. This can be done by the vendor, finder, coordinator, or all parties

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 NBs¹] comments on ISO/IEC 3rd WD 29147

1	2	(3)	4	5	(6)	(7)
NB 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
						involved in the responsible disclosure process. Once the unique identifier is assigned, it should be attached to all future correspondence. This can help cut down on many problems in subsequent contact, cross-vendor disclosure, etc. Common Vulnerabilities and Exposures (CVE) identifiers could be used for this purpose."
CA 16	7.6	Anticipated Response Times and Actions	Ed	Current response time is too long especially for higher risk vulnerabilities.	Change to 7 days maximum	Accepted. The following text will replace sentences 2 and 3 in paragraph 1: "The vendor should respond to a vulnerability report as soon as possible and as specified in the vendor's vulnerability disclosure policy. However, it is recommended that an acknowledgement of receipt of a vulnerability report be provided to a finder within 7 calendar days of receipt."
CA 17	8.2			Subclause 8.2 says "Finder releases vulnerability information before agreed date". It is the first time the concept of agreed date comes up. Again, this is part of the core concept of this IS which should be developed in clause 5.	See CA 2.	Not Accepted. See CA 2. If Canada would like to propose specific text for the next iteration, we will reconsider it.
CA 18	8.3	Web Site Considerations	Te	Need to add a section that covers off considerations for cloud vendors.	Add a new section 8.4 Cloud/SaaS Considerations with the following content: Cloud and SaaS providers represent a unique environment that includes increased	Not Accepted. See JP 17 for specific additions to the draft to cover online services, which will also encompass Cloud/SaaS.

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 NBs¹] comments on ISO/IEC 3rd WD 29147

Date: 2009-11-02	Document: SC27 Nxxx
------------------	----------------------------

1	2	(3)	4	5	(6)	(7)
NB 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

					<p>responsibility for proper disclosure handling.</p> <p>The infrastructure and application layers are both in scope in cloud/SaaS environments and thus require that providers maintain very current patch state as well as properly secured applications. Flaws inherent at either layer have the propensity to affect numerous enterprise-grade customers with the possibility of a vast number of consumers at risk.</p> <p>It is therefore recommended that cloud/SaaS providers:</p> <ol style="list-style-type: none"> 1) Dedicate a specific team (CERT) to address reported security issues 2) Clear contact methodology, including email addresses, phone numbers, and IRC/IM/social outlets on a dedicated web page should exist for this CERT 3) Transparency and regular communication during incidents is recommended via the use of a CERT blog or wiki 4) The above mentioned security and CERT page should be menu or footer linked from all root pages on the provider's primary website so as to be easily noted by reporting parties. 	
CA 19	8.3	Web Site Consideration	Ed	State date of fix	The fix date should be clearly identified as well as the version number.	Accepted. See US 43 for replacement

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 NBs¹] comments on ISO/IEC 3rd WD 29147

Date: 2009-11-02	Document: SC27 Nxxx
------------------	----------------------------

1	2	(3)	4	5	(6)	(7)
NB 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

		s				text.
CA 20	0			Incentive for Finder. The introduction makes it clear why a Vendor would want to adopt the processes in this IS. The incentive for the Finder is less evident. Why would a Finder delay public disclosure of a vulnerability, if the process doesn't guarantee public recognition of the find? Again, this ties in with CA 2.	See CA 2	Not Accepted. The Finder's actions are out of scope for this standard.
CA 21	Appendix	A.1	Te	Include the operating system with the information provided to the vendors.	Add operating system to include list	Accepted. "Operating system" will be included in bulleted list.
CA 22	Appendix	A	Ge	Add samples of a good vs bad disclosure	AppRiver servers as a recent example of excellent disclosure handling: http://holisticinfosec.blogspot.com/2009/08/a-prriver-saas-security-provider-sets.html Ameriprise/American Express as a example of disclosure handling gone wrong: http://holisticinfosec.blogspot.com/2009/08/a-prriver-saas-security-provider-sets.html http://holisticinfosec.blogspot.com/2008/12/online-finance-flaw-american-express.html	Accepted. The following examples provided in SC27 N6880 will be added to Annex A.3 Advisory Examples. The document above can be found at http://www.ipa.go.jp/security/ciadr/vuln_announce_manual_en.pdf .
CA 23	Appendix	A.2	Te	The CVE format does not appear to be correct	CVE uses YYYY-#### where 'y' denotes the year of disclosure	Accepted. The format will be changed to CVE-YYYY-####.
CA 24	17		GE	Probably shouldn't put vendor specific links to documentation in a standards document.		Accepted if the editor understands this comment as referring to the bibliography. See BE 12.
FI1	7.4 and 8	7: Whole paragraph	ed	CVE numbers are first mentioned in Section 7.4, but not spelled out until in Section 8.	Cut "(Common Vulnerabilities and Exposures)" out from section 8 and	Accepted. See CA 15 for replacement text.

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 NBs¹] comments on ISO/IEC 3rd WD 29147

1	2	(3)	4	5	(6)	(7)
NB 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
		8: First paragraph			paste it after the first occurrence of CVE in the text of section 7.4	
IE 01.	3.8		ED	Definition is a duplicate of 3.2	Remove 3.8	Not Accepted see CA 4.
IE 02.	3.10		ED	Definition previously defined in 3.4	Remove 3.10	Not Accepted see CA 6.
IE 03.	6	4	TE	This item should take into account the scenario where more than one product is impacted by the vulnerability and by a patch.	Add clarification that if multiple products are impacted, an advisory should be issued per product.	Not Accepted. Vendors will make the business decision about whether to issue an advisory and whether to issue multiple advisories if more than one of their products are affected.
IE 04.	6	4	TE	“Once the vendor is satisfied that the patch is effective and not harmful to most customer software environments” – Not all vulnerabilities will be resolved with a patch. Consider expanding the resolutions.	Suggested reword: “Once the vendor is satisfied that the vulnerability resolution is effective and not harmful to most customer software environments...”	Accepted. See CA10 for replacement text.
IE 05.	7		TE	Suggest that a statement be added regarding the development of the disclosure policy and that it should not be complicated procedure. Otherwise the policy may discourage finders from disclosing vulnerabilities.	Suggested Text: “The disclosure policy should provide an easy procedure for a finder to report a vulnerability.	Accepted. See BE 18 for replacement text.
JP 1	Introduction	1 st	Ge	We should begin the introduction with description about “vulnerability” itself and then move to “vulnerability	Rewrite the 1 st paragraph.	Not Accepted. See JP 4.

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 NBs¹] comments on ISO/IEC 3rd WD 29147

Date: 2009-11-02	Document: SC27 Nxxx
------------------	----------------------------

1	2	(3)	4	5	(6)	(7)
NB 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

		paragraph		disclosure”. The background section (1.1) of the internet draft on RVD process (http://tools.ietf.org/draft/draft-christey-wysopal-vuln-disclosure/draft-christey-wysopal-vuln-disclosure-00.txt) is a good alternative, saying: “Vulnerabilities are an inherent and unfortunate part of the design and development process. Vulnerability detection may occur during any phase of the product lifecycle, to include design, development, testing, implementation or operation. Ideally, vulnerabilities are largely prevented through a design process that considers security. However, due to a variety of reasons, many vulnerabilities are detected after a product is implemented in an operational environment and supporting customer objectives.”	Please refer to the proposed change of JP4.	
JP 2	Introduction	1 st paragraph	Ge	The second sentence (“Users, businesses, and governments have increased ...”) is not only too general observation to place here but also mismatching with the adjacent sentences.	Delete the 2 nd sentence.	Accepted. Entire first paragraph will be replaced per CA 1.
JP 3	Introduction	1 st paragraph	Te	Although it depends on what “technology” means, we don’t believe any vulnerabilities could be found in technology itself, while they may exist in design, implementation or installation of hardware and software.	Delete the 3 rd sentence.	Accepted. Entire first paragraph will be replaced per CA 1.
JP 4	Introduction	1 st paragraph	Ge	It is nonsense to mention the key stakeholders here (in the 4 th sentence), unless the reason why this IS has been	Change the 1 st paragraph as follows:	Not Accepted. See US 5. The last sentence of this paragraph will 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.

[All NBs¹] comments on ISO/IEC 3rd WD 29147

Date: 2009-11-02	Document: SC27 Nxxx
------------------	----------------------------

1	2	(3)	4	5	(6)	(7)
NB 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

				developed for vendors is explained, because the scope of this standard is only vendors.	“Vulnerability is weakness of products or systems that can be exploited by a threat. Although it is ideal for all vulnerabilities to be weeded out during implementation phases including design, development and testing, in reality some of them are found after the product or system is shipped out and put into operation, which possibly not only expose its users to security risks but also make the whole network or service unstable. What is crucial in order to reduce or eliminate such risks is vulnerability disclosure which informs all the need-to-know persons of the vulnerability so that they can take necessary actions timely.”	removed, which addresses the justification given by JP for this comment.
JP 5	Introduction		Ge	<p>With salesperson’s mind, we should explicitly describe why RVD is recommended to be adopted and/or what bad consequences non-responsible VD could cause.</p> <p>The following description in the paper “Efficiency of Vulnerability Disclosure Mechanisms to Disseminate Vulnerability Knowledge” by Hasan Cavusoglu et al in IEEE Tr. on SE Vol. 33 No. 3 (March, 2007) is a good example, saying:</p>	<p>Add the following description between the 1st sentence and the 2nd sentence.</p> <p>“Vulnerabilities are disclosed in various manners. Some of them might be sold in black or white markets, and others might be publicized with full details intentionally or unintentionally. The sequence and timing of announcement of the vulnerability, that is, how vulnerability knowledge is managed, affects the total cost of the</p>	Not Accepted. Information about other forms of vulnerability disclosure is out of scope for the Introduction. If Japan would please offer specific suggestions for text that provides contextual information about other forms of disclosure for another section of the draft, we can consider it for the next iteration.

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 NBs¹] comments on ISO/IEC 3rd WD 29147

1	2	(3)	4	5	(6)	(7)
NB 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

				<p>“The sequence and timing of announcement of the vulnerability, that is, how vulnerability knowledge is managed, affects the total cost of the vulnerability to the society. “</p> <p>As for some benefits of RVD described in clause 5, please refer to the JP25 comment.</p>	<p>vulnerability to the society, not to mention the vendor’s cost for responding the vulnerability.”</p>	
JP 6	Introduction	2 nd paragraph	Te	<p>The definition of RVD is too psychology (or internal process) oriented (e.g. “work together diligently”). We should define RVD based on the tangible interfaces.</p> <p>The description in the paper “Efficiency of Vulnerability Disclosure Mechanisms to Disseminate Vulnerability Knowledge” by Hasan Cavusoglu et al in IEEE Tr. on SE Vol. 33 No. 3 (March, 2007) seems to be more appropriate, which is shown in the proposed change column.</p>	<p>Replace the 2nd paragraph with the following description:</p> <p>The steps followed to handle dissemination of the knowledge of software vulnerabilities after a benign user identifies them are collectively known as the vulnerability disclosure process. Responsible vulnerability disclosure addresses how a vulnerability identifier should disclose vulnerability information to appropriate people, at appropriate times, and through appropriate channels in order to minimize the social loss associated with vulnerabilities.</p>	Accepted. See CA 1.
JP 7	Introduction	3 rd paragraph	Te	It is not only important but also unnecessary for vendors to receive information “in a uniform way.”	Remove “in a uniform way” or replace it with “in an appropriate way.”	Accepted. The text “in a uniform way” will be removed.
JP 8	Introduction	3 rd paragraph	Ge	It should be mentioned why the way for vendors to receive information about potential vulnerabilities and to distribute vulnerability resolution information is related to responsible vulnerability disclosure.	<p>Add brief explanation bridging the two.</p> <p>Or replace the 3rd paragraph with the following statement:</p>	Accepted. See CA 1 for the first part of the Introduction text. After that text, the following text will replace the rest of the introduction: “Through responsible

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 NBs¹] comments on ISO/IEC 3rd WD 29147

1	2	(3)	4	5	(6)	(7)
NB 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
					<p>“This International Standard provides a guideline for vendors to respond to report about potential vulnerabilities in the manner which encourages their finders to execute responsible vulnerability disclosure. This document also provides a guideline for vendors to distribute vulnerability resolution information in the manner which promotes customer’s needed responses and minimizes the social risk associated with vulnerabilities.”</p>	<p>vulnerability disclosure, vendors can work together diligently with vulnerability finders and produce a timely resolution to reduce users’ risks associated with the vulnerability in accordance with their business strategy.</p> <p>This International Standard provides a guideline for vendors on receiving information about potential vulnerabilities and distributing vulnerability resolution information toward accomplishing responsible vulnerability disclosure.</p> <p>"</p>
JP 9	1	1 st paragraph	Te	“All interested parties” are not an appropriate wording, since it may include attackers. We should exclude adversaries if possible.	Replace “interested” with “need-to-know.”	Accepted. The text "to be used by all interested parties" will be deleted.
JP 10	1	4 th paragraph	Te	We should mention what target vendors should pursue on RVD.	<p>Add some description about the target of RVD. The goal section (1.4) of the internet draft on RVD process (http://tools.ietf.org/draft/draft-christey-wysopal-vuln-disclosure/draft-christey-wysopal-vuln-disclosure-00.txt) is a good example, saying:</p> <p>“The goals of responsible disclosure</p>	<p>Accept. Will add the text after the first paragraph as a quote, as follows: "As defined by reference X in the bibliography, “The goals of responsible disclosure include:</p> <p>1) Ensure that vulnerabilities can be identified and eliminated effectively and efficiently for all parties.</p> <p>2) Minimize the risk to customers from</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 NBs¹] comments on ISO/IEC 3rd WD 29147

Date: 2009-11-02	Document: SC27 Nxxx
------------------	----------------------------

1	2	(3)	4	5	(6)	(7)
NB 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

					<p>include:</p> <ul 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 evaluate the level of security in vendors' products. 4) Provide the security community with the information necessary to develop tools and methods for identifying, managing, and reducing the risks of vulnerabilities in information technology. 5) Minimize the amount of time and resources required to manage vulnerability information. 6) Facilitate long-term research and development of techniques, products, and processes for avoiding or mitigating vulnerabilities. 7) Minimize the amount of antagonism that often exists between parties as a result 	<p>vulnerabilities that could allow damage to their systems.</p> <ul style="list-style-type: none"> 3) Provide customers with sufficient information for them to evaluate the level of security in vendors' products. 4) Provide the security community with the information necessary to develop tools and methods for identifying, managing, and reducing the risks of vulnerabilities in information technology. 5) Minimize the amount of time and resources required to manage vulnerability information. 6) Facilitate long-term research and development of techniques, products, and processes for avoiding or mitigating vulnerabilities. 7) Minimize the amount of antagonism that often exists between parties as a result of different assumptions and expectations, due to the lack of consistent and explicit disclosure practices. “
--	--	--	--	--	---	--

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 NBs¹] comments on ISO/IEC 3rd WD 29147

Date: 2009-11-02	Document: SC27 Nxxx
------------------	----------------------------

1	2	(3)	4	5	(6)	(7)
NB 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

					of different assumptions and expectations, due to the lack of consistent and explicit disclosure practices. “	
JP 11	3		Ed	The randomly ordered terms and definitions are very inconvenient to browse.	Please sort them out in alphabetical order.	Accepted. Terms will be sorted alphabetically.
JP 12	3.1		Te	Generally speaking, it is difficult for users to identify a vulnerability. They just find or discover anomaly which suggests possible vulnerabilities.	The definition of finder should be: “a person or an organization who discovered the possible vulnerability.”	Accepted. The definition text will be “person or organization who discovers a potential vulnerability”
JP 13	3.2		Ed	It is duplication of 3.8.	The clause 3.2 should be deleted.	Accepted. Clause 3.2 will be deleted.
JP 14	3.3		Te	<p>The service of a coordinator as a proxy is not its main role but only episodic.</p> <p>We can see a detail description in Appendix B of the NIAC’s report on “Vulnerability Disclosure Framework” (http://www.dhs.gov/xlibrary/assets/vdwgreport.pdf) saying:</p> <p>“Coordinators assist in the disclosure and response to new vulnerabilities. Established in 1988, the CERT Coordination Center (CERT/CC) in Pittsburgh, PA was the first organization to perform this function. In the past fifteen years, the CERT/CC has helped to establish other teams that serve as coordinators for various constituencies, including national teams.”</p>	<p>Replace it with the definition in of the internet draft on RVD process (http://tools.ietf.org/draft/draft-christey-wysopal-vuln-disclosure/draft-christey-wysopal-vuln-disclosure-00.txt) saying:</p> <p>“A Coordinator is an individual or organization who works with the Reporter and the Vendor to analyze and address the vulnerability. Coordinators are often well-known third parties. Coordinators may have resources, credibility, or working relationships that exceed those of the reporter or vendors. Coordinators may serve as proxies for reporters, help to verify the reporter's claims, resolve conflicts, and work with all parties to resolve the vulnerability in a satisfactory manner.</p>	Accepted. See US 9

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 NBs¹] comments on ISO/IEC 3rd WD 29147

Date: 2009-11-02	Document: SC27 Nxxx
------------------	----------------------------

1	2	(3)	4	5	(6)	(7)
NB 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
					Note: while Coordinators can facilitate the responsible disclosure process for a vulnerability, the use of Coordinators by other parties is not a requirement.”	
JP 15	3.7		Te	“Update” doesn’t seem to be the right word, since it conveys unnecessary connotation.	Change the term. A possible alternative term is “solution” or “resolution.”	Not Accepted. The term "update" will remain in place for this draft, since it is used in a few different contexts elsewhere. See Section 6 Lifecycle of a Vulnerability. If a new term is proposed in the next round of comments, the editor asks that specific comments with proposed changes to sentences throughout the draft also be submitted.
JP 16	3.8		Ed	A conjunction “or” is missing before “web service.”	Insert “or” just before “web service.”	Accepted. Will update accordingly.
JP 17	3.8		Te	If vulnerabilities of web service are included in the scope of this IS, we have to give special consideration for describing the 8 th clause (dissemination), which might make this IS complicated. For example, update is meaningless in most cases of web service vulnerabilities. We believe we had better exclude web service out of this IS scope.	Delete “web service.” Or add some description specific to vulnerabilities of web services.	"Accepted. The following text will be added to include more specific information about vulnerability handling as it applies to online services, as follows: 1. In the section marked Lifecycle of a Vulnerability, under the Resolution Phase, the list item will be added as follows: "d. Production system update:

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 NBs¹] comments on ISO/IEC 3rd WD 29147

Date: 2009-11-02	Document: SC27 Nxxx
------------------	----------------------------

1	2	(3)	4	5	(6)	(7)
NB 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

						<p>for online services vulnerabilities, implement the resolution in the production system".</p> <p>2. In the Verification Phase, the list item will be added as follows:</p> <p>"e. Exploit investigation: attempt to determine whether the vulnerability has been exploited so far and how widespread the exploitation is".</p> <p>3. In the section called Vulnerability Handling Policy, the following section will be added:</p> <p>"4. Sanction against legal action Vendors should declare that they will not take any legal actions against a finder who follows responsible vulnerability disclosure</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 NBs¹] comments on ISO/IEC 3rd WD 29147

1	2	(3)	4	5	(6)	(7)
NB 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

						<p>according to the vendor's published vulnerability handling policy".</p> <p>4. In Annex A.1, the following bulleted list items will be added as follows:</p> <ul style="list-style-type: none"> “- For online services vulnerabilities, time and date of discovery - For online services vulnerabilities, URL - For online service vulnerabilities, browser information including type and version - For online service vulnerabilities, input required to reproduce 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 NBs¹] comments on ISO/IEC 3rd WD 29147

1	2	(3)	4	5	(6)	(7)
NB 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

						<p>vulnerability".</p> <p>5. Further, the editor would like to request example online services vulnerability advisories in Annex A.3 Advisory Examples to be submitted for inclusion by national bodies.</p> <p>6. Under A.2 under the Solution section, change the text as follows: "For product vulnerabilities, provide information on how to install the fixed product, update and apply a security patch."</p> <p>7. In Annex A.4, the following text will be added to the end of the first paragraph:</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 NBs¹] comments on ISO/IEC 3rd WD 29147

Date: 2009-11-02	Document: SC27 Nxxx
------------------	----------------------------

1	2	(3)	4	5	(6)	(7)
NB 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
						"The NIAC Framework was written for product vulnerabilities in particular, and does not cover cases of online services vulnerabilities."
JP 18	3.8		Te	The word "application" is ambiguous. If it means "application software", there seems to be no need to mention it after "software." (Also related to 3.6.)	Delete "application."	Accepted. Definition text will be replaced by "person, organization, or company that developed the software, hardware, or online service, or is responsible for maintaining it"
JP 19	3.8		Te	We should keep in mind that standards, including ISs, and hardware may also possibly have vulnerabilities.	Add "standard" and "hardware" among software and so on. Or replace it with the definition in of the internet draft on RVD process (http://tools.ietf.org/draft/draft-christey-wysopal-vuln-disclosure/draft-christey-wysopal-vuln-disclosure-00.txt) saying: "A Vendor is an individual or organization who provides, develops, or maintains software, hardware, or services, possibly for free."	Accepted. See JP 18.

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 NBs¹] comments on ISO/IEC 3rd WD 29147

Date: 2009-11-02	Document: SC27 Nxxx
------------------	----------------------------

1	2	(3)	4	5	(6)	(7)
NB 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
JP 20	3.9		Te	<p>Since the theme of this IS is RVD, we don't need the definition of RVD itself.</p> <p>On top of that, the definition is not appropriate, because it is finder oriented while finders are out of scope of this IS.</p>	<p>Delete this entry.</p> <p>Or, change the entry into "vulnerability disclosure" with its proper definition.</p>	Accepted. This term will be deleted.
JP 21	3.11		Te	The definition is not true. Incident is not necessary related with an attack.	<p>Adopt the following definition in ISO/IEC 27000 (2.21):</p> <p>"information security incident: single or a series of unwanted or unexpected information security events (2.20) that have a significant probability of compromising business operations and threatening information security (2.19)"</p>	Not Accepted. The term will be deleted, since it is not used elsewhere in the draft. If the term is needed later, we will reintroduce it, using the ISO/IEC definition.
JP 22	3.12		Te	Vulnerability information service is not an organization but a service.	<p>Rewrite the definition as follows:</p> <p>"service to aggregate and distribute vulnerability information either on subscription base or for free."</p>	Not Accepted. See US 16.
JP 23	3.13		Te	The description is just observation, and can't be a term definition.	Rewrite the definition or remove the term entry.	<p>Accepted. The definiton and NOTE section will be replaced by the text "(noun) information about a vulnerability</p> <p>NOTE A vulnerability advisory may include advice on how to deal with the vulnerability. An advisory typically contains a description of the vulnerability including a list of vulnerable</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 NBs¹] comments on ISO/IEC 3rd WD 29147

1	2	(3)	4	5	(6)	(7)
NB 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

						software, potential impact, resolution and mitigation information, and references. An advisory may be published by a vendor, finder, or coordinator."
JP 24	5	1 st paragraph	Ge Te	Concerning the implication of RVD, please refer to JP6.	Same as proposed change of JP6.	Accepted. See CA 1.
JP 25	5	2 nd paragraph	Te Ed	In this context the benefit of RVD should be described more from the viewpoint of vendors than from a neutral viewpoint. Refer to JP5.	The following is a possible alternative description: "It can lift up the customer's trust to the vendor and its product through information disclosure which can minimize the risks of the customer."	Accepted. Paragraph 2 text will be replaced with "The benefits of responsible disclosure and vulnerability handling include the following: -It can increase the customer's trust in the vendor and its product through information disclosure, which can minimize the risks of the customer. - 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 – quality remedy that will have high uptake among the affected systems - It can also contribute to improving the engineering quality of software products, by supporting the academic and research communities'

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 NBs¹] comments on ISO/IEC 3rd WD 29147

1	2	(3)	4	5	(6)	(7)
NB 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
						ongoing efforts to identify insecure development methods and practices, including insecure design and coding that result in security vulnerabilities, the conditions under which they occur, and methods to avoid them."
JP 26	5	3 rd paragraph	Te	Since process for RVD is out of scope of this IS, we should not use the word "process" in this context.	Replace "This process" with just "This." (Delete "process.")	Not Accepted. See CA7 for replacement text.
JP 27	5	4 th paragraph	Te	"Vulnerability processing" is not a term used widely in the community.	Replace "vulnerability processing" with "vulnerability handling."	Not Accepted. See JP28.
JP 28	5	4 th paragraph	Ge	It is not in the scope of this IS both to outline the phases of vulnerability handling (or processing) and to provide any guidance for creating a vulnerability handling policy, since they are internal business for vendors. Please refer to JP29.	Delete the 1 st sentence.	Accepted. The entire 4th paragraph will be deleted "This IS first outlines the phases of vulnerability processing then goes on to provide some guidance for creating a policy. This concludes with issuance of advisory and insight to potential issues that will surround this process."
JP 29	6		Ge	Although the explanation about phases of a vulnerability handling process helps readers to understand this IS, we don't believe that it is in the scope of this IS.	Move the description of phases of a vulnerability handling process (the beginning part of chapter six above section 6.1) into the chapter three or "terms and definitions".	Not Accepted. The Phase descriptions are not "terms and definitions."
JP 30	6		Ge	A section on vulnerability handling policy should be placed somewhere else instead of in the chapter about life cycle of vulnerability.	Move the section title of 6.1 into chapter seven, and renumber the seventh chapter and the followings.	Accepted. See also US comment 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 NBs¹] comments on ISO/IEC 3rd WD 29147

Date: 2009-11-02	Document: SC27 Nxxx
------------------	----------------------------

1	2	(3)	4	5	(6)	(7)
NB 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
JP 31	6		Ge	The sentences of the form “X does Y” (e.g. A finders discovers a potential security vulnerability) can be interpreted as meaning that X should do Y.	Move the description of phases of a vulnerability handling process (the beginning part of chapter six above section 6.1) into the chapter three or “terms and definitions”. Please refer to JP29	Not Accepted. The Phase descriptions are not “terms and definitions.”
JP 32	6	1. Discovery Phase	Te	In order to appeal the value of RVD we might have to mention how irresponsible vulnerability disclosure affect IT system safety.	Please reconsider the description of the discovery phase referring to Figure 5 in “Modelling the Security Ecosystem- The Dynamics of (In)Security” by Stefan Frei et al (Workshop on the Economics of Information Security 2009, June 2009) (http://weis09.infoseccon.net/files/103/paper103.pdf), which also shows black markets, full disclosure and white markets.	Not Accepted. Phase 1 is not the right section to describe other types of vulnerability disclosure. Describing non-responsible disclosure is out of scope of this IS.
JP 33	6	4. Advisory	Ed	“Release” seems to be a more appropriate word than “advisory.” Please refer to the internet draft on RVD process (http://tools.ietf.org/draft/draft-christey-wysopal-vuln-disclosure/draft-christey-wysopal-vuln-disclosure-00.txt).	Replace “advisory” with “release” or “publication.”	Not Accepted. Advisory is the accepted term.
JP 34	7		Ge	<ul style="list-style-type: none"> The title “Vulnerability Handling Policy Consideration” seems to be inappropriate as one of main chapters’. While vulnerability handling means a whole process relating vulnerabilities, it is our consensus that this IS should focus on the interface, or receipt and dissemination. 	Change the chapter title into “Receipt of Vulnerability Information” or something similar to this expression.	Accepted. Title of this section will be renamed to “Receipt of Vulnerability Information. See US 23 for renumbering this section as section 8.

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 NBs¹] comments on ISO/IEC 3rd WD 29147

Date: 2009-11-02	Document: SC27 Nxxx
------------------	----------------------------

1	2	(3)	4	5	(6)	(7)
NB 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
JP 35	6.1		Te	Most coordinators hand over vulnerability information to a vendor under the condition which the coordinators have defined, which might not be the same as the vendor's policy.	If some description about a policy remained in this IS, it also should be mentioned to harmonize vulnerability handling policy with other parties including coordinators.	
JP 36	7.1	1 st paragraph of each section	Te	Some coordinators provide secure channels for communicate with vendors. In the case vendors don't have to prepare for it by themselves.	Replace "provide" with "use" in the 3rd sentence.	Accepted. Will update accordingly.
JP 37	7.2		Te	Generally speaking, it is difficult to judge if the issue affects multiple vendors or not. It can be told with confidence only after the source of vulnerability is identified instead of the point of receipt time. So this subject should not be told in the context of receiving vulnerability information.	Move this section to an appropriate chapter other than 7.2.	Accepted. This subsection will be moved under the clause "Disseminating of Vulnerability Information". See US 23 where this clause is renumbered to 9.
JP 38	7.2	1 st paragraph	Ed	The 1 st sentence has the following issues: <ul style="list-style-type: none"> ● A relative pronoun is expected. ● "And so on" is more appropriate than "or otherwise." 	Change the 1 st sentence as follows: Some vulnerabilities affect common protocols, software libraries and so on, which impact multiple vendors.	Accepted. Will update accordingly.
JP 39	7.4		Te	Since CVE is assigned to vulnerable implementation, it can be obtained only after the source of vulnerability is identified instead of the point of receipt time.	Replace "assign or obtain a CVE number" with "assign a vulnerability identification number."	Accepted. See US 29.
JP 40	7.4		Te	CVE does not seem to be appropriate to be referred in the sense of the anxiety about its service continuity and scalability.	Remove "CVE" from the main text of this IS. If it is kept in this IS, modify the explanation into a general description about CVE, and place it in an annex.	Accepted. See CA 15 for replacement text.

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 NBs¹] comments on ISO/IEC 3rd WD 29147

1	2	(3)	4	5	(6)	(7)
NB 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
JP 41	7.6		Te	The same statement is found in the 1 st paragraph of Section 7.3. ("However, it is recommended that a response be provided within 14 days of receipt.") We see no need to repeat it in this independent subclause.	Remove this section.	Accepted. This subclause and its contents will be removed.
JP 42	7.7	1 st paragraph	Ge	The last sentence has the following problems: <ul style="list-style-type: none"> We can't see what it means, possibly because of a grammatical error in its if-clause. Reference should be A5 instead of A4. As for A5, please refer to JP56.) 	Remove the last sentence. Or correct it grammatically and semantically.	Accepted. The last sentence of the first paragraph will be replaced with the text "A list of some coordinators is contained in Annex A.4: CERT and Coordinators Globally."
JP 43	8	1 st paragraph	Ge Te	The last sentence has the following technical issues; <ul style="list-style-type: none"> We don't know consensus about how to define or how to decide whether multiple vulnerabilities are the same or not. Since vendors develop vulnerability resolution of their products independently, they often have no information about other vendors and no chance to choose the same common vulnerability identifier unless a coordinator mentions them. 	Define how to decide whether multiple vulnerabilities are the same or not. If it can't be clearly defined, remove all the description relating to vulnerability commonness.	Accepted. Last sentence of first paragraph will be removed.
JP 44	8.2		Ge	The description is too ambiguous for readers to learn.	Please elaborate more detail referring to the vendor responsibilities sections of the internet draft on RVD process (http://tools.ietf.org/draft/draft-christey-wysopal-vuln-disclosure/draft-christey-wysopal-vuln-disclosure-00.txt), which includes: <ul style="list-style-type: none"> In validation phase 	Accepted. The following text will be placed in the clause labeled "Vulnerability Handling Policy", currently section 6.1 : "Vendors should define their responsibilities in the vulnerability handling policy. For an example, see the internet draft on RVD process (http://tools.ietf.org/draft/draft-christey-wysopal-vuln-disclosure/draft-christey-wysopal-vuln-disclosure-00.txt), which includes:

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 NBs¹] comments on ISO/IEC 3rd WD 29147

Date: 2009-11-02	Document: SC27 Nxxx
------------------	----------------------------

1	2	(3)	4	5	(6)	(7)
NB 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

					<p>1) If the vulnerability is found in a supported product, the Vendor MUST either (1) reproduce the vulnerability, (2) determine if there is enough evidence for the existence of the vulnerability when it cannot be reproduced, (3) determine if the vulnerability is already known (and possibly resolved), or (4) work with the Reporter to determine if the vulnerability is related to the specific environment in which it was discovered (including configuration errors or interactions with other products).</p> <p>2) If the vulnerability is found in an unsupported or discontinued product, the Vendor MAY refuse to validate the vulnerability. However, the Vendor MUST ensure that the reported vulnerability does not exist in supported product versions or other supported products based on the vulnerable product.</p> <p>3) The Vendor SHOULD NOT assume that the risk or impact of the vulnerability is limited to what has been identified by the Reporter or involved Coordinator.</p> <p>4) The Vendor SHOULD examine its product to ensure that it is free of other problems that are similar to the reported</p>	wysopal-vuln-disclosure-00.txt)."
--	--	--	--	--	--	-----------------------------------

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 NBs¹] comments on ISO/IEC 3rd WD 29147

Date: 2009-11-02	Document: SC27 Nxxx
------------------	----------------------------

1	2	(3)	4	5	(6)	(7)
NB 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

					<p>vulnerability.</p> <p>5) The Vendor MUST consult with the Reporter and involved Coordinators when more information or analysis is needed.</p> <p>6) The Vendor SHOULD provide status updates to the Reporter and any involved Coordinators every 7 days. The Vendor MAY negotiate with the parties for less frequent updates.</p> <p>7) The Vendor MUST notify the Reporter and any involved Coordinators when the Vendor is able to reproduce the vulnerability.</p> <p>8) The Vendor SHOULD attempt to resolve the vulnerability within 30 days of initial notification.</p> <p>9) If the Vendor cannot resolve the vulnerability within 30 days, then the Vendor MUST provide the Reporter and involved Coordinators with specific reasons why the vulnerability cannot be resolved.</p> <p>10) If the Vendor is aware of other vendors that share the same codebase as the affected product, then the Vendor MUST either (1) notify those vendors, or (2) notify a</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 NBs¹] comments on ISO/IEC 3rd WD 29147

Date: 2009-11-02	Document: SC27 Nxxx
------------------	----------------------------

1	2	(3)	4	5	(6)	(7)
NB 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

					<p>Coordinator that other vendors may be affected by the reported vulnerability.</p> <ul style="list-style-type: none"> ● Release Phase <ol style="list-style-type: none"> 1) The Vendor SHOULD work with the Reporter and involved Coordinators to arrange a date after which the vulnerability information may be released. 2) The Vendor MAY ask the Reporter and Coordinator to allow a "Grace Period" up to 30 days, during which the Reporter and Coordinator do not release details of the vulnerability that could make it easier for hackers to create exploit programs. 3) If the Reporter has not properly followed the process and publicly announces the vulnerability, then the Vendor SHOULD post its awareness of the vulnerability, and the Vendor's progress in its resolution, to appropriate forums. 4) If a Reporter has properly followed the process, then the Vendor MUST provide credit to that reporter. 5) If a Coordinator has properly followed the process, then the Vendor SHOULD provide credit to the Coordinator. 	
--	--	--	--	--	---	--

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 NBs¹] comments on ISO/IEC 3rd WD 29147

Date: 2009-11-02	Document: SC27 Nxxx
------------------	----------------------------

1	2	(3)	4	5	(6)	(7)
NB 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

					<p>6) If a Reporter has not properly followed the process and publicly announces the vulnerability, then the Vendor MAY provide credit to the reporter.</p> <p>7) The Vendor MUST NOT assume that the lack of vulnerability details will prevent the creation of an exploit.</p> <p>8) The Vendor SHOULD cryptographically sign all patches using a method that is commonly accessible on the platforms for the Vendor's product. The Vendor should clearly advertise its cryptographic key and provide cryptographic checksums for its patches.</p> <p>9) The Vendor SHOULD provide an easily accessible mechanism for Customers and the Security Community to obtain all security advisories, such as a web page. The most recent advisory SHOULD be listed first.</p> <p>10) The Vendor SHOULD provide a mechanism for notifying Customers and the Security Community when new advisories are published.</p> <p>11) The Vendor SHOULD provide a means</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 NBs¹] comments on ISO/IEC 3rd WD 29147

Date: 2009-11-02	Document: SC27 Nxxx
------------------	----------------------------

1	2	(3)	4	5	(6)	(7)
NB 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

					<p>for the Security Community to identify which reported vulnerabilities are genuine, but are not regarded by the Vendor as important enough to merit a security advisory.</p> <p>12) The Vendor SHOULD provide an easily accessible indicator that allows a Customer to determine if the resolution has been applied to a system, e.g., by modifying the product's version number or providing the Customer with a tool that identifies the resolutions that have been applied to a product.</p> <ul style="list-style-type: none"> ● Policy Publication <p>1) Where it complies (and does not comply) with the process outlined in this document.</p> <p>2) The typical amount of time after notification that the Vendor requires to produce a resolution.</p> <p>3) The Grace Period, if any, that the Vendor wishes to observe.</p> <p>4) How the Vendor determines whether a reported problem is serious enough to merit a security advisory.</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 NBs¹] comments on ISO/IEC 3rd WD 29147

Date: 2009-11-02	Document: SC27 Nxxx
------------------	----------------------------

1	2	(3)	4	5	(6)	(7)
NB 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
JP 45	8.3		Ge	These messages seem to be common to all web sites instead of special to vulnerability web sites.	Remove this section.	Not Accepted. See US 39.
JP 46	Annex A		Ge Te Ed	Some of the contents including the following sections can't be normative, since they are apparently just examples: <ul style="list-style-type: none"> ● CERT/CC Vulnerability Reporting Form ● IPA and JPCERT Vulnerability Reporting Form ● All part of A.3 ● All part of A.4 ● All part of A.5 	Change the attribute of the annex into informative. Or at least move the left mentioned sections to an informative annex.	Accepted. This will be changed to an Informative Annex.
JP 47	Annex A.1	1 st paragraph	Ed	The description should be written from the vendors' viewpoint.	Modify the language into the form that vendors should do something or that vendors are recommended to do something.	Accepted. The first sentence in the first paragraph will be replaced by "In order to help the vendor in the Verification Phase the vendor can request that the finder provide the following information."
JP 48	Annex A. 2		Ed	The title "Advisory Considerations" should be reconsidered.	Change the section title. A possible alternative title is: Vulnerability Disclosure Format.	Accepted. See US 45 for replacement title.
JP 49	Annex A. 2	Last paragraph	Ed	It seems a typo or an excerpting error. Please refer to the section 3.1.11 in SC27 N6880.	Modify as follows: Provide contact information in case the vulnerability information is unclear or the security patch has caused some trouble.	Accepted. The last sentence of Annex A.2 will be replaced with text as follows: "Provide contact information in case the vulnerability information is unclear or the security patch has caused some issue."

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 NBs¹] comments on ISO/IEC 3rd WD 29147

1	2	(3)	4	5	(6)	(7)
NB 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
JP 50	Annex A.3	Example from US CERT	Ge	It is inappropriate to include a vulnerability statement of real products in the IS text.	Remove names of real products and real companies and any description associated with them.	Accepted. CERT representative (from US National Body) will seek permission from Adobe to use their name in this context.
JP 51	Annex A.3	Example from Cisco	Te	Plain text copy of clickable web pages is extremely misleading. It is also inappropriate to include a vulnerability statement of real products in the IS text.	Reconsider how to excerpt from clickable web pages. Also remove names of real products and real companies and any description associated with them.	Accepted. Editor will replace text versions of advisory examples with images of the web pages, and also seek permission from the web site owners to use the images in this context.
JP 52	Annex A.3	Example of Microsoft Security Bulletin	Ge	We can't see why the title is "Example of Microsoft Security Bulletin" instead of "Example from Microsoft." Plain text copy of clickable web pages is extremely misleading. It is also inappropriate to include a vulnerability statement of real products in the IS text.	Change the title into "Example from Microsoft." Reconsider how to excerpt from clickable web pages. Also remove names of real products and real companies and any description associated with them.	Accepted. Title will be changed as noted.
JP 53	Annex A. 3	Example of CVE	Te	Since CVE aims to be a dictionary of vulnerability, its entry has only a very brief description.	<ul style="list-style-type: none"> ● If it is intended to an example of released information (or advisory), CVE is not appropriate and should be deleted. ● If it is mentioned to explain what CVE is, place it in an appropriate section other than A.3. 	Accepted. The following text will be removed: "Example of CVE CVE-2009-2031 smbfs in Sun OpenSolaris snv_84 through snv_110, when default mount permissions are used, allows local users to read arbitrary files, and list arbitrary directories, on CIFS volumes.

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 NBs¹] comments on ISO/IEC 3rd WD 29147

1	2	(3)	4	5	(6)	(7)
NB 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

						View the full report at http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2031 Example of CVSS Example of CPE"
JP 54	Annex A. 3	Example of CVSS	Te	It is not appropriate to place it here as an example of released information (or advisory) by its nature.	Delete it or place it in an appropriate section other than A.3.	Accepted. See JP 53.
JP 55	Annex A. 3	Example of CPE	Te	It is not appropriate to place it here as an example of released information (or advisory) by its nature.	Delete it or place it in an appropriate section other than A.3.	Accepted. See JP 53.
JP 56	Annex A.4		Ge	Most readers can't see why this IS includes this section.	Add the reference to this section or NIAC to an appropriate section of the IS main body. The appropriate section seems to be the 6 th clause. If there is no appropriate section for the reference in the main body, delete A.4.	Not Accepted. See CA 1 where the NIAC is referenced.
JP 57	A.5	Title	Ge	"CERT" is not appropriate for the title in the following sense: <ul style="list-style-type: none"> "CERT" as a proper noun is a registered trademark of Carnegie Mellon University. "CERT" as a common noun has been replaced with CSIRT (Computer Security Incident Response Team) in the cyber security community. 	Remove "CERT" and change the title into "Coordinators recognized globally" or "Global coordinators."	Accepted. Title will change to "Coordinators Recognized Globally".
JP 58	A.5	1 st paragraph	Te	A function as a coordinator should be focused instead of a vulnerability disclosure centre in this annex. In the	Change the 1 st paragraph as follows:	Accepted. The paragraph will be replaced as follows: "The following list

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 NBs¹] comments on ISO/IEC 3rd WD 29147

1	2	(3)	4	5	(6)	(7)
NB 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	Japanese case, the former is represented by JPCERT/CC and the latter is represented by a web site called Japan Vulnerability Notes or JVN, whose URL is http://jvn.jp/en/ .	The following list identifies vulnerability coordinators which are known globally.	identifies vulnerability coordinators which are known globally."
JP 59	A.5	List	Te Ed	<ul style="list-style-type: none"> The legitimate name and the formal URL should be cited for each organization. The order of entries should be alphabetical. 	Change the list as follows: Australian Computer Emergency Response Team (AusCERT) http://www.uscert.org.au/ CERT/CC (Software Engineering Institute (SEI) CERT Program of Carnegie Mellon University) http://www.cert.org/ Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) http://www.jpcert.or.jp/english/	Accepted. The list will be changed as indicated.
JP 60	A.5	List	Te	CERT-FI, Finnish national Computer Emergency Response Team, who has handled vulnerabilities actively in these years, should be added to the list.	Add the following entry to the list: CERT-FI (Finnish national Computer Emergency Response Team) http://www.cert.fi/en/	Accepted. CERT-FI will be added to the list.
JP 61	B.1	3 rd paragraph	Te	CSIRT (Computer Security Incident Response Team) seems to be more common rather than SIRT.	Replace "Security Incident Response Team (SIRT)" with "Computer Security Incident Response Team (CSIRT)."	Accepted. Text will be changed as indicated.
JP 62	B.1	3 rd paragraph	Ge	The email address "alert@<companyname.com>" is not general enough.	Change "company.com" to "company domain name."	Accepted. Text will be changed as indicated.
JP 63	B.1	3 rd paragraph from the	Ge	Please refer to JP56.	Change "local CERT agency" to "regional CSIRT" or "national CSIRT."	Accepted. Text will be changed to "regional CSIRT".

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 NBs¹] comments on ISO/IEC 3rd WD 29147

1	2	(3)	4	5	(6)	(7)
NB 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

		bottom				
LU 1	3.4		Te	The ISO/IEC 27000 is now publicly available, suggest to use the definition of vulnerability from this standard	Vulnerability : weakness of an asset or control that can be exploited by a threat	Accepted.
LU 2	3.8		Ed	This definition is a duplicate of the definition 3.2	Proposal to delete 3.8 and merge with 3.2	Not accepted. See JP 13.
LU 3	3.10		te	This definition is a duplicate of the definition 3.4 Why refer to a security policy to define vulnerabilities?	Use definition of 27000 instead (weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source) Proposal to delete 3.10 and merge with 3.4. See comment LU-2	Not Accepted. See CA 6.
LU 4	3.11		Te	Definition in contraction with 27000, where an incident is something that might happen, but not mandating that the attempt has been made.	Define information security event as “an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant” and information security incident as “a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security”, according to ISO 27000	Not Accepted. See JP 21.
LU 5	6.1	§1	Ed	The Appendix B1 is a Sample Vulnerability Disclosure	Harmonize title of the Appendix B1 with	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 NBs¹] comments on ISO/IEC 3rd WD 29147

Date: 2009-11-02	Document: SC27 Nxxx
------------------	----------------------------

1	2	(3)	4	5	(6)	(7)
NB 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

				Policy, not relating to disclosure policy	title given in §6.1	
LU 6	7.3 and 7.7		te	The recommendation to send a acknowledgement back to the finder only after 14 days is unfair for the finder.	Replace 14 days by asap or as soon as reasonable possible.	Accepted. See CA 16.
LU 7	7.3	§3	Te	We do not consider an e-mail address such as info@example.com as relevant to use as e-mail address to manage security incidents (too general and generic) We consider using specific security e-mail address as best practices	Proposal to remove alias given as info@example.com	Accepted. info@example.com will be deleted.
LU 8	7.4			CVE number has not been explained in the glossary	Add CVE in glossary and in acronyms	Accepted. See ZA 40 where abbreviations will be expanded in section 4.
LU 9	7.4			CVE is not the sole vulnerability database OSVDB (Open Source Vulnerability Database) is another example	See if relevant to add reference to OSVDB (also in glossary if selected) Do this reference to the rest of the document	Not Accepted. See US 29. Since the title and focus of this section has been changed to more generic unique identifiers, there is no need to add a listing of vulnerability databases.
LU 10	Annex B		Ed	This policy is from a vendor point of view Maybe it should be interesting to propose also a such policy from a researcher point of view (text to be available if proposal of change accepted)		Not Accepted. Researcher point of view is out of scope for this IS.
ZA 1	All	All	ed	Inconsistent use of case when referring to applicable stakeholders, e.g. finder versus Finder.	Use either lower case or upper case. It is proposed that lower case is used throughout the document, since the use of upper case does not add value.	Accept will update case where required
ZA 2	All	All	te	Some concepts, e.g. system, component, service, are	Add a clause	Not Accepted. The addition of a new

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 NBs¹] comments on ISO/IEC 3rd WD 29147

Date: 2009-11-02	Document: SC27 Nxxx
------------------	----------------------------

1	2	(3)	4	5	(6)	(7)
NB 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
				used without an introduction. Also, a number of issues need to be clarified in order to understand the context of the standard.	<p>5 <i>Concepts</i></p> <p>5.1 Products and services</p> <p>5.2 Vulnerabilities</p> <p>5.3 Stakeholders</p> <p>6 Responsible vulnerability disclosure</p> <p>A contribution will be provided if this comment is accepted.</p>	clause is not needed to address clarifications that can be made in other sections, such as the Terms and Definitions section.
ZA 3	All	All	te	<p>The scope of this document is the responsible disclosure of vulnerabilities in products and services, and probably more specific, products of the shelf and services that are publicly available. Systems and products developed under contract by a supplier for a specific acquirer are not applicable. Services that are supplied under contract are not applicable.</p> <p>Vulnerability disclosure in such cases will be addressed in the contract, support or service contract.</p> <p>This observation is based on e.g. the definition of responsible vulnerability disclosure, where distinction is made between private and public disclosure. Public disclosure is not applicable in the cases mentioned above.</p> <p>Examples where this argument may seen not to hold are:</p> <ol style="list-style-type: none"> 1. a “public” service is provided using a “private” product 	<p>Clarify the scope, making clear the scenarios in which this standard is applicable:</p> <p>“This International Standard is applicable to the responsible disclosure of vulnerabilities in products and publicly available services. Systems and products developed under contract by a supplier for a specific acquirer are not applicable. Services that are supplied under contract are not applicable.”</p>	Not Accepted. It is out of scope for this IS to specifically exclude products or services covered by contractual agreements. Contractual agreements will supersede any standards where applicable.

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 NBs¹] comments on ISO/IEC 3rd WD 29147

Date: 2009-11-02	Document: SC27 Nxxx
------------------	----------------------------

1	2	(3)	4	5	(6)	(7)
NB 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

				<p>2. a “private” service is provided using a public product.</p> <p>In these cases, the “public” side will be addressed using this standard, and the private side through the applicable contract. Thus, in the first example, this standard is used to disclose the vulnerability to the service provider, who will then determine if the vulnerability is due to a vulnerability in the product. This will be addressed further in terms of the applicable contract.</p> <p>In the second example, if a vulnerability is found by the client of the service, and reported via the applicable procedures, the provider can use this standard to disclose any contributing vulnerabilities in the product.</p>		
ZA 4	All	All	te	<p>With reference to the ZA comment stating that the scope of this document is the responsible disclosure of vulnerabilities in products and services.</p> <p>Although the term <i>product</i> is commonly used and understood, it may be necessary to add a definition to make the context of the document more clear, and to distinguish it from its definition in ISO 9000.</p> <p>The Concise Oxford English dictionary defines <i>product</i> as an <i>article or substance manufactured or refined for sale</i>.</p>	<p>The following definition is proposed: “item developed, manufactured or refined for sale</p> <p>NOTE 1 A service is generally not viewed as a product.</p> <p>NOTE 2 A product is often developed using a systems approach.</p> <p>NOTE 3 In information technology, distinction is often made between hardware and software products, although the boundary is not always clear.</p> <p>EXAMPLE A router can be seen as a</p>	<p>Accepted. The term "Product" will be added to section 3 Terms and Definitions. The definition will be taken from the correct source, in order of ISO rules. If that source is the Oxford Dictionary, then that definition will be used. If it is some other ISO definition, then that definition will be used.</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 NBs¹] comments on ISO/IEC 3rd WD 29147

1	2	(3)	4	5	(6)	(7)
NB 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

					hardware product, although it uses software.”	
ZA 5	All	All	te	<p>With reference to the ZA comment stating that the scope of this document is the responsible disclosure of vulnerabilities in products and services.</p> <p>Although the term <i>service</i> is commonly used and understood, it may be necessary to add a definition the make the context of the document more clear.</p> <p>ISO/IEC 12207:2008 defines <i>service</i> as <i>performance of activities, work, or duties associated with a product</i>. Thus does not seem correct in the context of this document. Interestingly, ISO/IEC 20000 does not define <i>service</i>.</p>		Accepted. Editor will add the term "Online Services" to the Terms and Definitions section and propose a definition for the term in the next iteration of the draft.
ZA 6	All	All	te	A number of stakeholders/role players are mentioned in the document, e.g. finder, vendor. However, these entities are not introduced and explained.		Not Accepted. See ZA 2.
ZA 7	All	All	te	<p>According to the Concise Oxford English dictionary, a vendor is <i>a person or company offering something for sale</i>. This is consistent with the everyday use of the term, i.e., the focus is on <i>selling</i>.</p> <p>When I go to my local software shop, <i>Pete's software</i>, to buy a copy of <i>Lotus Notes</i>, then <i>Pete's software</i> is the vendor. Potential vulnerabilities in <i>Lotus Notes</i> should be reported to Lotus, not to Pete.</p> <p>The same holds when I buy a Cisco switch from <i>Pete and sons IT suppliers</i>. A potential vulnerability must be reported to CISCO, not to <i>Pete and sons IT suppliers</i>,</p>		Not Accepted. The term "supplier" and its proposed definition does not fit the use of the current term "vendor" for this IS.

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 NBs¹] comments on ISO/IEC 3rd WD 29147

Date: 2009-11-02	Document: SC27 Nxxx
------------------	----------------------------

1	2	(3)	4	5	(6)	(7)
NB 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

				<p>who is the vendor.</p> <p>(I could have bought the items directly from Lotus or Cisco on their web-site, in which case they would have been the vendor. That is, however, irrelevant.)</p> <p>Even if a support or maintenance contract states that vulnerabilities are to be reported via the vendor or service provider, the organisation that will have to address the vulnerability is the originators of the product.</p> <p>According to the Concise Oxford English dictionary, a supplier is someone who makes something available to someone else. This is a wider concept than vendor.</p> <p>ISO/IEC 12207:2008 and ISO/IEC 15288:2008 define <i>supplier</i> as <i>the organization or individual that enters into an agreement with the acquirer for the supply of a product or service</i>, and states that a supplier could be a contractor, producer, seller, or vendor.</p> <p>Within the context of a product life cycle, the agreement processes define the activities necessary to establish an agreement between two organizations. If the Acquisition Process is invoked, it provides the means for conducting business with a supplier of products that are supplied for use as an operational system, or of services in support of an operational system, or of elements of a system being developed by a project. If the Supply Process is invoked, it provides the means for conducting a project in which the result is a product or service that is delivered to the acquirer. (See ISO/IEC 12207, clause 5.)</p> <p>The term “vendor” has been addressed in previous</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 NBs¹] comments on ISO/IEC 3rd WD 29147

Date: 2009-11-02	Document: SC27 Nxxx
------------------	----------------------------

1	2	(3)	4	5	(6)	(7)
NB 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
				<p>comments, and from the contributed documents to the study period and previous versions of the WD, it can be seen that this is a common term to use in this field.</p> <p>However, it is my opinion that the term is misleading. Also, using this term does not fit in with the use of ISO/IEC 12207, remembering that 12207 does not only focus on development, but any form of acquisition of a system, as well as the whole life cycle of a system.</p>		
ZA 8	All	All	te	Do not refer to "IS".	Replace "IS" with "International Standard" throughout the document.	Accepted. Will update accordingly.
ZA 9	All	All	te	Hanging paragraphs shall be avoided since reference to them is ambiguous. (Directives part 2, clause 5.2.4)	Introduce the necessary clause heading to remove hanging paragraphs.	Accepted. Editor will create a subsection heading for the paragraph currently under section 7.
ZA 10	All	All	te	An International Standard consists of clauses.	Replace each occurrence of "section" with "clause".	Accepted. Will update accordingly
ZA 11	All	All	ed	Inconsistent use of bullets in lists.	Use either · or – The preference is – to conform to the ISO template and thus contributing to consistency across ISO publications.	Accepted. Will update all list bullets to "–".
ZA 12	Front page	Title	ed	Inconsistency in dashes.	Replace "techniques -- Responsible" with "techniques – Responsible"	Accepted. Will update accordingly
ZA 13	1	par. 1	ed	Possible better sentence construction.	Replace	Accepted. Will update sentence to

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 NBs¹] comments on ISO/IEC 3rd WD 29147

Date: 2009-11-02	Document: SC27 Nxxx
------------------	----------------------------

1	2	(3)	4	5	(6)	(7)
NB 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

					"guidelines for the vendor to receive" with "guidelines for a vendor to receive" or "guidelines for vendors to receive"	"guidelines for vendors to receive".
ZA 14	1	par. 1	ed	Possible better sentence construction,	Replace "information about a potential vulnerability" with "information about potential vulnerabilities"	Accepted. Will update accordingly.
ZA 15	1	par. 2	te	Possible better sentence construction, taking into account the directives for using "may" and "can".	Replace "The vendor may include the following; software vendor, hardware vendor, application service provider and on-line/web application provider." with "Vendors can include software vendors, hardware vendors, application service providers and on-line/web application providers." or "A vendor can be a software vendor,	Accepted. The text "may" will be replaced with "can".

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 NBs¹] comments on ISO/IEC 3rd WD 29147

1	2	(3)	4	5	(6)	(7)
NB 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

					hardware vendor, application service provider or an on-line/web application provider." or "Examples of vendors are software vendors, hardware vendors, application service providers and on-line/web application providers."	
ZA 16	1	par. 2	te	Possible better sentence construction, taking into account the directives for using "may" and "can". Also, when looking at systems as defined in ISO/IEC 15288, it may be better to refer to system element, rather than subcomponent, or simply component, Also, the Standard's scope seems to include hardware, thus components are not restricted to software.	Replace "The vendor may act as a finder or in some instances as both when using a 3 rd party software subcomponent." with "A vendor can act as a finder or in some instances as both, e.g. when using a system element supplied by a 3 rd party." or "A vendor can act as a finder or in some instances as both, e.g. when using a system element supplied by another party." or "A vendor can act as a finder or in some instances as both, e.g. when using a component supplied by another party."	Accepted. See US 7. Second sentence of para 2 will 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.

[All NBs¹] comments on ISO/IEC 3rd WD 29147

Date: 2009-11-02	Document: SC27 Nxxx
------------------	----------------------------

1	2	(3)	4	5	(6)	(7)
NB 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
ZA 17	1	par. 3	te	The reason for the distinction between "created" and "developed" is not clear.	Remove "created" from the sentence.	Accepted. Will remove the text "created,".
ZA 18	1	par. 3	te	It is not only vulnerabilities in components that are addressed. For ease of reference, and consistency, it is proposed that the focus of the Standard is on "products". This term is to be explained under the proposed concepts clause, and will include references to software, hardware, application service, web services, web applications, as applicable.	Replace "vulnerability in a component" with "vulnerability in a product or product component"	Accepted. Will update accordingly.
ZA 19	1	par. 4	te	For consistency, use the term stakeholder, rather than party.	Replace "to all interested parties." with "to all applicable stakeholders." or "to all stakeholders."	Accepted. The text "all interested parties" will be removed per JP 9.
ZA 20	1		te	Vulnerability disclosure is part of information security management.	Add the following to the scope: "From the perspective of the finder, vulnerability disclosure is part of the information security incident management process. It is also relevant to the management of technical vulnerabilities. See ISO/IEC 27002 for more information.	Not Accepted. This comment is out of scope for this standard, as the Finder's directives and perspective are out of scope.
ZA 21	3	par. 1	te	The <i>Terms and definitions</i> clause should make reference to the definitions in 27000.	"For the purposes of this document, the terms and definitions given in ISO/IEC	Accepted. First sentence of section 3 Terms and Definitions will be replaced

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 NBs¹] comments on ISO/IEC 3rd WD 29147

Date: 2009-11-02	Document: SC27 Nxxx
------------------	----------------------------

1	2	(3)	4	5	(6)	(7)
NB 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

					27000, and the following apply."	by "For the purposes of this document, the terms and definitions given in ISO/IEC 27000, and the following apply."
ZA 22	3	All definitions	te	The term and term number shall be in bold.	Make all terms and term numbers bold. (Follow the rules for drafting and presentation of terms and definitions in Annex D of the ISO/IEC directives, part 2.)	Accept will update accordingly
ZA 23	3.1	finder	te	Reference was made in clause 1 to "potential vulnerability". Is it not more correct to state that the finder identifies a potential vulnerability, which will be verified later in the process?	Replace "person or organisation who identifies the vulnerability" with "person or organisation who identifies the potential vulnerability" or "person or organisation who identifies a potential vulnerability" or "stakeholder who identifies a potential vulnerability" (preferred)	Accepted. See JP 12 for replacement text.
ZA 24	3.2	vendor	te	As was explained in a previous ZA comment, the term <i>vendor</i> is incorrectly used. A vendor does not necessarily develop the product, or maintains it. Thus the definition is	Remove the definition for vendor. Add a definition for supplier.	Not Accepted. See ZA 7.

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 NBs¹] comments on ISO/IEC 3rd WD 29147

Date: 2009-11-02	Document: SC27 Nxxx
------------------	----------------------------

1	2	(3)	4	5	(6)	(7)
NB 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

				incorrect. Also with reference to the previous comment, it is not even necessary to refer to a vendor, unless the reporting structure requires involvement of the organisation that sold the product.		
ZA 25	3.2	vendor	te	If the definition of vendor is retained, the following is applicable. A company is an organisation. Also, for the sake of consistency, it is best to keep the references to entities in a certain context, the same throughout the document. With reference to previous comments on using "stakeholder", it would be preferred if this term is used.	Replace "person, organisation, or company" with "person or organisation" or "stakeholder" (preferred)	Accepted. Text will be replaced with "person or organization".
ZA 26	3.2	vendor	te	If the definition of vendor is retained, the following is applicable. From the Scope, it is assumed that this Standard is not limited to software systems. Thus, vulnerabilities in system (products) containing hardware are also applicable. It is proposed that the definition of "vendor" is simplified to address "products", and that "product" is defined and explained later in the "concepts" clause. With reference to previous comments on using "stakeholder", it would be preferred if this term is used.	Replace the definition for vendor with: "person of organisation that developed the product, or is responsible for maintaining it" or "stakeholder that developed the product, or is responsible for maintaining it" (preferred)	Accept with the following text: "person or organisation that developed the product, or is responsible for maintaining it"
ZA 27	3.3	coordinator	te	The definition does not adhere to the directives. Also, as explained before, use "person or organisation" or "stakeholder" for consistency. Also, the fact that the presence of a coordinator is optional, is not part of the	Replace the definition with: "person or organisation that serves as a proxy between the supplier and the	Accepted. See US 9.

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 NBs¹] comments on ISO/IEC 3rd WD 29147

1	2	(3)	4	5	(6)	(7)
NB 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

				definition.	finder, assists with technical evaluations, coordinates among multiple vendors, or performs other functions to promote the effectiveness of the vulnerability response process NOTE Participation of a coordinator is optional.” or, if retaining “vendor” "person or organisation that serves as a proxy between the vendor and the finder, assists with technical evaluations, coordinates among multiple vendors, or performs other functions to promote the effectiveness of the vulnerability response process NOTE Participation of a coordinator is optional.”	
ZA 28	3.4	vulnerability	te	The focus of the document is on product, meaning something that was acquired from a supplier. The product can be viewed as a system. However, a system can also be developed in house using other sub systems and products. This document does not address systems that were developed in house for the sole purpose of in house requirements. Also, the definition does not adhere to the directives.	Replace “a weakness in a system” with “weakness in a product”	Not Accepted. See ZA 29.
ZA 29	3.4	vulnerability	te	ISO/IEC 27000 defines “vulnerability” as	Use this definition:	Accepted. Definition text will be replaced with "weakness of 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 NBs¹] comments on ISO/IEC 3rd WD 29147

1	2	(3)	4	5	(6)	(7)
NB 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

				“weakness of an asset or control that can be exploited by a threat”	<p>“vulnerability weakness of an asset or control that can be exploited by a threat [ISO/IEC 27000:2009]”</p> <p>If necessary, add the definitions for asset, control and threat as it is in ISO/IEC 27000.</p> <p>or</p> <p>“vulnerability weakness of a product, service or control that can be exploited by a threat NOTE Adapted from ISO/IEC 27000:2009”</p>	hardware, or online service that can be exploited by a threat NOTE Adapted from ISO/IEC 27000:2009”
ZA 30	3.4 Note	vulnerability	te	Incorrect use of NOTE. Should be EXAMPLE.	Replace “NOTE” with “EXAMPLE”.	Not Accepted. See ZA29.
ZA 31	3.5	software	te	<p>The Concise Oxford English dictionary defines <i>software</i> as <i>programs and other operating information used by a computer</i>. This definition is sufficient. ISO uses this dictionary as the base for definitions – thus is shouldn’t be necessary to define the term.</p> <p>The following definitions exist for <i>software</i>, as found via the SC 7 and IEEE vocabulary database (the on line version of (ISO/IEC 24765:2009 Systems and software engineering vocabulary)</p> <p>(1) all or part of the programs, procedures, rules, and</p>	Remove the definition for software.	Accepted. This term will 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.

[All NBs¹] comments on ISO/IEC 3rd WD 29147

Date: 2009-11-02	Document: SC27 Nxxx
------------------	----------------------------

1	2	(3)	4	5	(6)	(7)
NB 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

				associated documentation of an information processing system. (ISO/IEC 2382-1:1993 Information technology-- Vocabulary--Part 1: Fundamental terms, 01.01.08) (2) computer programs, procedures, and possibly associated documentation and data pertaining to the operation of a computer system (IEEE 829-2008 IEEE Standard for Software and System Test Documentation, 3.1.32) (3) program or set of programs used to run a computer (ISO/IEC 26514 Systems and software engineering-- requirements for designers and developers of user documentation, 4.46) Example: command files, job control language Note: includes firmware, documentation, data, and execution control statements See Also: application software		
ZA 32	3.6	application		<p>The Concise Oxford English dictionary defines <i>application</i> as <i>a program or a piece of software designed to fulfil a particular purpose</i>.</p> <p>ISO/IEC 24765 provides the following possibilities:</p> <ol style="list-style-type: none"> 1. a system for collecting, saving, processing, and presenting data by means of a computer. ISO/IEC 24570:2005 Software engineering -- NESMA functional size measurement method version 2.1 – Definitions and counting guidelines for the application of Function Point Analysis 2. a coherent collection of automated procedures and data supporting a business objective. ISO/IEC 20968:2002 Software engineering -- Mk II Function Point Analysis -- Counting Practices Manual.10. 3. a cohesive collection of automated procedures and data supporting a business objective. ISO/IEC 	Remove the term <i>application</i> . Rather refer to product, as in software product or hardware product.	Accepted. This term will 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.

[All NBs¹] comments on ISO/IEC 3rd WD 29147

Date: 2009-11-02	Document: SC27 Nxxx
------------------	----------------------------

1	2	(3)	4	5	(6)	(7)
NB 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
				20926:2003 Software engineering -- IFPUG 4.1 Unadjusted functional size measurement method -- Counting practices manual. Syn: application system, information system cf. system		
ZA 33	3.7	update	te	Updates to software are not restricted to addressing vulnerabilities. Rather make distinction between updates and security updates. Also, the current definition is not sufficient	software update maintenance change or addition to a software product to correct anomalies or improve usability security update software update to correct vulnerabilities or improve security	Not Accepted. The term "update" will remain in place for this draft, since it is used in a few different contexts elsewhere. See Section 6 Lifecycle of a Vulnerability. If South Africa would please make specific text substitution suggestion in context elsewhere in the draft, then we will reconsider changing the term.
ZA 34	3.8		te	Already defined in 3.2	Remove 3.8	Not Accepted. See JP 13.
ZA 35	3.10		te	Already defined in 3.4	Remove 3.10	Not Accepted. See BE 7.
ZA 36	3.11	security incident	te	The definition should adhere to ISO/IEC 27000	information security event identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that may be security relevant [ISO/IEC 27000:2009] information security incident single or a series of unwanted or	Not Accepted. See JP 21.

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 NBs¹] comments on ISO/IEC 3rd WD 29147

Date: 2009-11-02	Document: SC27 Nxxx
------------------	----------------------------

1	2	(3)	4	5	(6)	(7)
NB 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
					<p>unexpected information security events that have a significant probability of compromising business operations and threatening information security</p> <p>[ISO/IEC 27000:2009]</p> <p>NOTE In the context of this International Standard, the focus is on information security incidents related to possible vulnerabilities in the products used in the information system.</p>	
ZA 37	3.12	vulnerability information service	te	Error in definition (see directives)	<p>Replace</p> <p>“an organization”</p> <p>with</p> <p>“organization”</p>	Not Accepted. See US 16.
ZA 38	3.13	advisory	te	<p>The definition not correct, since the word is not defined. Also, an advisory is a common English word, thus it would be better to distinguish between <i>advisory</i> and <i>vulnerability advisory</i>.</p>	<p>vulnerability advisory</p> <p>official announcement or warning about a vulnerability in a product</p> <p>NOTE 1 A vulnerability advisory may include advice on how to deal with the vulnerability.</p> <p>NOTE 2 An advisory typically contains a description of the vulnerability including a list of vulnerable software, potential impact, resolution and mitigation information, and references.</p>	Accepted. See JP 23 for replacement text.

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 NBs¹] comments on ISO/IEC 3rd WD 29147

Date: 2009-11-02	Document: SC27 Nxxx
------------------	----------------------------

1	2	(3)	4	5	(6)	(7)
NB 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

					NOTE 3 An advisory may be published by a vendor, finder, or coordinator.	
ZA 39	4	Heading	te	Symbols are not applicable	Rename the clause to “Abbreviated terms”	Accepted. Editor will double-check that this heading is not part of a required ISO template before making the recommended change.
ZA 40	4	All	te	List of abbreviated terms found which may have to be included in clause 4.	BBS CC CCE common configuration enumeration CERT CPE common platform enumeration CVE common vulnerabilities and exposures CVSS common vulnerability scoring system DLL ID IPA JPCERT URL PDF portable document format	Accepted. The editor will identify all abbreviated terms used in this draft and list them here, making sure to check the ISO directives for the proper location for abbreviated terms in an IS.

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 NBs¹] comments on ISO/IEC 3rd WD 29147

1	2	(3)	4	5	(6)	(7)
NB 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
					POC proof of concept PGP Pretty Good Privacy SIRT security incident response team SRM secure receiving model	
ZA 41	5	par. 1	ed	Capital letter	Replace "Responsible Disclosure" with "Responsible disclosure"	Accepted. Will update accordingly.
ZA 42	6	List	ed	Inconsistent and incorrect punctuation.	The entries with alphabetical numbering should all end with a full stop.	Accepted. Will update accordingly.
ZA 43	6	Last par.	ed	Unnecessary word.	Replace "potential vulnerability issue" with "potential vulnerability"	Accepted. Will update accordingly.
ZA 44	6	Last par.	te	Possible better construction to highlight the two primary functions.	Replace the last paragraph with: These phases identify at a high level the tasks related to dealing with a potential vulnerability. They can be aligned to two primary functions: receiving and dissemination. - Receiving deals with obtaining the details of the possible vulnerability.	Accepted. The last paragraph will be replaced with the text "These phases identify at a high level the tasks related to dealing with a potential vulnerability. They can be aligned to two primary functions: receiving and dissemination." - Receiving deals with obtaining the details of the possible vulnerability.

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 NBs¹] comments on ISO/IEC 3rd WD 29147

Date: 2009-11-02	Document: SC27 Nxxx
------------------	----------------------------

1	2	(3)	4	5	(6)	(7)
NB 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
					- Dissemination focuses on getting that information to all interested parties. The remainder of this document focuses on these two primary aspects, including some initial preparatory details for organizations that lack process maturity.	- Dissemination focuses on notifying affected parties. The remainder of this document focuses on these aspects."
ZA 45	6	Last par.	ed	Unnecessary words.	Replace "focuses on these two primary aspects" with "focuses on these aspects"	Accepted. Will update accordingly.
ZA 46	6	Last par.	te	Unnecessary words. Also see next comment.	Replace "some initial preparatory details" with "some initial details"	Accepted. See ZA 44 for replacement text.
ZA 47	6	Last par.	te	"lack process maturity" is a very general statement to make. This statement should be elaborated on, or not made.	Replace "The remainder of this document focuses on these two primary aspects, including some initial preparatory details for organizations that lack process maturity." with "The remainder of this document focuses on these aspects."	Accepted. See ZA 44 for replacement text.

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 NBs¹] comments on ISO/IEC 3rd WD 29147

Date: 2009-11-02	Document: SC27 Nxxx
------------------	----------------------------

1	2	(3)	4	5	(6)	(7)
NB 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
ZA 48	6.1	par. 1	te	Incorrect reference to clause number.	Replace "B1" with "B.1" Replace "Appendix" with "Annex" or "Clause"	Accepted. Text will be replaced by correct labelling format. See UK 6 for renumbered and titled Annexes.
ZA 49	6.1	Last par.	te	Incorrect reference to clause number.	Replace "B1" with "B.1" Replace "Appendix" with "Annex" or "Clause"	Accepted. Text will be replaced by correct labelling format. See UK 6 for renumbered and titled Annexes.
ZA 50	6.1	Last par.	ed	Unnecessary repetition of statement already made in par. 1.	Remove one of the two references made to Annex B.	Accepted. Will update accordingly.
ZA 51	7	par. 1	te	Unnecessary reference to the fact that a "vendor" creates software or hardware. This is stated in the definition.	Replace "Vendor who creates software and hardware will have different" with "vendor will have different" or "supplier will have different"	Accepted. The replacement will be as follows: Replace "Vendor who creates software and hardware will have different" with "vendor will have different"
ZA 52	7	par. 1	te	Possible better sentence construction for easier reading and understanding. See also the following comment.	Replace "This section discusses in detail some considerations when creating a policy." with "This clause discusses considerations to be taken into account when creating a policy."	Accepted. Text will be replaced as indicated.

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 NBs¹] comments on ISO/IEC 3rd WD 29147

Date: 2009-11-02	Document: SC27 Nxxx
------------------	----------------------------

1	2	(3)	4	5	(6)	(7)
NB 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
ZA 53	7	par. 1	te	Possible better sentence construction for easier reading and understanding. See also the following comment.	<p>“As each Vendor will have different requirements and resources available for dealing with security vulnerability information; understanding some of these topics in detail will help to provide guidance when they arise.”</p> <p>with</p> <p>“Each vendor has different requirements and resources available for dealing with security vulnerability information. Understanding the topics in this clause will help to provide guidance when they arise.”</p>	Accepted. Text will be replaced as indicated.
ZA 54	7	par. 1	te	Proposal for new paragraph.	<p>Replace par. 1 with:</p> <p>“Each vendor has different requirements and resources available for dealing with security vulnerability information. This clause discusses considerations to be taken into account when creating a policy.”</p>	Accepted. See ZA 53.
ZA 55	7.7	par. 1	te	Incorrect reference to clause number.	<p>Replace “A4” with “A.4”</p> <p>Replace “Appendix” with “Annex” or “Clause”</p>	Accepted. References will be replaced as indicated.
ZA 56	Annex A	Title	te	The current content of Annex A is not normative.	State that Annex A is informative	Accepted. See JP 46.
ZA 57	Annex A	Title	te	Annex A has no title.	Provide a title. No proposal – not sure what the overall purpose is of Annex A.	Accepted. See UK 6 for renumbered and titled Annexes.

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 NBs¹] comments on ISO/IEC 3rd WD 29147

1	2	(3)	4	5	(6)	(7)
NB 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

ZA 58	Annex A	All	te	The reference to specific suppliers make create the impression of endorsing those suppliers. Even referencing specific CERTs may create a problem. Using existing policies, forms from existing organisations as examples has the risk of becoming outdated.	Do not use existing policies, forms and advisories as examples. Use them as input to create new generic examples (organisation neutral).	Not Accepted. It is common practice to include specific examples in ISO documents.
ZA 59	A.4	All	te	There is no need to include this clause on a USA specific framework.	Use what is applicable from the framework in the International Standard itself. Reference can be made in the Bibliography.	Not Accepted. However, in order to keep the annex relevant, the editor will remove the following extra text from A.4: "The following seven recommendations are made to the President to direct appropriate Departments and Agencies involved in any aspect of managing software vulnerabilities. <ul style="list-style-type: none"> • Support development of a common vulnerability management architecture, including common terms and universally compatible procedures to be employed in the public and private sectors for identifying, reporting, scoring, remediating, and resolving vulnerabilities. This includes standardized E-mail addresses for reporting and standardized Web site locations and content for sharing information effectively. • Provide policy and funding to ensure that trusted environments are available to protect vulnerability

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 NBs¹] comments on ISO/IEC 3rd WD 29147

1	2	(3)	4	5	(6)	(7)
NB 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

						<p>information and ongoing investigations.</p> <ul style="list-style-type: none"> • Promote universal use of multiple compatible encryption methods to ensure the U.S. federal government can participate effectively in the global vulnerability management process. • Conduct a regulatory framework review. The federal government should review existing federal regulations and practices in order to identify barriers to resolving software vulnerabilities. • Support robust voluntary information sharing through policy and funding. The federal government should set up or support neutral clearinghouses for vulnerability management, accessible to researchers, the private sector, and federal agencies. • Support a robust infrastructure for international coordination. • Promote and fund advanced university and industry security research and education.”
ZA 60	A.5	All	te	It will useful to have the list of examples of response teams and coordinators in a separate informative annex.	Move A.5 to a new informative Annex.	Accepted. See UK 6 for new annex numbers and titles.
ZA 61	Annex B	Title	te	Annex B has no title.	Provide a title. No proposal – not sure what the overall purpose is of Annex B.	Accepted. See UK 6 for new annex numbers and titles.

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 NBs¹] comments on ISO/IEC 3rd WD 29147

1	2	(3)	4	5	(6)	(7)
NB 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
ZA 62	Bibliography	All	te	The following entries are not necessary: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12	Remove these entries from the Bibliography.	Accepted. These will be removed as noted.
ZA 63	All	All	ge	ISO/IEC 27035 addresses incident management.	I may be worthwhile to see if there is overlap, or at least to make reference to each other.	Not Accepted. If South Africa would please provide specific instances of overlap for the next round of comments, it would be appreciated for consideration.
ZA 64	All	All	ge	This International Standard should be a requirements standards, i.e. it should be possible to claim conformance against requirements stated as "shall". Normative content must be provided.	Adapt the current content to enable: - Conformance by a user/consumer to e.g. processes for vulnerability detection and disclosure. - Conformance by a supplier to processes to e.g. handle vulnerability disclosure, updating of products, dissemination. - Normative content of information items such as policies, receipts, reports, etc. A contribution will be provided if this comment is accepted.	Not Accepted. The purpose of this IS is to be a guideline, since most implementations of an application security response and vulnerability handling policy are dependent on the business decisions and resources of the vendor. If South Africa could please propose specific conformance clauses for the next round of comments, we can reconsider this.
UK 1	Foreword	3	Ed	In the template text, "should" should be "shall".	Fix	Accept. Text "should" will be replaced with "shall".
UK 2	Introduction	2	Ed	The word "finder" is capitalised to indicate it is a special term. However, the scope clause is often used in isolation from the rest of the Standard and thus this will not be clear.	Replace second sentence by "A vendor may of course discover a vulnerability in a third party's software component and in some instances both find and	Accepted. See CA 1 for replacement text.

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 NBs¹] comments on ISO/IEC 3rd WD 29147

1	2	(3)	4	5	(6)	(7)
NB 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
					disseminate information about it.”	
UK 3	3	-	Ed	Definitions should be in alphabetical order.	Fix	Accepted.
UK 4	3.13	-	Te	The text given is not a definition – if substituted for the defined term, it does not make sense.	Replace current definition by “a public notification of the existence of a vulnerability” and move current text to the note following.	Accepted. See JP 23 for replacement text.
UK 5	7.7	-	Te	The Draft does not specify what a finder should do if the vendor ignores a notification, or issues a misleading advisory, and the vendor has no conflict arbitration procedure.	Expand 7.7 to state that the vendor should always offer a conflict arbitration service.	Not Accepted. Requiring the vendor to provide conflict arbitration services is out of scope for this IS.
UK 6	Annex A, B	-	Ed	Annex A has no title and appears to cover four unrelated topics. Likewise Annex B has no title and appears to cover two unrelated topics	Split both current annexes into multiple annexes.	Accepted. The existing annexes will be renumbered as follows: A.1 will become A; A new Annex called Annex B Advisories will contain the currently labeled A.2, which will become B.1; currently labeled A.3 will become B.2; A.4 will become C; A.5 will become D; B.1 will become E; B.2 will become F.
US 1	Overall	N/A	Te	In Beijing, China, all National Body representatives agreed to the following: 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. See SC27N7799_WG3N999_DOC_29147: Comment US	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.	Not Accepted. If the US would provide specific text for replacement, we will reconsider this.

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 NBs¹] comments on ISO/IEC 3rd WD 29147

1	2	(3)	4	5	(6)	(7)
NB 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
				1.		
US 2	Overall	N/A	Ge	In Beijing, China, all National Body representatives agreed to the following: A number of areas of this document need fleshing out before it can progress to CD status. See SC27N7799_WG3N999_DOC_29147: Comment UK 1.	Complete document as a matter of urgency.	Accepted. The editor would ask the experts provide the necessary information necessary to complete section they deem as incomplete. This will ensure the document is completed as a matter of urgency.
US 3	Overall	N/A	Ed	In Beijing, China, all National Body representatives agreed to the following: The document is full of typos and grammatical errors. See SC27N7799_WG3N999_DOC_29147: Comment US 2.	Proofread and edit the entire document for spelling and grammar.	Accepted. Will continue to review and make correction. The editor asks the specific references be indicated going forward.
US 4	Entire Document	N/A	Te	“Vendor” is the most frequently used term in this standard for the key stakeholder that is responsible for the affected product’s maintenance. However, the term “Organization” (in sections 5, 6, 6.1, 7.4, etc.) and “Developer” (in section A.2) is also used.	Replace all appropriate instances of “Organization” and “Developer” with “Vendor” for consistency.	Accepted. Changed will be made throughout as indicated.
US 5	Introduction	¶ 1, last sent	Te	In Beijing, China, all National Body representatives agreed to the following: 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.”	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.”	Accepted. See CA 1.

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 NBs¹] comments on ISO/IEC 3rd WD 29147

Date: 2009-11-02	Document: SC27 Nxxx
------------------	----------------------------

1	2	(3)	4	5	(6)	(7)
NB 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

				See SC27N7799_WG3N999_DOC_29147: Comment US 7.		
US 6	Introduction	¶ 2	Te	The phrase “work together diligently” is somewhat prescriptive, Well-intentioned stakeholders may not be able to do this.	Replace “work together diligently” With: “work together in good faith”	Not Accepted. See CA 1 for replacement text.
US 7	1 Scope	¶ 2	Te	The sentence “The vendor may act as a Finder or in some instances as both when using a 3 rd party software subcomponent.” is not clear and not necessary. Where the Finder works, whether it is at a Vendor company or a Coordination center, is immaterial.	Remove the sentence “The vendor may act as a Finder or in some instances as both when using a 3 rd party software subcomponent.”	Accepted. Second sentence of para 2 will be removed.
US 8	2	Normative References	Te	The list is currently empty. Given the nature of this standard, the US would like to review the references that are regarded as normative. See SC27N7799_WG3N999_DOC_29147: Comment UK 3.	Complete clause as a matter of urgency.	Not Accepted. If the US will provide specific text for this section, we will consider it for the next iteration..
US 9	3.3	Term Coordinator	Te	The definition of coordinator should be minimal, with further provisions that make for a “good coordinator” explained in the body of the document. Not all coordinators can or will provide the proxy services or multi-vendor coordination listed in the current definition.	Replace “An optional participant that can serve as a proxy between the Vendor and Finder, assists with technical evaluations, coordinates among multiple vendors, or performs other functions to promote the effectiveness of the vulnerability response process” With “an optional participant that can assist	Accepted. Definition text will be replaced with “an optional participant that can assist Vendors and Finders in managing and disclosing vulnerability information” .

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 NBs¹] comments on ISO/IEC 3rd WD 29147

1	2	(3)	4	5	(6)	(7)
NB 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

					Vendors and Finders in managing and disclosing vulnerability information.”	
US 10	3.4	¶ 2	Te	The existing text is paraphrased poorly from NIAC Framework. Instead, quote directly from the NIAC definition, citing credit.	<p>Replace</p> <p>“NOTE 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> <p>With</p> <p>“NOTE From the National Infrastructure Advisory Council Vulnerability Reporting Framework, “Examples of the unauthorized or unexpected effects of a vulnerability may include any</p> <p>of the following:</p> <ul style="list-style-type: none"> · _ Executing commands as another user · _ Accessing data in excess of specified or expected permission · _ Posing as another user or service within a system 	Not Accepted. See ZA 29.

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 NBs¹] comments on ISO/IEC 3rd WD 29147

1	2	(3)	4	5	(6)	(7)
NB 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
					<ul style="list-style-type: none"> · _ Causing an abnormal denial of service · _ Inadvertently or intentionally destroying data without permission · _ Exploiting an encryption implementation weakness that significantly reduces the time or computation required to recover the plaintext from an encrypted message. <p>Common causes of vulnerabilities are design flaws in software and hardware, botched administrative processes, lack of awareness and education in information security, and advancements in the state of the art or improvements to current practices, any of which may result in real threats to mission-critical information systems.”</p>	
US 11	3.7	Term Update	Te	<p>Some vulnerabilities can be addressed by a change to the Product’s documentation.</p> <p>Some vendors us the term “hotfix.”</p>	<p>Replace</p> <p>“patch, fix, upgrade, or configuration change to address a vulnerability NOTE 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. Vendor use different</p>	<p>Accepted. Definition text will be replaced with "patch, fix, upgrade, configuration or documentation change to address a vulnerability</p> <p>NOTE A change intended to resolve or mitigate a vulnerability. An update typically takes the form of</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 NBs¹] comments on ISO/IEC 3rd WD 29147

1	2	(3)	4	5	(6)	(7)
NB 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

					terms including patch, fix and upgrade. “ With “patch, fix, upgrade, configuration or documentation change to address a vulnerability. NOTE Vendors may use different terms including patch, fix, hotfix, and upgrade.”	a configuration change, binary file replacement, hardware change, or source code patch, etc. Updates are usually provided by vendors. Vendor use different terms including patch, fix, hotfix, and upgrade.”
US 12	3.8	Term Vendor	Ed	Duplicate of section 3.2	Delete section 3.8	Not Accepted. See CA 4 and JP 11.
US 13	3.9	Term Responsible Vulnerability Disclosure	Te	Responsible Vulnerability Disclosure is too complex a subject to write a simple definition for in this section. .	Replace the term “Responsible Vulnerability Disclosure” and subsequent definition with “Vulnerability Disclosure” and define it as in the introduction “the practice of reporting, coordinating, and publishing information about a vulnerability”.	Not Accepted. See JP 20.
US 14	3.10	Term Vulnerability	Ed	Duplicate of section 3.4	Delete section 3.10	Not accepted see BE 6 and JP 11.
US 15	3.11	Term Security Incident	Te	A security incident is not just evidence (of attacks); it is the action (of the attacks).	Delete “evidence of”	Not Accepted. See JP21.
US 16	3.12	Term Vulnerability Information	Te	Vulnerability information service is defined here but this term is not used anywhere else. A vulnerability information service plays no part in the resolution of a vulnerability or in its responsible disclosure. In fact some	Delete section 3.12	Accepted. Term will be deleted.

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 NBs¹] comments on ISO/IEC 3rd WD 29147

Date: 2009-11-02	Document: SC27 Nxxx
------------------	----------------------------

1	2	(3)	4	5	(6)	(7)
NB 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

		Service		vulnerability information services act irresponsibly in the context of this standard by publishing information about a vulnerability without the agreement of the key stakeholders (Finder, Vendor and Coordinator) and prior to an update being available.		
US 17	3.13	Term Advisory	Te	Current wording is not a definition of an Advisory. The advice provided in an Advisory is aimed at users of the Products affected by the Vulnerability. It therefore does not need to be anything more than information about the Update that addresses the Vulnerability. Ideally it will also contain enough information about the Vulnerability to persuade and encourage users of the affected Products to apply the Update or act on the advice provided.	Replace definition of “Advisory” with “(noun) information about an Update that addresses a Vulnerability and may include information about the Vulnerability .”	Accepted. See JP 23 for replacement text.
US 18	5	1	Te	This section starts by stating what Responsible Vulnerability Disclosure implies rather than what it is. We propose a description of what it is	Replace “Responsible Disclosure implies that the vulnerability finder and vendor work together diligently to produce a timely resolution to reduce user’s risks associated with the vulnerability.” With “Responsible Vulnerability Disclosure is the act of releasing information about a vulnerability in a manner that provides users of products subject to the vulnerability with the ability to protect themselves against attackers who exploit the vulnerability. This usually requires an announcement of the availability of an update for the affected product at the same time as, or before,	Accepted. See JP 25 for replacement text.

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 NBs¹] comments on ISO/IEC 3rd WD 29147

Date: 2009-11-02	Document: SC27 Nxxx
------------------	----------------------------

1	2	(3)	4	5	(6)	(7)
NB 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

					any other information about the vulnerability is released. Normally this announcement takes the form of an advisory issued by the vendor. If a vendor decides no update is necessary, the vendor should advise the finder of this decision, allowing the finder to publish information about the vulnerability if the finder desires.”	
US 19	5	2	Te	Academic and research communities usually focus on identifying insecure development methods and practices which includes insecure coding that leads to security vulnerabilities. It is not their goal per se to simply identify security vulnerabilities.	Replace “identify common security vulnerabilities” with “identify insecure development methods and practices, including insecure design and coding that result in security vulnerabilities”	Accepted. Text will be replaced as indicated.
US 20	6	All except 6.1	Te	Lifecycle of a vulnerability is better handled by having a reference to the NIAC diagram in the annex.	Delete section 6 “Lifecycle...” except for section 6.1. Refer to the NIAC diagram in the Annex wherever the first reference to the “lifecycle of a vulnerability” occurs in this document.	Not Accepted. Lifecycle of a Vulnerability is important information to be in the body of the draft and provides context for the reader.
US 21	6.1	¶ 2 1 st number list item	Te	Once a vendor has created a contact for receiving vulnerability information, the vendor should publish the contact information on their website, and also should give their contact information to CERTs and various other registries.	Add the text: “Once a vendor has created a contact for receiving vulnerability information, the vendor should publish the contact information on their website, and also should give their contact information to CERTs.”	Accepted. The text will be added as follows “Once a vendor has created a contact for receiving vulnerability information, the vendor should publish the contact information on their website, and also should give their contact information to vulnerability coordinators.”

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 NBs¹] comments on ISO/IEC 3rd WD 29147

1	2	(3)	4	5	(6)	(7)
NB 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
US 22	6.1	¶ 2 2 nd number list item	Te	A vendors' vulnerability policy should explain what responses and actions a finder can expect from the vendor, but specifying a turn around time for these should be optional, except for initial acknowledgement as covered in section 7.3	Replace "2. Expected turn around times for responses and action" with "2. Expected responses"	Accepted. Text will be replaced with "Expected responses".
US 23	6.1	Entire	Te	Section 7 is called "Vulnerability Handling Policy", therefore, the currently labelled section 6.1 "Vulnerability Handling Policy Considerations" belongs as a subsection of section 7.	Move section 6.1 under Section 7 as the first subsection of section 7 (7.1).	Accepted. Section 6.1 Vulnerability Handling Policy will become section 7, and labeled "7 Vulnerability Handling Policy". Current section 7 and all subsections will become section 8. See JP 34 for new name for this section. Current section 8 and all subsections will become section 9.
US 24	7.2	¶ 1 sent 2	Ge	Finders are out of scope for this IS.	Replace second sentence with: "For Vulnerabilities that are suspected to affect multiple vendors, stakeholders should consider notifying a coordinator to help handle vulnerability notification and resolution." Delete second paragraph.	Accepted the second sentence of the first paragraph and the second paragraph will be replaced with the following text: "For Vulnerabilities that are suspected to affect multiple vendors, vendors should consider notifying a coordinator to help handle vulnerability notification and resolution."
US 25	7.3	¶ 1 sent 1	Te	The standard should not impose that the internal identifier used to track a vulnerability is a number. However, it should be unique.	Replace "an internal tracking number" with "a unique internal identifier, typically a number"	Accepted. Text will be replaced as indicated.
US 26	7.3	¶ 2 sent 2	Te	Many small vendors may not have registered their own mail domain, but instead use free web mail applications. This attempt at enforcing non-repudiation is excessive.	Delete requirement concerning official mail domain registration. Delete	Accepted. Text will be deleted as indicated.

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 NBs¹] comments on ISO/IEC 3rd WD 29147

1	2	(3)	4	5	(6)	(7)
NB 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
					"If e-mail is agreed upon, this e-mail should be sourced using and address from the receiving parties official mail domain registration."	
US 27	7.3	¶ 1	Te	14 days is too long for acknowledgement of a report, but in order to accommodate for international holidays, it seems like a decent upper-bound.	Change language to "no more than 14 calendar days" to illustrate that the time period is an upper bound.	Not Accepted. See CA 16.
US 28	7.3	¶ 4	Te	support@ and info@ are sub-optimal, require vendor to monitor general purpose addresses for security/vulnerability reports. Should emphasize more specific addresses.	Remove support@ and info@. Or, note that general/multi-purpose addresses require the vendor to monitor for vulnerability reports and that more specific-use addresses are preferred.	Accepted. support@example.com and info@example.com will be deleted.
US 29	7.4	Title	Te	Change title of section to describe generic identifier. Not all Vendors will use CVE. Expand upon CVE further in the section itself.	Replace "Obtaining a CVE Number" with "Assigning a Unique Identifier to a Vulnerability"	Accepted. Title of this clause will be changed to "Assigning a Unique Identifier to a Vulnerability".
US 30	7.4	1	Te	This is the first reference to CVE. It has not been defined earlier. It should be explained in more detail, and its proposed use should be justified. Some vendors may prefer their own unique identification system and this should not be prohibited for vulnerabilities that affect no other vendors.	Replace "At the time of receiving vulnerability information neither the Finder nor Vendor will be required to assign or obtain a CVE number. Larger vendors are typically provided a block of CVE numbers that can be used when the data received is recognized as a vulnerability and the advisory is made public. Otherwise smaller organizations can contact CVE directly to obtain a number."	Accepted. See CA 15 for replacement text.

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 NBs¹] comments on ISO/IEC 3rd WD 29147

Date: 2009-11-02	Document: SC27 Nxxx
------------------	----------------------------

1	2	(3)	4	5	(6)	(7)
NB 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

					<p>With</p> <p>"A vendor should assign a unique identifier to each vulnerability. The identifier should be available for reference by customers and the public. The vendor may use this or other identifiers for internal bug or case tracking. A vendor may wish to use Common Vulnerabilities and Exposures (CVE) Identifiers, either as the only identifier for a vulnerability or in addition to the vendor's identifier.</p> <p>From <http://cve.mitre.org/cve/identifiers/index.html>:</p> <p>"CVE Identifiers (also called "CVE-IDs," "CVE names," "CVE numbers," and "CVEs") are unique, common identifiers for publicly known information security vulnerabilities."</p> <p>CVE assigns numbers for publicly disclosed vulnerabilities as they are published. Before public disclosure, a vendor or finder can obtain a CVE identifier from a CVE Candidate</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 NBs¹] comments on ISO/IEC 3rd WD 29147

Date: 2009-11-02	Document: SC27 Nxxx
------------------	----------------------------

1	2	(3)	4	5	(6)	(7)
NB 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
					Numbering Authority < http://cve.mitre.org/cve/cna.html >.”	
US 31	7.5	Entire	Ed	This section is confusing and appears to duplicate part of section 6.1 related to how a vendor would like to be contacted.	Since Section 6.1, per US comment 23 is to be moved within Section 7, Delete the current section 7.5.	Not Accepted. See JP 34 where clause 7 is renamed to "Receipt of Vulnerability Information". This subclause belongs in this section.
US 32	7.6	Entire	Ed	Duplicates section 7.3	Delete section 7.6	Accepted. See JP 41.
US 33	7.7	Title	Te	Change title of this section to reflect the role of Coordinator, as an instructional item for the Vendor audience of this document.	Replace “Conflict Arbitration between a Vendor and Finder” with “Role of a Coordinator”	Accepted. Title of this section will be changed to "Role of a Coordinator".
US 34	7.7	Entire	Te	This section assumes a coordinator is only required when a conflict arises between a vendor and a finder. Coordinators should only be used when (i) a vulnerability affects more than one vendor and the work of coordinating is too much for the finder, and (ii) a finder prefer to allow a coordinator to act on the finder’s behalf (as the finder’s proxy). This latter reason (ii) for using a coordinator covers the situation when a conflict between a finder and a vendor occurs without needing to spell out typical conflicts.	Delete section 7.7 or rewrite it to focus on the positive roles a coordinator plays without the primary reference to conflict resolution. “A Coordinator is an optional participant that can assist Vendors and Finders in managing and disclosing vulnerability information. An effective coordinator should be objective, have the technical capacity to understand vulnerabilities and their scope, and be able to communicate securely with Vendors, Finders, and other stakeholders.”	Not Accepted. See US 33.
US 35	8	¶ 1, sent 1	Te	Some vendors only release advisories to their customers, not to the general public. As long as all users of affected products are notified and able to protect themselves,	Replace “to the public” with “Vendors should set up a way to release vulnerability information to affected	Accepted. Text will be replaced as indicated.

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 NBs¹] comments on ISO/IEC 3rd WD 29147

1	2	(3)	4	5	(6)	(7)
NB 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

				there is no need for public disclosure. In practice, ensuring that all affected users are identified and notified is much more difficult to do privately than publicly, but the option should be noted.	parties. This may commonly include public disclosure, and may also involve private customer notifications. “	
US 36	8.2	Entire	Ge	The vendor’s vulnerability handling policy covered in section 6.1 should cover all situations including all these.	Delete this section and move its content to section 6.1 where the ideas should be clarified. Note per US Comment 23, section 6.1 should be moved under section 7.	Accepted. This section will be deleted. The text “When an exception to the vulnerability handling process occurs, such as the finder releases vulnerability information before the mutually-agreed date, or the vulnerability is being actively exploited, the vendor should define how it will handle these exceptions.” as well as the suggested text in JP 44 will be included in the section labelled “Vulnerability Handling Policy” (currently section 6.1). The reason to delete this from clause 8 Disseminating of Vulnerability Information is because this section defines actions that will be taken on a recurring basis, where the section on Vulnerability Handling Policy will describe the creation of a policy, which should only occur once. Defining the exception process for the policy should also occur once.
US 37	8.2		Te	Additional example of special consideration – vulnerability	Add bullet point that active exploitation of a vulnerability can drive deviation	Accepted. See US 36.

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 NBs¹] comments on ISO/IEC 3rd WD 29147

Date: 2009-11-02	Document: SC27 Nxxx
------------------	----------------------------

1	2	(3)	4	5	(6)	(7)
NB 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

				is being actively exploited.	from normal processing. Note per US Comment 36 that these concepts should be moved under section 6.1, which in turn should be moved under section 7.	
US 38	8.2			Note the situations that Vendors must consider as part of their vulnerability handling policy, but do not provide prescriptive guidance on what exactly Vendors should do for each contingency.	Delete the sentence "This section provides guidance to these situations and what can be done."	Accepted. See US 36.
US 39	8.3	Title	Te	Not all Vendors will have a vulnerability servicing model that includes a web repository for vulnerability information or updates. Some vendors may choose to send a CD containing updates to affected customers, for example.	Replace "Web Site Considerations" with "Public Advisory Release Considerations"	Accepted. Title of this section will be changed as indicated
US 40	8.3	¶ 1	Te	Add a sentence to the beginning of this section to outline options for public advisory release.	Insert "If a Vendor intends to release an advisory to the public, the following are common considerations for such public release."	Accepted. The first sentence in the clause will be replaced by the text as written.
US 41	8.3	1 st bullet list item	Te	If Vendors have a website for public advisory information, then Vendors should have a clear way for customers to reach that information.	Replace "If the web site has a deep hierarchy or the layout is complicated, it is difficult for the users to get to vulnerability information. Make sure that the users do not have to go through the layers of web pages to view vulnerability information " With "Clearly identify security information and its location on Vendor's website. A	Accepted. The first bulleted list item will be replaced with the text as follows: "Clearly identify security information and its location on Vendor's website. "

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 NBs¹] comments on ISO/IEC 3rd WD 29147

Date: 2009-11-02	Document: SC27 Nxxx
------------------	----------------------------

1	2	(3)	4	5	(6)	(7)
NB 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
					common web layout for security information is www.company.com/security . Another common location is under the support section of the website such as www.company.com/support/security .”	
US 42	8.3	2 nd bullet list item	Ge	Using a vulnerability’s title as hyperlink text is not ideal as vulnerabilities’ titles are not always unique and sometimes change as new information emerges. It also seems strange for a standard to specify this level of detail for a web page design.	Delete this bullet.	Accepted. This bullet will be deleted.
US 43	8.3	3 rd bullet list item	Ge	“1.3.10” is not the universal format for a date, and looks more like a product version number. It also seems strange for a standard to specify this level of detail for a web page design.	Delete “such as 1.3.10 (Revision History).”	Accepted. The 1st bullet text will be replaced with "Put the first publication date and the last updated date in the advisory. Consider using the ISO 8601 date format."
US 44	Annex A		Te	This Annex needs to be Informative, rather than Normative. It seems to be instructions for Finders on what kind of information to submit to Vendors when reporting vulnerabilities. Since the target audience of this standard is Vendors, any advice to Finders is for informational purposes only.		Accepted. See JP 46.
US 45	A.2	Title	Te	If this IS is specific to vendors, then advisory considerations are specific to vendors, reflect this in title. Others (coordinators, VIS, CSIRTs) also publish advisories.		Accepted. Title of this annex will be changed as indicated. See UK 6 for new number for this annex (B.1).
US 46	A.2	¶ 1	Te	While vendors will certainly make severity determinations,		Accepted. Last sentence of first

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 NBs¹] comments on ISO/IEC 3rd WD 29147

Date: 2009-11-02	Document: SC27 Nxxx
------------------	----------------------------

1	2	(3)	4	5	(6)	(7)
NB 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
				vendors should strive for consistency. Exceptional vulnerabilities that require unusual remediation or mitigation steps or are particularly difficult to understand would likely require more information.		paragraph will be replaced as indicated.
US 47	A.2	¶ 7	Te	<p>“Several methods for exchanging vulnerability information” do exist, but at least b. CCE is not widely adopted.</p> <p>Is the point to recommend certain formats, or provide a list of generally acceptable/used formats?</p> <p>If this section is to provide more of a list/menu for readers, provide some other formats and guidance language to make the intention clear, e.g., “The following vulnerability information formats are well researched or generally accepted/used. You may wish to adopt one or more of these formats.”</p>		Accepted. This item will be removed.
US 48	A.2	¶ 7	Ed	Vulnerability information formats lack references.	Provide references for whatever formats are listed.	Accepted. See ZA 40.
US 49	A.5	All	Te	Two other CSIRTs (at least) do coordination work, CERT-FI and CSIRT-UK/CPNI.	Assuming they agree (wish to advertise globally their coordination services), add CERT-FI and CSIRT-UK/CPNI.	Accepted. List will include these as noted and in the format required by JP 59.
US 50	Annex B	¶ 6	Te	PGP, not S/MIME, is the accepted practice.	<p>Remove S/MIME and replace with OpenPGP, or add OpenPGP, noting that it is the current accepted practice.</p> <p>Add RFC4880 (OpenPGP) to the bibliography.</p>	Not Accepted. However, the editor will replace sentences 2 and 3 of paragraph 6 with the following text: "We are equipped to receive encrypted messages. Our encryption key can be found on our website with this policy."

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.