February 12, 2018

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

COMMENT #	SOURCE	TYPE i.e., Editorial Minor Major	LINE # PAGE etc.	RATIONALE for CHANGE	PROPOSED CHANGE (specific replacement text, figure, etc. is required)
1	Kurt Danis, Joint Functional Component Command Integrated Missile Defense/J66; Information Systems Security Manager; 720 Irwin Avenue, Room 1409 Schriever AFB, CO 80912-7200; 719-721-9957, kurt.danis@jfcc-imd.stratcom.mil	Major	Line 228, p. vi	From the Red Book, our current cybersecurity doctrine is predicated on trusted systems. Yet, the cybersecurity community tends to ignores untrusted systems. This is a mistake. In short, we ought to have a strategy for dealing with untrusted systems... Internet of Things, ICS, SCADA, Platform IT, and even standalone (one of) machines. Clearly, untrusted systems have utility and have persisted for some time. For this reason, a rudimentary security model is provided for untrusted systems. Reference: 1987-07-31 NCSC-TG-005 Ver.1 Red Book	Add line that says: • Annex H — Security model for untrusted IoT (Annex H)

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

COMMENT #	SOURCE	TYPE i.e., Editorial Minor Major	LINE # PAGE etc.	RATIONALE for CHANGE	PROPOSED CHANGE (specific replacement text, figure, etc. is required)
2	Kurt Danis, Joint Functional Component Command Integrated Missile Defense/J66; Information Systems Security Manager; 720 Irwin Avenue, Room 1409 Schriever AFB, CO 80912-7200; 719-721-9957, kurt.danis@jfcc-imd.stratcom.mil	Major	Line 315, p. 3	See comment #1.	Add bullet that says: • Security model for untrusted IoT (Annex H)

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

COMMENT #	SOURCE	TYPE i.e., Editorial Minor Major	LINE # PAGE etc.	RATIONALE for CHANGE	PROPOSED CHANGE (specific replacement text, figure, etc. is required)
3	Kurt Danis, Joint Functional Component Command Integrated Missile Defense/J66; Information Systems Security Manager; 720 Irwin Avenue, Room 1409 Schriever AFB, CO 80912-7200; 719-721-9957, kurt.danis@jfcc-imd.stratcom.mil	Major	Annex H	See comment #1.	To understand untrusted systems, we use an nautical analogy: (a) Consider closed-celled vessels having water-tight integrity; they float, but cannot be submerged. That would correlate to our federal information systems (unclassified and classified); (b) Consider submarines having air-tight integrity, that would be a National Security Systems (governed by CNSS issuances); (c) Consider a lobster trap (no integrity, and fully immersed), that would equate to an untrusted system... fully immersed in the wild with viruses, malware, and affected by every known and unknown malfeasance. Yet, the device has utility. At the end of the day, this is where we get our lobster. Do we sanitize the lobster trap? Do we equip the trap with the latest anti-macrobiotics. Absolutely not. But rest assured, we will boil the lobster! Likewise, we sanitize the data for ingestion into our federal information systems. For this reason, a rudimentary security model is provided for untrusted systems. Security Model for Untrusted Systems Where IoT devices operate in an unprotected mode, designed to receive, process, store, and transmit data, the transmission (data output) is sanitized or converted prior to being ingested by a trusted system. Digital or printed data may be translated with reprographics, processed through the use of cross domain systems, handled manually for transcription, or processed with any other non-contact method such that viruses or malware cannot be transmitted to a trusted system.

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

COMMENT #	SOURCE	TYPE i.e., Editorial Minor Major	LINE # PAGE etc.	RATIONALE for CHANGE	PROPOSED CHANGE (specific replacement text, figure, etc. is required)