Infineon

December 5th, 2013

National Institute of Standards and Technology
Information Technology Laboratory
ATTN: Adam Sedgewick
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899-8930
csfcomments@nist.gov

Subject: Comments to the Preliminary Cybersecurity Framework
Executive Order 13636, Improving Critical Infrastructure Cybersecurity

Dear Mr. Sedgewick:

Infineon Technologies North America Corp. welcomes the opportunity to provide comments to the preliminary framework developed by NIST in partnership with a wide range of private sector stakeholders. Infineon is a global semiconductor developer and manufacturer of security technology products supporting the government, finance, health, transportation and automotive sectors. In particular, Infineon provides technologies for authentication, identification, secure communications and secure storage. Securing data flows and transactions through Hardware Roots of Trust (HRoT) is a core competency for Infineon. We work today with government and private sector partners to secure critical infrastructure systems from cyber attack and look forward to continued engagement in this sector.

The structure of the preliminary framework – core, profile and implementation tiers – is strong and well supported both by international standards, and by NIST special publications such as ISO/IEC27001, NIST SP 800-53,SP800-34, and NIST SP 800-39.

Additional considerations for the framework that Infineon believes would strengthen security include:

1. Use of standardized and interoperable communication protocol and test/validation procedures already adopted by industry in place of proprietary protocols and testing methods. So, by adopting widely-used protocols, such as the Internet Engineering Task Force (IETF) TLS, Secure/Multipurpose Internet Mail Extensions (S/MIME), IPSec, Security Content Automation Protocols (SCAP), the framework would enable interoperability, reduced testing and qualification efforts, and information exchange among stake holders.

2. Distinguish between legacy devices and new devices to modernize the grid. For new systems, state of the art security technologies designed in from initial development should be recommended to address cyber security issues, whereas for legacy systems pluggable security solutions (Ex: adding a new secure communication module to an existing meter) should be recommended.

3. Leverage known and proven Cyber security solutions already deployed in other industries, such as secure authentication and encryption protocols currently used in the payments industry and the electronic passport. This will reduce the efforts required for defining and implementing solutions and increase interoperability.

4. Strongly recommend and foster the use of standard NIST-approved algorithms for all the cryptographic methods, key lengths and modes, instead of use of deprecated algorithms/key lengths and modes. As per NSA's Cryptographic Interoperability Strategy (CIS), select a set of NIST-approved cryptographic techniques, known as NSA Suite B, which recommends usage of AES with keys sizes of 128 and 256 bits for encryption, ECDH for key exchange, ECDSA for digital signature, SHA-256/384 for Hashing. This will enable entities to implement scalable security across a wide spectrum of devices and systems in critical infrastructure.

5. For the devices and systems used in critical infrastructure, the Framework should strongly recommend the following best practices which will enable entities to establish trust on the devices/systems connected to the network, quickly identify the rogue devices/systems and isolate them from the network, and control the authorized firmware/configuration updates:

   - Infrastructure should have the ability to track the lifecycle phase of all the physical devices connected to the infrastructure network, locally or remotely, such as device development, production, initialization/configuration, installation, maintenance and revocation.

   - Devices connected to the network should establish trust through cryptographic mutual authentication using asymmetric cryptography.

   - Each device connected to the network should have unique identifier and its hardware root of trust is embedded in a secure storage area protected from physical and logical attacks such as a low cost hardware security module (HSM), which acts as root of trust and to enforce security policies.

   - Software/configuration updates for the devices used in infrastructure should be done in a secure way using cryptographic mechanisms and through secure channel and appropriate access conditions.

- Always protect the device's Data-at-Rest and Data-in-Motion using encryption mechanisms. Also need to protect data leak from the device.

- Devices should always have a secure and trustworthy audit logging mechanisms which will provide for authenticity of data for instances of real-time or post attack forensics.

All these are standard non- proprietary and best practices successfully used around the world in different sectors such as PC/Payment/ Pay TV.

Infineon strongly supports the preliminary Framework document as constructed and proposes additional security measures for inclusion. A key measure for successful implementation of the Framework within the government and outside the government will be the use of proven standards and interoperability protocols, proven algorithms, and best practices from existing deployments in security-enabled sectors.

I would be happy to provide more detailed explanations or answer any questions about our above recommendations.

Sincerely,

Jörg M. Borchert

Joerg Borchert
Vice President
Chip Card and Security ICs
Infineon Technologies North America Corp.