On behalf of the Information Technology Sector Coordinating Council (IT SCC), we appreciate the opportunity to provide comments on the preliminary version of the Cybersecurity Framework (Preliminary Framework) to the National Institute of Standards and Technology (NIST). We value the open, collaborative process conducted by NIST developing the Preliminary Framework, and contributed to that process in numerous ways. The IT SCC responded[1] to the NIST's Request for Information "to help identify, refine, and guide the many interrelated considerations, challenges, and efforts needed to develop the Framework" in April of this year, and many SCC member companies did as well. IT SCC leadership and members also participated in all five of NIST's workshops to help develop the Framework.

We view these comments as part of the ongoing dialogue and engagement with NIST to develop and refine a Final Framework, and, eventually to update and refine the Framework based on lessons learned. We also consider this effort within the broader context of implementation of the Executive Order (EO) on cyber security and Presidential Decision Directive (PDD) on security and resilience of critical infrastructures, both issued in February 2013. We continue to engage and contribute across the full range of efforts (e.g., cyber dependent infrastructure identification, incentives, procurement, information sharing) being driven through the Interagency Task Force.

We look forward to continuing to work with NIST and our industry colleagues in other sectors to help finalize the Framework and work on related efforts to help to improve cyber security of critical infrastructures.

The IT SCC

The IT SCC was established in January 2006 for the purposes of bringing together companies, associations, and other key IT Sector participants on a regular basis to coordinate strategic activities and communicate broad sector member views associated with infrastructure protection, response and recovery that are broadly relevant to the IT Sector.

The IT SCC has considerable experience with cyber risk management efforts, as corporate entities managing risks for ourselves and our customers, and as a sector collaborating with the government to assess and manage national-level risks to the IT Sector[2].

The IT SCC response to the NIST request for comments on the Preliminary Cybersecurity Framework addresses three topics: the degree of alignment with the guiding principles from our April 2013 response to the Request for Information; sectoral considerations for use[3] of the Framework; and the importance of establishing a governance process that integrates lessons learned from any use into future iterations of the Framework and related policies and initiatives.

---

[1] http://csrc.nist.gov/cyberframework/rfi_comments/040813_it_scc.pdf

[2] IT Sector Baseline Risk Assessment http://it-scc.org/documents/itscc/IT_Sector_Risk_Assessment_Report_Final.pdf.
Risk management strategies http://it-scc.org/viewdocs/index.php.
Domain Name Resolution Services Function Risk Profile. Provided upon request; please contact the SCC officers.

[3] IT SCC comments on the Preliminary Framework briefly discuss "use" of the document, but do not take a position on organizational or sector implementation or adoption of the Framework. This is discussed more in sectoral considerations

Alignment with IT SCC recommended guiding principles

The IT SCC suggested the Framework must have defined specific security objectives; include a complete and repeatable risk-based approach for assessing and prioritizing cyber risks to critical infrastructure; ensure maximum flexibility for critical infrastructure owners and operators in their efforts manage risks using security outcomes and global, consensus-based standards; and be domestically and internationally relevant.

- Defined Security Objectives. The IT SCC suggested that "government and private sector must have a clear and common view on the desired security objectives(s) the Framework is seeking to achieve," and suggested that there were at least two distinct, but related, security objectives to consider in the context of improving the cyber security of critical infrastructure: baseline cyber security, or "cyber security hygiene," and more significant, or "greatest" cyber risks presented by advanced threats. The Preliminary Framework states it "provides guidance to an organization on managing cybersecurity risks," but does not as clearly define the security objective(s) it is seeking to advance within these organizations.
- Risk-based. Entities, including those who own or operate are critical infrastructure, have differing business models and changing technology infrastructure, and each faces a unique risk landscape. As such, the IT SCC suggested that "the Framework must recognize that risk profiles, risk tolerance, and resources to manage risks will – *and should* - differ across sectors and within sectors' functions, for critical infrastructure." The Preliminary Framework highlights the importance of risk management and explicitly acknowledges variations in business models and risks, and risk tolerance.
- Flexible. In the IT Sector's experience, mandating specific practices and driving universal and consistent application is not an effective approach to cyber risk management. The IT SCC suggested that "the Framework must establish desired outcomes and identify relevant global standards that are cost-effective and may help to achieve those outcomes, rather than defining a list of specific standards, controls, or measures that must be applied." The security focused guidance in the Core of the Preliminary Framework is founded on outcomes and references broadly recognized international standards; the cost effectiveness of the approach is not yet clear.
- Domestic and International Relevance. The IT suggested it was " it is essential that the Framework to define risk assessment and management approaches and standards that advance not only the interests of the United States, but also functions as an example of how to improve cyber security while maintaining and promoting innovative open markets for the benefit of all. Leveraging global standards will provide value beyond the border of the United States and the companies who operate here, and will help sustain free-trade environment." The Preliminary Framework includes broadly recognized global standards, and we believe that maintaining this approach will increase the likelihood that the Framework, once in use, could fulfill the intent of this principle.

The IT SCC's RFI response also discussed attributes for national-level approaches to assess and manage critical infrastructure cyber security, but since the Preliminary Framework focuses on organizational risks, those concepts are not as applicable.

Sectoral considerations for use of the Framework

The IT Sector is a globally distributed, diverse, and ever changing. Our six critical functions[4] represent countless, varied, and evolving sub-functions provided by small, medium, and large organizations that operate in and serve various domestic and international markets. The diversity of IT sector is one of our key strengths, providing rich and varied perspectives to inform and shape organizational, national, and international efforts to advance cyber security. Within the IT SCC we have a common vision of a secure, resilient, and protected global information infrastructure that can rapidly restore services if affected by an emergency or crisis, ensuring the continued and efficient function of information technologies, infrastructures and services for people, governments, and businesses worldwide. We work collaboratively with government and industry partners to improve cyber security and the security and resilience of critical infrastructures.

Implementation or "adoption" of the Framework is a topic of considerable and ongoing discussion within the IT Sector and in other sectors, and interpretations vary. The diversity of the IT Sector, including different perspectives on concerns associated with use, may limit sector-wide efforts to foster or drive use of the Framework; it is more likely that individual organizations and/or communities of shared interest may determine if and how the Framework may be relevant for their consideration and use. Regardless of interpretations, the IT Sector broadly agrees that for Framework to be meaningful, it will need to be used, analyzed, and improved.

Ongoing Governance

As stated in our April 2013 RFI response, we agree that the Framework must be a "living document…to address constantly evolving risks to critical infrastructure cybersecurity."[5] We believe that NIST must work with industry to establish an effective governance process for the Framework, that:

- Encourages government to share information that can inform and incent organizations' risk management activities consistent with the Framework's desired outcomes,
- Provides flexibility for critical infrastructure organizations to modify or augment suggested standards as they deem necessary to manage dynamic cyber risks,
- Fosters and enables exchange among the critical infrastructure community,
- Incorporates lessons learned to improve the document and the associated efforts, and
- Is sustainable, including appropriate resourcing to support the necessary evolution of the approach over time.

Our hope is that the Framework evolves and matures to be meaningful, relevant, and useful in our shared efforts to improve the cyber security of critical infrastructures.

---

[4] The IT Sector's six critical functions are: Producing and providing IT products and services; Providing incident management capabilities; Providing domain name resolution services; Providing identity management and associated trust services; Providing Internet-based content, information and communications services; and Providing Internet routing, access, and connections services.

[5] https://www.federalregister.gov/articles/2013/02/26/2013-04413/developing-a-framework-to-improve-critical-infrastructure-cybersecurity.