Comment Template for Draft NIST Interagency Report (NISTIR) 8200 -- Status of International Cybersecurity Standardization for the Internet of Things (IoT)

Comments of CTIA (filed April 18, 2018)

COMMENT #	SOURCE	TYPE i.e., Editorial Minor Major	LINE # PAGE etc.	RATIONALE for CHANGE	PROPOSED CHANGE (specific replacement text, figure, etc. is required)
1	N/A	Major	Section 8, pages 46-47; and Annex D, pages 63 *et seq.*	NIST's *Cybersecurity Framework* is a leading example of how voluntary, flexible, and consensus-based approaches enhance security. Highlighting the *Cybersecurity Framework* throughout Draft NISTIR 8200 would provide helpful guidance to the international standards community.	NIST should discuss and urge adoption of the *Cybersecurity Framework*, emphasizing the characteristics that made it a success—namely its voluntary, risk-based, flexible, and cost-effective approach. *See* CTIA Comments, at 3.
2	N/A	Major	Section 8, pages 46-47; and Annex D, pages 63 *et seq.*	Like the *Cybersecurity Framework*, highlighting other NIST guidance, industry activities, and public-private partnerships would provide helpful guidance to the international standards community.	NIST should discuss other NIST guidance, industry activities, and public-private partnerships. *See* CTIA Comments, at 3.
3	N/A	Minor	Section 1, page 1; Section 2, page 3; Section 6, page 22; and Annex D, page 63	Without this clarification, Draft NISTIR 8200 may inadvertently lead readers to conclude that adoption of identified standards is mandatory or that NIST recommends these standards.	NIST should clarify that private use of standards is voluntary and that identification of standards does not constitute endorsement. *See* CTIA Comments, at 4.
4	N/A	Major	Section 9, Table 4, pages 53-54.	Table 4 lacks support, is confusing to readers, and presents an inaccurate picture on the status of cybersecurity standardization for IoT applications.	NIST should more accurately characterize the availability and uptake of standards by deleting or adjusting Table 4. *See* CTIA Comments, at 4-5.
5	N/A	Major	Section 6.7, pages 28-29; Section 8.7, page 50; Section 9, Table 4, page 54; and Annex D, pages 122-142.	Draft NISTIR 8200 does not recognize the different roles SDOs play in the development of network security standards or the complexities inherent in standards adoption. It also overlooks many existing and developing network security standards in Appendix D.	NIST should expand the discussion on network security and develop the network security standards in Appendix D. *See* CTIA Comments, at 5.

Comment Template for Draft NIST Interagency Report (NISTIR) 8200 -- Status of International Cybersecurity Standardization for the Internet of Things (IoT)

Comments of CTIA (filed April 18, 2018)

COMMENT #	SOURCE	TYPE i.e., Editorial Minor Major	LINE # PAGE etc.	RATIONALE for CHANGE	PROPOSED CHANGE (specific replacement text, figure, etc. is required)
6	N/A	Major	Section 5.1, pages 9-10; Section 7.2, pages 37-39; and Annex D, pages 63 *et seq.*	Draft NISTIR 8200 largely omits recent developments by the auto sector and NHTSA to develop cybersecurity standards for connected vehicles.	NIST should expand the discussion on connected vehicles and develop the connected vehicle standards in Appendix D. *See* CTIA Comments, at 5-6.
7	N/A	Major	Throughout Draft NISTIR 8200, including Executive Summary, page ii; Section 5.3, page 14; Section 7.3, page 41; and Section 7.4, page 43	Draft NISTIR 8200 is intended for use by the IICS WG member agencies to assist in standards planning and U.S. government participation in international cybersecurity standardization for IoT. *See* Executive Summary, at ii.	NIST should focus on the federal government and clarify its use cases. *See* CTIA Comments, at 6-7.
8	N/A	Major	Throughout Draft NISTIR 8200, including Section 5.5, page 20	Draft NISTIR 8200 is intended for use by the IICS WG member agencies to assist in standards planning and U.S. government participation in international cybersecurity standardization for IoT. *See* Executive Summary, at ii.	NIST should remain focused on security issues. *See* CTIA Comments, at 7.
9	N/A	Major	Section 10, page 56	Uniform labels are not likely to be applicable across sectors and may undermine the core principle of risk-based decision making.	NIST should not endorse consumer-facing logos or labeling. Rather than labeling, NIST should encourage agencies to foster private innovation and development of appropriate certifications. *See* CTIA Comments, at 10.