



April 8, 2013

Docket No. 130208119-3119-01

Submitted electronically to cyberframework@nist.gov

Comments of the Communications Sector Coordinating Council

Re: *“Developing a Framework to Improve Critical Infrastructure Cybersecurity”*

This letter is in response to the Request for Information on how to improve the critical infrastructure cybersecurity posture of the nation and what role the Communications sector, one of 16 Critical Infrastructure/Key Resource (CI/KR) sectors, can play in support of this initiative.

The Communications sector has a long history of security planning and operations in partnership with the 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 within our sector.

The Communications industry is continuously evolving its cybersecurity capabilities, innovating new technologies and offering new services throughout a vast, global network. The interconnected nature of the business has fostered a long history of cooperation and collaboration among the wireline, wireless, cable, satellite and broadcast segments. We have been and remain focused on addressing the risk management practices that support the country's national security and emergency preparedness needs.

The development of the 2005 DHS's National Infrastructure Protection Plan (NIPP) was the first major contribution of the CSCC, and laid the foundation for the partnership between industry and the designated government Sector Specific Agency (SSA). Consistent with the NIPP, a Sector Specific Plan (SSP) for Communications was developed between the partners. It provided a comprehensive risk management framework, outlined the sector goals, risks, whether joint mitigations programs were required, and defined the respective roles of government and the private sector in supporting those programs to enhance the protection of the sector's assets and services.


A key component of the sector's risk management framework is the development of a sector-specific, National Sector Risk Assessment (NSRA). This assessment acts as the foundation for the sector's protection and resiliency activities. The 2008 NSRA helped inform government and industry stakeholders of higher priorities and assisted with baseline risk across the sector.

The 2012 risk assessment comprehensively assessed logical/cybersecurity, physical and human scenarios, and identified the potential consequences in light of current protective measures. The findings and recommendations from the 2012 NSRA are leading the private and government sector partners to work together to reduce risk through steady-state planning and implementation of joint programs.


Given the sector's long history of collaborating with the government on security planning and operations, the Communications Sector Coordinating Council believes it is in a good position to help promote how the frameworks, guidelines and best practices developed in this process are reflected in Communications Sector practices.

Thank you for the opportunity to participate in the NIST activities as together we develop a cross-sector baseline Framework to reduce risk to critical infrastructure.

Sincerely,



Rosemary Leffler
Chair
Communications Sector
Coordinating Council



Kathryn Condello
Vice Chair
Communications Sector
Coordinating Council



Mike Alagna
Secretary
Communications Sector
Coordinating Council