February 12, 2018 – **Ruwan Welaratna, Member – Cybersecurity Group, GCTC Wireless SuperCluster**

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		Minor	281	1 Introduction Add a more holistic view of the IoT to the summary	...these networked connected devices*, along with the cloud servers providing data services, and any associated stored data,* needs to be secure and resilient.
2		Minor	485	Grammar	LED lights are ~~increasing~~*increasingly* being added to vehicles...
3		Minor	512-513	Add some important use cases	door locks, door openers, ~~and~~ smart lightbulbs*, room occupancy sensors, motion detectors, security cameras, pet monitors, and baby monitors*.
4		Minor	676-677	Grammar and logic errors	Individually they open the building control app and ~~submits~~*submit* their ~~request~~*requests* to ~~lower~~*raise* the temp...
5		Major		In Section 6, Cybersecurity Areas and IoT, should the risks of (1) RF interference and (2) physical access to distributed sensors be mentioned? I am not familiar enough with the 802.11, 802.15, and other standards to know if RF is covered there. In any case it makes sense to call this out as an area of risk for Iot.	New **Section 6.8 Radio Frequency Transports** IoT components will often be connected to their cloud using RF connections. These RF connections may be based on ISM band, cellular data, or other standards. RF interference should be considered as a source of risk for IoT deployments. Individual sensors may be disabled or degraded by RF interference. This could be inadvertent, e.g., use of a poorly shielded microwave oven near an IP based security camera; or malicious, e.g., use of a cell-phone jammer to prevent LTE-connected motion sensors from transmitting activity to a security officer monitoring station. Antenna and RF radio design and appropriate shielding may mitigate such attacks but they may be impossible to prevent. Therefore system design should take into account graceful degradation of service. This may include user notification when sensors go offline, redundant sensor placement, and multiple backhaul technologies. Cost/benefit tradeoffs must be considered. System design documents should include a discussion of these points. New **Section 6.12 Physical Security** IoT components will often be distributed over a wide area. Physical security of sensors should be taken into account in system design. An attacker may seek to disable an individual component, or replace it with a component that appears to serve the same purpose but is compromised. Individual system components should be identifiable and authenticated.

COMMENT #	SOURCE	TYPE i.e., Editorial Minor Major	LINE # PAGE etc.	RATIONALE for CHANGE	PROPOSED CHANGE (specific replacement text, figure, etc. is required)
					It may not be practical to prevent vandalism or deliberate disabling of sensors, their communication channels, or their power supplies. Therefore system design should take into account graceful degradation of service. This may include user notification when sensors go offline, redundant sensor placement, battery backup, and multiple backhaul technologies. Cost/benefit tradeoffs must be considered. System design documents should include a discussion of these points.
6		Major	1298-1300	Different layers of the application stack will have different networking technologies and considerations.	An IoT system should use a network topology that has multiple layers, with each layer's security considered separately, so that all communication occurs with as much security and reliability as afforded by the technology.
7		Major	1305-1311	Mention RF and physical considerations when discussing individual IoT components	Consideration should be given to RF attack vectors and physical access to individual components.
8		Major	1353	Call out that risk evaluation should include the wider Internet as a whole	This example shows that the risks introduced by the adoption and deployment of IoT systems, or indeed cloud based systems in general, may not be to the owner or operator of the insecure system. In fact the risk may be to a different publicly accessible system on the Internet, or in fact to the Internet as a whole. Therefore risk assessment may need to consider a wholly different perimeter than traditionally considered in IT system risk assessment.
9		Major	1692	Add RF and physical security	IoT components are highly heterogeneous (operating systems, network interfaces/protocols/*physical layers including RF technologies*, functions*, physical accessibility*.
10		Major	1704-1707	"It is better to lose functionality than lose security". Really? What if someone is able to tap into an IP security camera, but not take it offline. Isn't it better to still have viewing and recording capability even if the attacker also has viewing?	Replace paragraph starting on 1704 with: "IoT systems may affect the safety, reliability, resiliency, performance, and other aspects of an owner's computing infrastructure and physical presence. If a failure occurs, consideration should be given to the desired failure mode. If a compromised component can still provide primary functionality to the owner, perhaps the component should be kept online while the compromise is addressed. In other systems the preferred outcome may be to take the component offline. Each system must be considered on its own merits, and the rationale for the decisions should be documented as part of the system design.
11		Major		RF And physical security additions to section 8	New **Section 8.6 Radio Frequency Transports** and **Section 8.12 Physical Security**

February 12, 2018 – **Ruwan Welaratna, Member – Cybersecurity Group, GCTC Wireless SuperCluster**

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)
					(I don't have the background to know if there are already standards in these areas. Are there any existing documents around surveillance cameras, street lighting, and emergency service radios that might apply)?