Template for comments and secretariat observations

Date: October 6, 2021	Document: **Public comments**	Project: NIST cybersecurity whitepaper: "Baseline Security Criteria for Consumer IoT Devices"

MB/NC[1]	Line number (e.g. 17)	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
Deloitte & Touche LLP	4	N/A	1	ge	Maintain consistency throughout document of either Internet-of-Things or Internet of Things	Replace "Internet-of-Things" with "Internet of Things" throughout document; or simply replace all instances with IoT as it has been defined. No need to re-define again (ex. Line 9 and 12)	
Deloitte & Touche LLP	5	N/A	1	ed	"NIST also is to consider ways to incentivize manufacturers and developers to participate in these programs" is difficult to read and asymmetrical in its current wording and sentence structure.	Suggest rewording to "NIST will consider ways to incentivize manufactures and developers to participate in these programs.".	
Deloitte & Touche LLP	25	N/A	3	ed	Remove the word "draft" from the wording if the whitepaper will ultimately be published: "This white paper presents draft baseline security criteria for consumer IoT devices developed using the [NISTIR 8259A] baseline of device cybersecurity capabilities..."	Suggest rewording to "This white paper presents baseline security criteria for consumer IoT devices developed using the [NISTIT 8259A] baseline of device cybersecurity capabilities…."	
Deloitte & Touche LLP	48	N/A	5	ge	The "section for Feasibility of Implementation" considers technical requirements but does not address the time needed for implementation.	Consider updating Feasibility of Implementation" to include information on time needed for implementation	
Deloitte & Touche LLP	56	N/A	5	ed	"*For conformity*: Are the technical criteria suitable for conformity assessment?"	Suggest rewording to "*For conformity*: Are the technical criteria suitable for a conformity assessment."	
Deloitte & Touche LLP	58	N/A	6	ge	This section seems to speak to commentors of the whitepaper, and not the actual criteria of the Consumer IoT devices "NIST seeks comment on all aspects of cybersecurity labelling technical criteria for IoT devices. Specific areas for consideration include..."	Suggest moving this section out of the whitepaper if it is directed at commentors; if it is not directed at commentors, what is the connection to consumer IoT devices?	
Deloitte & Touche LLP	77	N/A	7	ed	Remove the italics from this sentence: "One notable extension of the baseline that may be appropriate is consideration of the cybersecurity of the *IoT product* rather than that of only the IoT device:	Suggest rewording to "One notable extension of the baseline that may be appropriate is consideration of the cybersecurity of the IoT product rather than that of only the IoT device"	

1 **MB** = Member body / **NC** = National Committee (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

Template for comments and secretariat observations

Date: October 6, 2021	Document: **Public comments**	Project: NIST cybersecurity whitepaper: "Baseline Security Criteria for Consumer IoT Devices"

MB/NC[1]	Line number (e.g. 17)	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
Deloitte & Touche LLP	91	N/A	9	ge	The criteria for distinguishing between the three (3) tables isn't clearly defined.	The Table descriptions should better explain the hierarchy (if applicable) and what differentiates the three tables.	
Deloitte & Touche LLP	N/A	N/A	Table 1	te	The Product Security IoT Product Cybersecurity Capability in Table 1 creates confusion	While the previous rows are cybersecurity capabilities or domains, this term adds confusion to what is being discussed. Companies that manufacture IoT products will typically have an internal function called "Product Security" which adds confusion with what is being discussed here.	
Deloitte & Touche LLP	129	N/A	10	ge	The tiers are not clearly defined. "The bottom tier (or level) provides a minimum meaningful amount of assurance about the security of an IoT product"	Consider including a diagram or image of the different security tiers/levels and the associated amount of "security/protection" of the IoT product.	
Deloitte & Touche LLP	146	N/A	12	ge	The approach for a conformity assessment does not require companies to maintain IoT certifications.	Regarding relevant certification companies can get for their IoT devices; this should be added as a requirement for a Conformity Assessment	
Deloitte & Touche LLP	150	N/A	13	ed	"In the context of consumer IoT products, the purchaser may be unequipped to meaningfully assess the cybersecurity of an IoT device, so conformity assessment – including provision of meaningful, consumer-oriented information about the implication of that assessment – could be critical."	Suggest rewording to "In the context of consumer IoT products, the purchaser may be unequipped to meaningfully assess the cybersecurity of an IoT device, so a conformity assessment – including provision of meaningful, consumer-oriented information about the implication of that assessment – could be critical."	
Deloitte & Touche LLP	166	N/A	15	ge	The term "Consumer" and "purchaser" is used interchangeably throughout the white paper, and has not been differentiated	Consider differentiating "Consumer" and "Purchaser" early on or chose to solely use one term.	

1 **MB** = Member body / **NC** = National Committee (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

Template for comments and secretariat observations

Date: October 6, 2021	Document: **Public comments**	Project: NIST cybersecurity whitepaper: “Baseline Security Criteria for Consumer IoT Devices”

MB/NC[1]	Line number (e.g. 17)	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Observations of the secretariat

1 **MB** = Member body / **NC** = National Committee (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