**Before the**
**DEPARTMENT OF COMMERCE AND NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY**
**WASHINGTON, D.C. 20554**

|  |  |  |
|---|---|---|
| In the Matter of: | ) |  |
|  | ) |  |
| Views on the Framework for Improving Critical Infrastructure Cybersecurity | ) | **Docket No. 151103999-5999-01** |
|  | ) |  |
|  | ) |  |
|  | ) |  |
|  | ) |  |
|  | ) |  |

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

## BACKGROUND

Telcordia Technologies, Inc.,[1] doing business as iconectiv ("Telcordia" or "iconectiv"), is pleased to submit these comments in response to the NIST Request for Information on views on the framework for improving critical infrastructure cybersecurity.[2] A US-based company, iconectiv has been a major architect of the United States' telecommunications system since it was formed at the divestiture of AT&T in 1983. We have first-hand knowledge of the intricacies and complexities of creating, operating and securing the country's telecommunications infrastructure and have profound appreciation for the criticality of these systems. When the company was first created as a neutral, trusted, third-party company, it was for the purpose of meeting

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

[2] National Institute of Standards and Technology (NIST), Views on the Framework for Improving Critical Infrastructure Cybersecurity, 80 Fed. Reg. 76934 (Dec. 11, 2015)("RFI").

national security and emergency preparedness requirements[3] and to provide technical support in the "construction, operation and maintenance of local exchange networks.[4]

iconectiv now provides market-leading solutions, including number portability clearinghouses and databases, that enable operators to interconnect networks, devices, and applications critical to evolving the global telecommunications marketplace. In March 2015, the Federal Communications Commission conditionally approved the recommendation of the North American Numbering Council (NANC) that iconectiv serve as the next local number portability administrator (LNPA) of the Number Portability Administrator Center (NPAC).

In all that we do, cybersecurity continues to be a key priority at iconectiv as we look to protect our customers' sensitive information and our products and services. We are intrinsically involved in the cybersecurity discussions in the industry and are active participants in the CTIA Cybersecurity working group, ATIS Cybersecurity ad hoc Group and the Communications Sector Coordinating Council as subject matter experts in risk management, cybersecurity and critical infrastructure protection. We commend NIST for its major effort in creating the Cybersecurity Framework (CSF). We are applying the CSF as part of our risk management program and offer the following comments based on our experience thus far.

[3] See, United States v. Western Elec. Co., 569 F. Supp. at 1114 n.253 (citing Plan of Reorganization at 418-419.

[4] *Id.*

## DISCUSSION

### Experience with the Cybersecurity Framework

Using our experience in enterprise infrastructure risk management and critical infrastructure products and services we are capturing current and planned controls using the CSF functions, and the categories and sub-categories. Specifically, we have worked with the Framework core - addressing the five functions and the associated categories: profile-organizing appropriate functions and categories and sub-categories to the business, and the applications and services.

We believe that the major benefit of the Voluntary Risk Management Framework is that it can be applied to different business models, technologies and applications. It creates a uniform structure to characterize controls and identify residual risks, emphasizing outcomes and adaptation to evolving threats. It, appropriately, avoids revisiting privacy and other specific security controls already dealt with in other vehicles. It acknowledges that one risk management solution does not fit the variety of critical infrastructure providers and associated technologies and services.

As NIST develops its plans for the CSF, the Implementation Tiers should be considered for greater definition to identify the major risk elements that need to be addressed and help organizations define baseline and target tiers that align with their business context. Also, there is limited guidance in selecting the appropriate risk management profile for a given infrastructure or service as reflected in the variety of approaches noted in the Communication Security, Reliability and Interoperability Council (CSRIC) Working Group (WG4) efforts. There are key risk areas that are barely covered in the CSF (e.g., supply chain risk management) that will warrant attention once strategies and requirements for those topics are more fully developed. The CSRIC WG4 has also identified five major barriers that need to be addressed more effectively.

The CSF wisely avoids prescribing specific metrics which will naturally vary according to the mission and position of the organization. Nonetheless, the Framework has been helpful to us in reducing risk because it has helped raise awareness across the company and at the highest levels of management. It helps in sorting through the variety of commercial security standards and best practices and in identifying key applicable areas that need to be addressed by an organization.

**Regulatory Issues**

To "prevent duplication of regulatory processes and prevent conflict with or superseding of regulatory requirements, mandatory standards, and related processes" as required by the Cybersecurity Enhancement Act of 2014, we believe that it is important to maintain the Voluntary Risk Management Framework. It is also important to maintain the CSF approach at the federal level instead of having different sets of state and local security requirements. With threats, business models and technology constantly changing, NIST should continue to provide the appropriate cybersecurity guidance and best practices to address emerging risks. The CSF is considered a "living document" in terms of capturing lessons learned, applying them, and identifying areas that need further development to produce a robust risk management strategy. Cybersecurity is not static so the CSF needs to be viewed as dynamic and providing the structure for underlying standards and guidelines addressing technology innovations, new services and business and operations models.

Once more actionable materials have been developed in key areas such as the Supply Chain, System Development Life Cycle (SDLC) and synchronizing international cybersecurity standards, we believe that it would be appropriate for the CSF to be updated. As new standards and sector specific guidelines and practices are developed in the US and internationally, they need to be referenced in the CSF. For the communications sector this includes the International Telecommunications Union (ITU) and other standards and industry forums (e.g., Alliance for Telecommunications Industry Solutions (ATIS)). Continuous updating by including new standards will provide more guidance to organizations in addressing critical infrastructure risks by leveraging best practices. There are various industry groups that are providing best practices in specific risk areas and the CSF structure should capture these principles, in the future, to build the knowledge base for using the framework and utilizing the appropriate controls.

Thus, as NIST and the industry develop more insights and best practices in these areas they should be captured in the CSF. NIST should follow the highly successful collaborative process that they used for the first version of the CSF. This would keep the CSF in sync with new legislation, standards and technology innovations. As a relatively new framework, however, adoption efforts are at various stages of maturity across the industry and companies should be afforded the opportunity to stabilize their security approach based on the current version of the CSF.

NIST has a well-defined process for updating cyber risk management best practices, and controls for specific areas. The preferred approach is by soliciting industry inputs, creating drafts of the proposed changes, asking for feedback through the website and at meetings and then releasing the final document. Future changes adopted by this process will build upon the current CSF so current assessments should not be greatly impacted and disruption to current application plans should be minimized.

Currently, security practices are being shared across the government. Different industry players including service providers, suppliers and standards organizations share information within industry forums. We still need to recognize that the use of the term "best practice" can mean different things to different organizations and impact many dimensions such as cost, operations, end users, and others. The CSRIC WG 4 report identified major barriers that need to be constantly worked in the process.

To facilitate information sharing and best practices, the government needs to ensure that the voluntary approach to the CSF continues. Continuously sharing the best practices that various agencies create provides timely insights that allow stakeholders to implement best practices with agility. NIST and Department of Homeland Security (DHS) have various cybersecurity and critical infrastructure protection focused forums and programs that can be used to promote the sharing of best practices, experiences with the CSF, lessons learned and issues. The industry should be a collaborative partner with NIST in the evolution of the CSF.

**Transition of the CSF**

We believe that NIST is the appropriate organization to maintain leadership in the evolution of the CSF, promote security awareness and enable the ongoing cross-sector collaboration and voluntary government-industry partnership. NIST should also continue its coordination with the Department of Homeland Security's (DHS) critical infrastructure protection programs.

If a transition had to occur then the major elements of the NIST CSF and DHS National Protection and Programs Directorate (NPPD) programs will need to be re-established to continue the voluntary adoption of the CSF. If a transition had to occur, then the "new" organization needs to be an active player in critical infrastructure protection. This entails many elements including neutrality, appropriate technical skill-sets, domestic and international standards outreach and respect, the ability to coordinate across critical sectors and different business sizes and to manage the public-private partnership.

## CONCLUSION

We have found that the CSF is effective at incorporating key solution components, physical, logical, and personnel into the scope of what needs securing. We continue to look forward to working with NIST on its efforts to continuously improve the Cybersecurity Framework.

Respectfully submitted,

By: ________________

Chris Drake
Chief Technology Officer

________________

Michael Iwanoff
Chief Information Security Officer

iconectiv
444 Hoes Lane
Piscataway, New Jersey
(732) 699-6800
www.iconectiv.com

February 9, 2016