October 10, 2014
Submitted electronically to cyberFramework@nist.gov

Comments of the Communications Sector Coordinating Council

Re: "Experience with the Framework for Improving Critical Infrastructure Cybersecurity"

This letter is submitted by the Communications Sector Coordinating Council (CSCC) in response to the Request for Information (RFI) to gauge the level of awareness and initial experiences regarding the National Institute of Standards and Technology (NIST) Cybersecurity Framework released on February 12, 2014.

As previously indicated in the CSCC response to the initial April 2013 NIST RFI, the Communications sector has a long history of security planning and operations in partnership with government. Historically, the sector collaborated through the National Security Telecommunications Advisory Committee and the National Coordinating Center for Telecommunications, which to this day are still in full effect. While the Communications Sector Coordinating Council (CSCC) is the most recent partnership, it has already made significant contributions in promoting the protection of the networks and information systems throughout our sector.

The CSCC is comprised of five segments including broadcast, cable, wireless, wireline, and satellite and represents over 40 organizations including service providers, equipment manufacturers, and trade associations. Our sector is one of 16 Critical Infrastructure/Key Resource (CI/KR) sectors and the Council has played a major role in the year-long process to develop the Framework and is actively engaged in subsequent activities to adapt the cross-sector Framework to our five segments and to promote the awareness and use of it as a voluntary and flexible cybersecurity risk management tool.

The CSCC acknowledges the significant contribution that NIST has made, and continues to make, through its facilitation of collaborative activities to advance our nation's cybersecurity posture. There is much evidence that the Framework has spurred a national conversation around cybersecurity policy and risk management activities at the sector and enterprise levels. By providing a common taxonomy that enables organizations to communicate needs and expectations to both internal and external stakeholders, and by promoting a voluntary, flexible, and enterprise-specific approach, the Framework can become a cornerstone for national and global collaboration and coordination.

The RFI asks for comments in areas related to awareness and experience with the Framework as well as future Framework related activities. Our comments are intended to communicate sector participation in a variety of events and venues and to provide some perspective regarding the key areas of inquiry.

The CSCC and its members have been actively following developments and issues related to the

Framework since its release almost nine months ago and we continue to engage in a variety of activities to promote awareness across our industry segments. The CSCC Cybersecurity Committee holds weekly calls with industry participants to coordinate, among other things, planning activities related to Framework activities across multiple public and private venues. Since the release of the Framework in February 2014, CSCC members participated in multiple events to promote awareness including sponsoring webinars, association forums, and key speaking engagements at various policy venues. The Communications sector has been consistently invited to participate on NIST workshop panels and has been invited to participate in the upcoming October workshop to be held in Tampa Florida.

Perhaps the most significant Framework-related sector engagement is currently underway at the FCC Communications Security Reliability and Interoperability Council (CSRIC IV) where Working Group 4 is working to adapt the NIST Cybersecurity Framework to the five segments that make up our sector. Currently, there are more than 100 professionals working to evolve aspects of the Framework that were not part of the initial Version 1.0 deliverable. The CSRIC effort includes segment-specific assessments of critical infrastructure and the essential services that depend on the associated systems and assets. The segments have developed an analytical Framework to evaluate and prioritize risk management practices and they are developing use cases that can serve as a guide to individual enterprises as they consider the applicability of the Framework to their operating environments. Separate, but related work streams are underway to consider the current threat environment, the nature of the ecosystem, the unique considerations of small and medium enterprises, the barriers and challenges to using aspects of the Framework, and consideration of indicators that can be used over time to evaluate progress. Once this effort is completed and recommendations are submitted and voted on by the CSRIC in March 2015, the sector will continue its work with the appropriate stakeholders to advance the goals of the Executive Order and the NIST Cybersecurity Framework.

Given the sector's active participation in this development work within the CSRIC, we expect sector enterprises will evaluate relevant, cost-effective findings, perspectives and recommendations for applicability into their business operations. Having said that, the CSCC is aware that many sector companies have already begun an evaluation process that in most instances involve examining how the Framework fits into their current cybersecurity risk management regime. In some cases, companies are just starting to familiarize themselves with the Framework's guidelines and standards, while for other companies the Framework is a smaller sub-set of more expansive and comprehensive risk management programs.

With respect to future NIST efforts to develop areas identified in the Roadmap, the CSCC is ready to engage in further discussions to advance these efforts and to ensure that key foundational principles so critical to the early success of the Framework development are retained and buttressed. The significant levels of sector resources committed to these activities are highly correlated to the expectation that the Framework will not become a precursor to regulation and unfunded mandates. We are encouraged that NIST and other government officials have publicly rejected the notion of a checklist- type regime in favor of industry-led market-based solutions.

We are also aware of the need to foster an environment of shared responsibilities where the entire ecosystem can be convened to address sector-specific interdependencies. For that reason, we encourage the Department of Commerce to initiate an Internet Security Task Force as a follow-up to the June 2011 inquiry and Green Paper "Cybersecurity Innovation and the Internet Economy." It would be our expectation that representatives across federal, state, local and tribal government and across sectors with increasingly converging characteristics (i.e., "I3S" or "Internet and Information Innovation Sector" as described in Green Paper) can assemble and collaborate on cybersecurity issues of broad national and International concern.

On behalf of the Communications Sector Coordinating Council members, we once again state our appreciation to NIST for undertaking this vital national initiative and we look forward to continuing our active engagement in these pursuits.

Sincerely,

Kathryn Condello	**T. Brooks Fitzsimmons**	**Andy Scott**
CenturyLink	AT&T	NCTA
Chair	**Vice Chair**	**Secretary**

Communications Sector Coordinating Council