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

RE: IT SCC Response to NIST Request for Information for Experience with the Framework for Improving Critical Infrastructure Security

Dear Mr. Sedgewick:

The Information Technology Sector Coordinating Council (IT SCC) is pleased to submit our response to the National Institute for Standards and Technology's (NIST) Request for Information (RFI) seeking information from industry on their experiences with the Framework for Improving Critical Infrastructure Cybersecurity.

The IT SCC was established in January 2006 for the purpose of bringing together stakeholders from across the IT Sector, including owner operators and representative trade associations, to coordinate strategic activities to help improve the security and resiliency of the IT Sector and the cybersecurity of other sectors.

Since the IT SCC's inception we have undertaken several efforts as a Sector to understand and collaborate with the government to mitigate national-level risks to the not just the IT Sector, but the nation's critical infrastructure as a whole. For 2014, the IT SCC established a set of priorities to strategically guide and inform our activities. One of those priorities was to understand how the Cybersecurity Framework is being considered by our members, and we are sharing the following thematic observations in response to the RFI.

First, awareness of the Framework is high among those who provided input; it should be noted that observations are from organizations that have "self-selected" to contribute, and those organizations may be more aware of activities and initiatives than those organizations that did not respond. Based on anecdotal information, awareness of the Framework outside of organizations directly involved with the government is considerably lower. In general, awareness of the Framework is slowly happening, but it is too early to characterize the situation.

Second, organizations are continuing to evaluate the Cybersecurity Framework, both with respect to organizational risk management practices, as well as in interactions with customers and vendors. Regarding organizational risk management, there are organizations that had existing practices in place similar to those in the Cybersecurity Framework; these organizations do not necessarily rely on the Framework itself, but already have robust risk management approaches in place that are based on or similar to the outcomes and international standards described in the Framework. Other organizations are using the Framework to review or assess their risks, and some are changing/adapting their practices to incorporate some practices identified in the Cybersecurity Framework. Finally, some organizations are observing initial impressions and watching how the Framework process unfolds. While a few organizations may consider the Framework in interactions with their customers and vendors, it is not regularly part of discussions.

Third, IT SCC members noted that more time is needed to understand the potential impacts of the Cybersecurity Framework, particularly among those organizations that are not engaged in U.S. public policy activities on cybersecurity. A few IT SCC members noted the need for broader awareness and exchange among the membership, and expressed interest in exploring if and how we might foster an ongoing, progressive exchange of experiences among the SCC membership related to the policy initiatives resulting from the Executive Order.

Many IT SCC members continue to believe that there remain two significant gaps in this effort that if more extensibly addressed, may contribute to greater awareness of the Framework as a toolbox to assist in identifying standards, measures, and best practices to improve their cybersecurity risk profile. First, IT SCC members look forward to the implementation of a comprehensive and sustained national education and awareness campaign that would focus on how stakeholders can improve their basic, fundamental cyber hygiene that would thereby improve their cyber risk profile. Secondly, IT SCC members would look forward to a continued discussion about the economics of cybersecurity and how the Framework can be an important resource in efforts to align security and business needs with available resources to improve an organization's cyber risk profile.

Finally, IT SCC members continue to support the voluntary, risk-based, outcome-focused, and flexible approach of the Cybersecurity Framework. This approach enables a diversity of critical infrastructure sectors and organizations all with unique business challenges, varying risk tolerances, and complex technological environments to adapt in light of the dynamic, ever-changing cyber threat environment.

IT SCC members note that the Framework is an evolving document, and are encouraged by the open, inclusive process NIST has used to solicit input into efforts associated with the Cybersecurity Framework. We welcome the opportunity to continue to work with NIST and the industry partners on efforts to advance the cybersecurity of critical infrastructures. Please contact Angela McKay, Chair of the IT SCC if you have any questions or would like additional information.

Sincerely,

Angela L. McKay

Angela McKay
Chair, Information Technology Sector Coordinating Council