UTILITIES TELECOM COUNCIL

1129 20th Street | Suite 350 | Washington, DC 20036
202.872.0030 *Phone* | 202.872.1331 *Fax*
www.utc.org

October 9, 2014

Mr. Adam Sedgewick
U.S. Department of Commerce
1401 Constitution Avenue NW.
Washington, DC 20230

Re: Experience With the Framework for Improving Critical Infrastructure Cybersecurity

Dear Mr. Sedgewick,

Utilities Telecom Council (UTC) is pleased to submit this response to the Request for Information (ROI) Experience With the Framework for Improving Critical Infrastructure Cybersecurity in support of the efforts to facilitate adoption of the Cybersecurity Framework. Our response reflects input from UTC's municipal, cooperative and investor-owned utilities. As a utility trade association focused specifically on information and communications technologies, this response is based on UTC's cybersecurity programs and initiatives developed with guidance from utility members, industry members, and regulatory and academic stakeholders.

UTC has been an ardent supporter of NIST's efforts in the development and implementation of the Cybersecurity Framework both through our participation in the development of the Framework, and through our outreach to UTC members and the broader utilities community. UTC has implemented several training and assessment tools and initiatives to promote the implementation of the framework as a foundational element of critical infrastructure security.

UTC is looking forward to continue participating in the Cybersecurity Framework efforts through workshops, dialog, and other venues. If you have any questions about the content of this response, please do not hesitate to contact us.

Sincerely,

Nadya Bartol, CISSP, CGEIT
Vice President, Industry Affairs and Cybersecurity Strategist
202-833-6809
Nadya.bartol@utc.org

UTILITIES TELECOM COUNCIL

1129 20th Street | Suite 350 | Washington, DC 20036
202.872.0030 *Phone* | 202.872.1331 *Fax*
www.utc.org

UTC Overview

Founded in 1948, the Utilities Telecom Council (UTC) is a global trade association dedicated to being the source and resource for information and communications technology (ICT) solutions for utilities and other critical infrastructure industries. UTC brings a worldview with a regional focus as a market leader for utility telecommunications advocacy and education with members in the United States, Europe, Canada, Latin America, the Middle East, Asia and Africa.

UTC core members include utilities (energy, water, gas), pipelines and other critical infrastructure companies that operate mission-critical telecommunications and data networks in support of their core business operations. UTC's members include large investor-owned utilities that serve millions of customers across multi-state service territories, as well as relatively small rural electric cooperative utilities and municipal utilities that may serve only a few thousand customers each. UTC members also include providers delivering ICT products and services to utilities.

UTC focuses on practical solutions to technical challenges that confront its members. UTC's primary audience is the utility cybersecurity practitioner and the utility technology practitioner. A utility cybersecurity practitioner is someone who performs cybersecurity activities as a full time job and is a member of a cybersecurity organization within a utility. A utility technology practitioner is engaged in designing, acquiring, engineering, and maintaining a variety of utility systems and networks that enable delivery of essential services to the general public and businesses.

Cybersecurity may be a part of these individuals' responsibilities -- which makes them critical to utilities' ability to manage cybersecurity risks. However, these individuals are not full-time cybersecurity practitioners and are frequently not members of a cybersecurity organization within their respective utility. It should be noted that utilities have a great variety of cybersecurity governance models where not all utilities have formal cybersecurity organizations and designated cybersecurity practitioners. In those utilities utility technology practitioners perform cybersecurity functions as a part of their role. All of these individuals are the key target audience of UTC's outreach efforts with respect to good cybersecurity practices and the benefits of applying the Cybersecurity Framework.

UTC Outreach Activities in Support of the Cybersecurity Framework

UTC is committed to assisting our members improve and enhance their cybersecurity practices. This includes numerous outreach and knowledge sharing activities. Since the publication of the Framework UTC has worked extensively to increase awareness and use of the Framework among its members and the overall utilities community.

UTILITIES TELECOM COUNCIL

1129 20th Street | Suite 350 | Washington, DC 20036
202.872.0030 *Phone* | 202.872.1331 *Fax*
www.utc.org

UTC believes that to achieve the objective of the Framework to improve critical infrastructure cybersecurity the knowledge of the Framework and its application/use need to reach beyond cybersecurity practitioners within the critical infrastructure owners/operators. To achieve that goal, numerous leaders and practitioners within these organizations need to be aware of the Framework, including its benefits, intent, and how it is relevant to their organizations' success.

As a part of UTC Cybersecurity program of work, UTC has reached out to a broad group of utility executives, managers, and technology practitioners to increase awareness of the Framework and promote its use through our own events and publications, as well as speaking engagements at events hosted by groups other than UTC. UTC has also been an active participant in the development of the Energy Sector and Communications Sector Framework Guidance, mapping of Energy industry regulations to the Framework, and in the Prudent Cybersecurity Investments and Opportunities for Utilities Working Group.

The remainder of our response is structured according to the sections in the NIST RFI. We have taken the liberty of grouping questions where appropriate.

Current Awareness of the Cybersecurity Framework

Questions 1-4: Awareness of the Framework and Its Intent and How People Learn About It

Numerous associations, non-profits, and government agencies are putting a tremendous amount of effort into increasing awareness of the Cybersecurity Framework as a tool to help improve the cybersecurity of the national critical infrastructure. In the six months since the release of the Framework, the awareness of its existence has undoubtedly increased among utility cybersecurity practitioners and some technical practitioners who are not officially attached to a cybersecurity function within their utility. We believe that the next step is to expand awareness among utility executives, managers, and technical practitioners who are not engaged in daily cybersecurity activities.

The awareness of the Framework has definitely increased among UTC stakeholders, including utilities and utility technology partners. However, there are still numerous utility executives, managers, and practitioners that are not aware of the full value of the Cybersecurity Framework, or its potential impact on their organizations. Through UTC outreach to the utilities community we routinely conduct polls with respect to awareness of the Cybersecurity Framework. When speaking to a general utility audience of non-cybersecurity executives, managers, and practitioners, the awareness of the Framework is under 20%[1]. The picture is

[1] Both awareness percentages in this section are based on informal polling of the audience during speaking engagements as in "those aware of the Framework please raise your hand."

UTILITIES TELECOM COUNCIL

1129 20th Street | Suite 350 | Washington, DC 20036
202.872.0030 *Phone* | 202.872.1331 *Fax*
www.utc.org

different when the audience is focused on cybersecurity or the audience has been engaged in UTC cybersecurity activities – the latter two audiences are at least 70% aware of the Framework.

Utilities learn about the Framework from a variety of sources. Many of these sources are mentioned in Question 2 of the RFI. Additionally, consultants and legal experts are letting their clients know about the Framework and have productive conversations about its use and impact.

The Framework's voluntary nature is not uniformly known in the utilities space. While NIST and other US government agency officials have clearly communicated the Framework's voluntary intent, there are persistent concerns among the utilities community that the Framework will at some point become a de jure or de facto regulation.

There is also some confusion with respect to whether the Framework is yet another "stovepiped" set of activities that a utility must perform to achieve a certain compliance mandate. The questions and debates about the nature of the Framework (whether it is a new type of regulation that needs to be adhered to differently than existing regulations or standards and guidelines) are frequent. While many individuals engaged with UTC understand that the Framework represents a "plain English" way of articulating established concepts, this is not yet uniformly understood by all relevant stakeholders in the broader utilities community. Furthermore, it is not broadly understood that organizations that have consistently implemented existing cybersecurity frameworks, (such as ISO/IEC 27001) have already effectively implemented the Framework.

Some of the confusion and uncertainty associated with the meaning of the Framework should be resolved or at least reduced with the publication of sector-specific Framework implementation guidance. An example is the recently released Energy Sector Cybersecurity Framework Implementation Guidance. This document provides generic guidance on how to apply the Cybersecurity Framework in the energy sector. It also provides guidance for using the Energy Sector Cybersecurity Capability Maturity Model (C2M2) to implement the Framework. Appendix A provides a mapping of the Framework to C2M2 (which can be used for both the Electricity and Oil and Gas Subsectors of the Energy Sector).

It should be noted that the Electricity Subsector is somewhat unique in that many of its members are subject to North American Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards. Over the last 6 months UTC has answered questions from many members about how the Framework relates to NERC CIP, whether NERC CIP will be modified to accommodate the Framework, or whether utilities that are already compliant with NERC CIP need to implement the Framework. The resolution of this particular question will be helped by an ongoing industry-led activity to map the Cybersecurity Framework to NERC CIP. This mapping is a detailed spreadsheet that maps each Framework subcategory to individual NERC CIP requirements and provides additional implementation guidance. The mapping is planned for release in the Fall 2014.

UTILITIES TELECOM COUNCIL

1129 20th Street | Suite 350 | Washington, DC 20036
202.872.0030 *Phone* | 202.872.1331 *Fax*
www.utc.org

Questions 5 and 9: Challenges and Opportunities to Improve Awareness of the Framework

Utilities operate in a regulated and resource-conscious environment. Cybersecurity is a priority that competes for mind share with numerous others including reliability, safety of the general public and employees, and achieving regulatory compliance. Awareness of the Framework is only important inasmuch it advances the broader improvement of cybersecurity practices in critical infrastructure.

Participation and buy-in from individuals critical to cybersecurity but not focused on it on a daily basis in their jobs is required to achieve a noticeable improvement in cybersecurity, whether it is done through the Framework or not. These individuals include:

- Members of Boards of Directors
- Utility executives
- Technical managers and practitioners.

The cybersecurity challenge needs to be framed in a way that tells these individuals what they can do to help. This may need to be specific to each critical infrastructure sector, subsector, or segment.

For example, UTC has had numerous discussions with technical managers and practitioners about ensuring that cybersecurity communications are allocated sufficient bandwidth when new networks are designed and implemented. This means that security has become a functional requirement because in addition to the true functional requirements these networks have to support the dataflow required to achieve security requirements, such as encryption and multifactor authentication. Practical data about "how much bandwidth is needed for security" is difficult, if not impossible to find. Some solutions are better than others. It is likely that similar challenges exist in other critical infrastructure sectors. These questions demonstrate a significant shift in the content of cybersecurity conversation in the last 6 months to practical implementation challenges such as: How should I design my network to ensure I have enough bandwidth for security so that it does not impact availability and reliability of my communications and information. **Demonstrating how the Cybersecurity Framework can lead to a resolution of these technical and functional challenges would substantially increase its awareness among the non-cybersecurity practitioners in utilities.**

Another example is the auditing/financial consulting community's reluctance, observed by some UTC members, to transition or translate their activities to the Cybersecurity Framework. While cybersecurity is now included in annual financial audits, our members comment that these auditors are not familiar with this "new" framework, and rely on a much more complicated and lengthy assessment framework, which is more focused on the financial sector than utilities. This includes not only third party auditors but also internal auditors who are more familiar with

UTILITIES TELECOM COUNCIL

1129 20th Street | Suite 350 | Washington, DC 20036
202.872.0030 *Phone* | 202.872.1331 *Fax*
www.utc.org

COBIT and other governance or IT frameworks. **The auditing/financial consultant community represents an opportunity for Federal outreach and awareness on the value of using the Cybersecurity Framework. Increasing that community's awareness of the Framework will help critical infrastructure owners/operators further integrate and streamline their compliance activities.**

Finally, our members report that there is a disconnect in the area of risk assessment guidance, methods, and tools, especially with respect to using the Framework to integrate cybersecurity into overall budget planning and master planning. **Collecting and publicizing case studies for how this is done in other organizations (especially if organized by critical infrastructure sector), would be a powerful outreach tool.**

Other challenges are well known and have been articulated by many during the Framework development process. **They include costs of cybersecurity and availability of a qualified cybersecurity workforce that understands both cybersecurity and utility business and systems.**

Question 6: Global Awareness of the Framework

The international utilities community is interested in hearing about the Framework and how it may apply to their own environments. However, utilities in other countries are quite focused on their own cybersecurity directives, strategies, and frameworks, such as the ENISA Cybersecurity Directive.

Question 7: Is the Regulator aware of the Framework

Electric utilities are regulated at the Federal level by the Federal Energy Regulatory Commission (FERC). Utility wireless communications are regulated by the Federal Communications Commission (FCC). Utilities are also regulated at the State and Local levels by numerous regulators. Both FERC and FCC have been actively participating in the efforts to increase awareness of the Framework. The National Association of Regulatory Utility Commissioners (NARUC) has also been engaged in making its members aware of the Framework and its benefits.

Question 8: Your Organization's Outreach Activities and Plans

UTC is committed to providing cybersecurity outreach, awareness, and education on cybersecurity risk management to its members and to other utilities and utility ICT providers. Below is a summary of UTC efforts focused specifically on the outreach and awareness of the Framework. IT should be noted that UTC's cybersecurity outreach, awareness, and education are much broader than the Framework and encompass numerous technical cybersecurity topics as well as cost-effective access to premier cybersecurity education and training opportunities.

UTILITIES TELECOM COUNCIL

1129 20th Street | Suite 350 | Washington, DC 20036
202.872.0030 *Phone* | 202.872.1331 *Fax*
www.utc.org

1. UTC conducts monthly UTC Security Committee meetings where the members receive updates on the work of the Framework and available US government cybersecurity resources for the utilities such as DHS C^{3}Program
2. UTC invited numerous US government cybersecurity experts to participate in its plenary executive policy maker panel and in two security track panels at the UTC TELECOM 2014 in May 2014 – UTC's annual conference – to discuss the NIST Cybersecurity Framework and available US government cybersecurity resources.
3. UTC also invited US government cybersecurity experts to participate in the UTC Canada Annual Conference in September 2014 to discuss a variety of US national cybersecurity efforts including the NIST Framework
4. UTC held a publicly available webinar to mark the Framework release in February 2014
5. UTC presented on the NIST Cybersecurity Framework at several events attended by over 3,000 individuals working for utilities and utility ICT providers. At least 60% of these individuals are not cybersecurity practitioners.
6. UTC is planning to hold a "year in review" public webinar October 16 2014 to continue increasing awareness among the utilities and utility technology partners of the benefits that the Framework provides.
7. UTC provided regular updates on the Framework and related US Government and industry activities in its weekly publication, UTC Intelligence sent to over 6,000 individual UTC members working in utilities or utility ICT provider organizations.
8. UTC has provided regular updates in its quarterly publication, the UTC Journal, sent to over 6,000 individual UTC members on the development and progress of the Framework. UTC also published several articles dedicated to the Framework, what it means for utilities, and how the Framework relates to utility cybersecurity practices, in the UTC Journal.

UTC plans to continue awareness and outreach activities with its membership and the overall utilities community.

Experiences With the Cybersecurity Framework

UTC has had numerous conversations with member utilities about their use of the Cybersecurity Framework and other cybersecurity standards and guidelines. There is no overarching pattern yet of how the Framework is used or lessons learned from the Framework application.

UTILITIES TELECOM COUNCIL

1129 20th Street | Suite 350 | Washington, DC 20036
202.872.0030 *Phone* | 202.872.1331 *Fax*
www.utc.org

Roadmap for the Future of the Cybersecurity Framework

Questions 1 and 2. Roadmap Enhancements

We believe that the focus should be gradually shifting from raising awareness to providing practical knowledge of what the use of the Framework actually means to the individuals on the ground. The earlier example of utilities seeking practical information on the network requirements for security represents a practical outcome of cybersecurity as a functional requirement rather than an add-on after the fact. The Roadmap could facilitate development of approaches and methods for identifying similar functional requirements and directing efforts to find answers to those practical questions.

Question 3. Recent National and Global Developments

Supply Chain Risk Management is one of the Areas for Development, Alignment, and Collaboration articulated in the NIST Roadmap. A key standard in that space has been finalized since the publication of the Framework and is now available for use globally. International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27036 – Information Technology – IT Security Techniques – Information Security for Supplier Relationships, is a 4-part standard dedicated to the practice of managing risks associated with supplier relationships. Part 3, ICT Supply Chain Security, was publicly available at the time of the Framework release. Since then Parts 1 and 3 of this standard, Overview and Concepts and Requirements have been finalized and are now publicly available. Part 4 (that addresses cloud services) is still under development but it heavily leverages Parts 1-3 (http://www.iso.org/iso/search.htm?qt=27036&sort_by=rel&type=simple&published=on&active_tab=standards). Global availability of standards that address establishing supplier relationships with security in mind helps advance one of the objectives of the Framework to facilitate a productive dialog on security among acquirers and suppliers.

Nationally, a key document that addresses the same challenge in the energy utility space developed by an industry expert group was finalized and released by the Department of Energy. The document is Cybersecurity Procurement Language for Energy Delivery Systems (http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014). Availability of this document for the Energy Sector acquirers and suppliers helps advance the same objective in the Energy Sector.

Finally, existence of these documents, both globally and nationally, helps advance the importance of supply chain risk management across critical infrastructure owners/operators and their technology partners.