From: **Subramanian, Suresh**
Date: Mon, Apr 10, 2017 at 1:26 PM
Subject: iconectiv Comments on Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity
To: "cyberframework@nist.gov" <cyberframework@nist.gov>
Cc: "Drake, Chris", "Tucker, Louise M"

To Whom It May Concern:

Attached are the comments filed on behalf of iconectiv for the NIST Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity.

best regards,

suresh

**Suresh Subramanian, Ph.D.**
VP – Global Industry Relations
iconectiv
444 Hoes Lane | Piscataway, NJ | 08854

[Attachment Copied Below]

**BEFORE THE**
**DEPARTMENT OF COMMERCE AND NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY**
**Washington, D.C. 20554**

| | |
|---|---|
| **Request for Comments** | **)** |
| | **)** |
| **NIST Proposed Updates to the** | **)** |
| **Framework for Improving Critical** | **)** |
| **Infrastructure Cybersecurity** | **)** |
| **Version 1.1 (Draft)** | **)** |

## COMMENTS OF TELCORDIA TECHNOLOGIES, INC. D/B/A ICONECTIV

Telcordia Technologies, Inc.,[1] doing business as iconectiv ("Telcordia" or "iconectiv"), files these comments in response to the NIST revised draft to the Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1).

## BACKGROUND

iconectiv, headquartered in the United States, develops market-leading solutions that enable operators to interconnect networks. The company`s solutions are used by more than 1,200 service providers, regulators, enterprises, and content providers worldwide. iconectiv is also the global leader in providing numbering solutions and most recently was designated by the U.S. Federal Communications Commission to serve as the Local Number Portability Administrator in

---

[1] Since February 14, 2013, Telcordia, a wholly owned subsidiary of Ericsson, has been doing business as iconectiv.

the U.S. As such, iconectiv has a unique cybersecurity perspective in that it develops and maintains critical infrastructure products and services.[2]

iconectiv has been using the NIST Cybersecurity Framework ("CSF" or "Framework") since it was released. It is both voluntary and flexible. It has become a critical cybersecurity risk management guide to help assess the current cybersecurity profile of a business and the associated risks derived from its own people, technology and processes. NIST has an important and evolving role in expanding existing cybersecurity subject areas and incorporating critical risk components into the Framework. This draft revised version 1.1 contains new material on integrated risk management, cyber supply chain and metrics. All of these expanded and new areas are critical components of an enterprise risk profile. These new areas of the revised draft provide additional guidance in applying the Framework to a given business as appropriate, managing the risk through people, technology and processes and using metrics to determine effectiveness and the need for adjustments. We appreciate the opportunity to submit comments on the revised draft Framework.

## DISCUSSION

### Management and Access Control

iconectiv supports the clarified and expanded definition of "authentication" and "authorization". The guidelines should link identity management with access control credentials and privileges. We also agree with the concept of "identity proofing". As part of the user registration process the identity of the user should be verified, as well as for appropriate

---

[2] iconectiv's LERG, TRA, Number portability clearinghouse and the NPAC are critical infrastructure.

transactions. The rigorousness of the verification process depends on the nature of the application, its supporting operating environment and relevant threats. Being a framework, NIST should likely refrain from further levels of detail in this body of work and focus on the relevant Special Publications for that.

**Threat Intelligence**

The use of cyber threat intelligence from internal and external sources is mentioned in a few areas. iconectiv agrees that this element provides valuable input into achieving more accurate risk management decisions, timely incident responses and remediation. However, even with the addition of different information sharing forums and mechanisms there are still major issues that need to be addressed to maximize their value in risk management and key activities such as Supply Chain Risk Management (SCRM). Major issues include the intermingling of relevant and irrelevant information, the lack of critical infrastructure sector specific (e.g., telecommunications use cases) threats and vulnerabilities and the confidence level of the intelligence information. All of these factors reduce the effectiveness and value of this component and increases the need for continued development of appropriate processes and technology to ensure timely, relevant and actionable information.

**Supply Chain Risk Management**

iconectiv has considerable experience in cyber supply chain risk management ("SCRM") and the wide variety and sizes of suppliers, products and services procured to support a typical enterprise, its internal business operation and the externally-focused functions and customer

services. The assessment of the supplier itself and its products and services to determine risks and acceptable ways to manage risks continues to be complex and challenging. We agree that the SCRM category belongs in the Identify Function. The Subcategories also identify security assessment processes, contractual requirements and enforcement and ongoing monitoring and testing.

There are other key components that should be emphasized in the framework such as product lifecycle management. There are updates and patches that are issued by the supplier to address operational and functionality problems and provide new features. It is critical that an effective and ongoing risk management process be established to vet these changes and ensure the proper handling of them with integrity controls before they affect production.

Supplier business operations may change over time due to many things including acquisitions, ownership changes, and changes in business and marketing strategies. Monitoring the supplier's business and operational environment may create the need to re-evaluate the supplier and lead to changes in the enterprise's risk management approach Changes in the supplier's development, integration, testing and technical support processes, need to be included into the controls framework discussion. Outside of the Framework, some attention on a standard and reliable way of managing supplier risk would be of substantial cross-sector benefit.

**Data Security**

The data security category has been changed to include different integrity verifications for software, firmware and hardware. This is a significant change in the Framework in terms of breadth and scope. For example, the use of anti-tampering technologies needs to be appropriately used by the enterprise and its suppliers to protect highly confidential data. The

different mechanisms should be linked to the different data types, actions and control artifacts to provide an organized way to apply the proper controls to address the risks.

**Measurements & Metrics**

Measurements and Metrics are complex topics to define, apply and interpret the analysis results. Organizations need to be able to calibrate the coverage and effectiveness of the actual controls against the threats and their risk management program and identify any weaknesses or gaps. Version 1.1 introduces the area and provides descriptive guidance, but appropriately leaves more prescriptive methods of how measurements should be done up to individual entities. Fundamental questions such as the goals of the measurements, key process and technical focus areas , executive and operational audiences, data sources, benchmarks and meaningful metrics needs to be understood in relation to the different types of existing and emerging telecommunications infrastructures, services and business objectives. The draft seems to indicate that the audience for cybersecurity measurements and metrics is externally focused. However, measurements and metrics should provide guidance for the internal senior management, risk managers, and the internal compliance functions. The measurements and metrics should support a voluntary self-assessment approach, and not some external purpose.

When describing measurements and metrics, the framework should include all key resources that have a bearing on the risk profile of the business and its suppliers. This includes the business priorities, people, processes, technology (e.g., hardware, software), and environments. The overall measurements process should also be further described, with the Implementation Tiers to provide the necessary guidance in applying it to the different types of businesses and operational and services' models.

## CONCLUSION

We commend NIST on its ongoing efforts to improve its voluntary and flexible Cybersecurity Framework. We urge NIST to revise its framework consistent with our foregoing comments, including due consideration on the level of detail appropriate for the Framework as opposed to other NIST Special Publications which may be more suitable as vehicles for various specific guidance. Above all, there is no one-size-fits-all solution to cybersecurity. The guidelines should therefore support a flexible and market-driven approach.

Respectfully submitted,

By:

Chris Drake
Chief Technology Officer
iconectiv
444 Hoes Lane
Piscataway, New Jersey
(732) 699-6800
www.iconectiv.com

Dated: April 10, 2017