infineon

April 8, 2012

Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899
cyberframework@nist.gov

**RE: Developing a Framework to Improve Critical Infrastructure Cybersecurity
Docket Number 130208119-3199-01**

Dear Ms. Honeycutt,

Infineon Technologies welcomes the opportunity to provide comments on NIST's preliminary Framework to improve cybersecurity for critical infrastructure as part of the implementation of the President's Executive Order on Cybersecurity.

Infineon is a global semiconductor company providing security solutions for markets protecting sensitive information through secure encryption technology. These markets include government identity documents, financial transactions, transportation transactions, broadcast content, and computing platforms. Each of these markets require scalable, interoperable, technology-agnostic, global, and open cybersecurity standards in order to operate effectively in the dynamic electronic environment of information flows in the world today. Establishing a like environment for critical infrastructure cybersecurity standards is necessary to create interoperable products and competitive markets.

Infineon's security business unit conducts extensive research into attack scenarios and extensive product development to thwart attacks far into the future. In this highly dynamic threat environment, Infineon has deep experience in understanding attack vectors, defining attack scenarios and designing solutions to mitigate and prevent intrusions. We offer our comments as a leading supplier of cybersecurity technology, an ongoing participant in the Smart Grid Interoperability Project Cyber Security Working Group, and an active leader in other security technology work groups.

As a part of these comments on a broader Cybersecurity framework, Infineon strongly endorses the process and outcome of the Smart Grid Interoperability Project Cyber Security Working Group, in the form of the NISTIR 7628. These guidelines addressing cybersecurity strategy, architecture, high-level security requirements, data privacy and analyses and reference documents are a crucial tool for a diverse electric power sector to design their own cybersecurity strategies. The public-private partnership, and its broad array of stakeholders, produced detailed security recommendations which may be used as a reference/foundation in structuring the cybersecurity Framework for broader sectoral use.

Infineon supports the preliminary goals for the Framework development process as outlined in the NIST RFI. It is important that the Framework promote usage of basic common testing methodologies, and qualification and certification processes across all sectors to enable vendors to build cost effective/interoperable technologies and products which can be used by different sectors.

Goal 1:

To identify existing Cybersecurity standards, guidelines, frameworks, and best practices that are applicable to increase the security of critical infrastructure sectors and other interested entities;

As a participant in the SGIP 1.0 CSWG subgroup process which brought critical stakeholders together to identify existing standards and existing gaps in standards, prioritize standards for adoption, and lay out a roadmap for additional standards, Infineon strongly supports the first goal in the NIST cybersecurity Framework. It is an efficient and effective process to adapt the work done by some of the standards bodies, industry workgroup alliances and forums who have already deployed cybersecurity solutions globally in financial, personal identification, and transportation sectors, among others.

Some standards groups to look to in this exercise include:

- Smart Grid groups such as SGIP CSWG , NESCOR, OpenSG-SG Security
- ISO/IEC standards group has done significant work on developing security frameworks, cybersecurity standards, implementation/certification/metrics guide lines for financial, energy, telecom, network, health, industrial control systems and identification sectors. Much of this work can be referenced at the following link: http://www.iso27001security.com/index.html.
- **NIST SP 800 standards** . : http://csrc.nist.gov/publications/PubsSPs.html
- Common criteria : http://www.commoncriteriaportal.org/
- ANSI- *American National Standards Institute,* BSI - British Standards Institute, BSI = Bundesamt fur Sicherheit in der Informationstechnik
- NERC CIP Cyber Security Standards

- Trusted Computing Group: http://www.trustedcomputinggroup.org/
- EMVCo: http://www.emvco.com/
- Global platform : http://www.globalplatform.org/
- ISO7816: http://www.cardwerk.com/smartcards/smartcard_standard_ISO7816-4_5_basic_organizations.aspx#chap5_2
- NRECA:Guide to Developing a Cyber Security and Risk Mitigation Plan

Goal 2:

To specify high-priority gaps for which new or revised standards are needed;

From Infineon's perspective, the main gap that needs to be filled is the absence of collaboration among key stakeholders in engineering, research, and IT – groups that have been working separately on these issues.

Supervisory Control and Data Acquisition (SCADA), Distributed Control (DCS) and/or Process Control (PCS) systems, referred to generally as an Industrial Control System (ICS), have legacy systems with proprietary technologies, implementation and test / qualification methodologies. Interoperability of these type of systems on a critical infrastructure network becomes very challenging.

ICS vendors use proprietary protocols for inter-process communications, which were developed when the devices were used in standalone mode and not built for operating over a TCP IP network. Many of these proprietary and industrial protocols lack any means of authentication or integrity checking, and some industry protocols are published with information freely available on the Internet. With ICSs no longer isolated from the corporate/IT world, these insecure protocols put the systems at risk of a cyber attack.

Specifically some issues that need to be addressed in this newly vulnerable environment are:

- The corporate and ICS networks should not communicate directly, all corporate communications into and out of the ICS network should be brokered through a functional DMZ or other mitigating architecture.
- Critical infrastructure owners need to build a proactive security model instead of a reactive one.

- Currently most of the testing is black box testing which may hide some of the vulnerabilities and so we need to encourage white box testing.
- The end point devices lacking strong security are a potential threat to critical infrastructure. Those devices need to authenticate to the network cryptographically and they should have a tamper proof root of trust mechanism.

An example of a standards gap that does not adequately address these vulnerabilities is:

- SEP 2.0: Supporting only certain Algorithms/modes/keylengths (No RSA). Restricting usage of high secure technologies. WIB2.0: IEC 62443-2-4

Goal 3:

To collaboratively develop action plans by which these gaps can be addressed. It is *contemplated that the development process will have requisite stages to allow for continuing* engagement with the owners and operators of critical infrastructure, and other industry, academic, and government stakeholders.

Infineon welcomes the opportunity to offer further information regarding implementation of the Framework process as the process moves forward, and encourages NIST to use its convening authority to bring the operators of critical infrastructure together with the experts from the technology and other sectors.

Current Risk Management Practices: As a security products vendor to various sectors, Infineon provides answers to the below questions not only from its own operational experience but from dialogue with a wide variety of customers.

1. **What do organizations see as the greatest challenges in improving Cybersecurity practices across critical infrastructure?**
   a. Scalability
   b. Huge magnitude of infrastructure
   c. Heterogeneous network
   d. Return on Investment
   e. Distinguishing operational control system security from IT security

2. **What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure?**
    a. Standards are developed in small groups (silos)
    b. Hard to find people who have both critical sector operational knowledge and security knowledge
    c. Lack of consensus in standard development bodies, which delays the release of standards
    d. Simultaneous work of different groups on same topic resulting in huge number of same or similar standards

3. **(RFI #12) What role(s) do or should national/international standards and organizations that develop national/international standards play in critical infrastructure cybersecurity conformity assessment?**

    1. International bodies should work together and leverage the work already done and establish a mechanism to resolve the conflicts and develop a interoperable standards for implementation in a timely manner.

    2. Establish a global testing and certification standard across all sectors.

Infineon is pleased to contribute its experience to the NIST process for developing a Framework to improve critical infrastructure cybersecurity. We welcome any follow up questions and look forward to future participation with the process.

Sincerely,

Joerg Borchert
Vice President
Chip Card and Security ICs
Infineon Technologies North America Corp.
640 North McCarthy Blvd
Milpitas, CA 95035