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	901 6.4 Identity and Access Management See white papers: Comment preparation: ProjectSafety.org MerlinCryption *A Newly Clarified Fourth state of Data* *Embedded Encryption Platform Benefit Analysis* IoT Is Changing the Cybersecurity Industry Is Cybersecurity Encryption Ready to Break?		1725 8.1 Cryptographic Techniques	Cryptographic standards need to secure four types of data. *Data-at-Rest, Data-in-Motion, or Data-in-Use and a new definition of data Data-in-Change***.** The cryptographic standards and technology need to protect all these data types while offering strong authentication. Cryptographic techniques will need adjustments and innovations to accommodate the IoT. Scalability, performance, memory- and power-limited devices, and constrained communication channels all contribute to the cryptographic challenges associated with the IoT. The computational demands of public-key cryptography, which may not be feasible for tiny IoT devices, must be weighed against the key management and protocol limitations that come with symmetric key cryptography. As an example, and given the immense scale envisioned for IoT applications, certificate revocation, which include resource-hungry activities such as the processing and storage associated with certificate revocation lists (CRLs) or the bandwidth associated with Certificate Status Protocol (OSCP), would have to be compared to the manual process and vulnerability of symmetric key distribution and update. Some current standards can support IoT systems but must often have to reduce the computational size of the algorithms offering weak encryption. For instance, many IoT components can support the Advanced Encryption Standard (AES) block cipher, included in ISO/IEC 18033-3:2010. IoT security requires encryption techniques with higher grade encryption capabilities with much lower overhead. The rational for change for new cryptographic techniques offer the need adjustments and innovations to accommodate IoT security requirements. IoT requires changes not only needed to secure IoT but changes needed in what IoT connects to and what connects to IoT. All cryptographic techniques need to be changed and the unique needs of securing IoT highlights these needs. These must be light weight but powerful enough to address the computational power of the Quantum computer.	Unencrypted data is at risk in each of the four states of data: Data-at-Rest, Data-in-Motion, the newly clarified Data-in-Use, and the newly clarified and defined, Data-in-Change. The proposed change addresses the strong encryption and authentication of all these data types. The proposed Anti-Statistical Block Encryption (ASBE) offers: • Nondeterministic Encryption Algorithm. • Every encrypted transmission is different. • Produces differential cyphertext, even when repeating the same plaintext, key, and password. • All output is variable. There is no static behaviors or repeating patterns. • Scrubs memory after each encryption or decryption. •Shredded files not available for theft. The proposed Anti-Statistical Block Encryption (ASBE) offers: • Nondeterministic Encryption Algorithm. • Every encrypted transmission is different. • Produces differential cyphertext, even when repeating the same plaintext, key, and password. • All output is variable. There is no static behaviors or repeating patterns Every encrypted file or data stream has an encrypted variable length digital signature (in the range 1 to 65535 bytes - which by itself is stronger than AES256). We call this digital signature "password". Variable length encryption keys (making the key length unpredictable to hackers by adding non-mathematically structured exponential strength. Even quantum computers cannot brute force the encryption.

				Cryptographic techniques will need adjustments and innovations to accommodate the IoT. Scalability, performance, memory- and power-limited devices, and constrained communication channels all contribute to the cryptographic challenges associated with the IoT. Many of these same issues cross all current cryptographic techniques requiring change. Current encryption keys have a “fixed” length. Fixed Keys can be identified, making them easier to crack. Key transfer is detectable and predictable. Other crypto systems require that keys are sent back and forth to users or computers. Other encryption systems store keys in central key deposits. Stored keys can and have been stolen. Key encryption methodologies must change to eliminate this weakness. PKI is also an expensive laborious process. Most PKI systems demand high CPU and memory overhead. .	Communications between collaborating applications contain parameterized machine-to-machine (or rather application-to-application) authentication handshake (challenge and response) in an exponentially large space (> 10 to the power 50,000). The space is not explored by the applications, but each message is known by our trade secret algorithms to be correct or not. We have two categories of such M2M authentications and multiple different authentication systems in each category. The proposed change does not send or store encryption keys (making the keys no longer subject to interception and theft and eliminating PKI overhead, risks and costs). Hackers additionally cannot identify the encryption key by its size. The proposed change offers an efficient minuscule footprint of 58 KB Low Overhead Platform and a 284 KB Embedded Encryption Platform. Many encryption offerings require large CPU and memory real estate. Critical nodes may be left at risk due to lack of available space. The proposed change satisfies restricted memory requirements and saves money. utilizing existing hardware. This is facilitated using existing systems and configurations.