On behalf of the Information Technology Sector Coordinating Council (IT SCC), we appreciate the opportunity to provide input to the National Institute of Standards and Technology (NIST) to its Request for Information (RFI) concerning a Framework for Improving Critical Infrastructure Cybersecurity (the Framework). We agree that the Framework must be a "living document…to address constantly evolving risks to critical infrastructure cybersecurity."[1] We look forward to further working with NIST and our industry colleagues in other sectors to help develop a Framework that improves cyber security of critical infrastructure in the near-term, and defines a construct to assure the necessary collaboration with stakeholders, through the Critical Infrastructure Partnership Advisory Committee (CIPAC), to innovate and advance cyber security of critical infrastructures over time.

I. Introduction to the IT SCC and our role in cyber security

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 Sector envisions 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.

The IT Sector has considerable experience with cyber risk management efforts. As corporate entities, we face numerous multifaceted global threats from natural and manmade events, including cyber threats, on a daily basis, but these events most often do not have significant consequences because of individual entities' existing security and response capabilities. The same is true for the critical infrastructure owners and operators in other sectors: most events are managed successfully and do not result in significant consequences.

As a sector, we have undertaken several efforts to understand and collaborate with the government to mitigate national-level risks to the IT Sector, including developing and publishing the IT Sector Baseline Risk Assessment[2] in 2009 and five risk management strategies[3] in the 2011, and updating and publishing the Domain Name Resolution Services function risk profile[4] in 2012. These efforts are discussed further in section III. We have examined operational and policy considerations, and capabilities associated with response to a significant cyber incident through exercises, such as the CyberStorm Exercise series. Finally, we have participated in, and contributed to, numerous policy and operational initiatives, such the National Infrastructure Protection Plan (NIPP), the National Strategy for Trusted Identities in Cyberspace, the International Strategy for Cyberspace, and the Obama Administration's 60-day Cybersecurity Policy Review, with Federal agencies, including the Departments of Homeland Security, State, Defense, and Commerce, to manage risks to critical infrastructure.

IT Sector products and services are integrated into and enable functions for have a wide variety of customers - including consumers, small businesses, mid- to large-size enterprises, and governments – around the world. Each of these customers, including those who own or operate are critical

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

[2] http://it-scc.org/documents/itscc/IT_Sector_Risk_Assessment_Report_Final.pdf

[3] http://it-scc.org/viewdocs/index.php

[4] Provided upon request; please contact the SCC officers

infrastructure, have differing business models and changing technology infrastructure, and each faces a unique risk landscape. Leveraging commercial technologies enables all customers to benefit from advanced hardware, software, and services at lower reduce costs and to take advantage of new features and security innovations. IT companies work directly with critical infrastructure owners and operators to understand their risks, and also engage at a national-level through the Cross-Sector Cyber Security Working Group.

We view our response to this RFI as initiating an ongoing dialogue and engagement with NIST throughout development of the Framework, and its implications within broader context of implementation of the Executive Order (EO) and Presidential Decision Directive (PDD) related to cyber security. For example, IT Sector representatives are engaged and participated in NIST's recent workshop on the Framework, and will be represented in the three workshops being planned. We are also trying 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 Forces. We see these efforts as fundamentally related, though the timelines and sequencing of activities may make developing and harmonizing them to optimize the outcomes difficult. We welcome an opportunity to meet and discuss our RFI response directly with NIST and DHS, and to develop a regular cadence for engagement among the IT SCC, NIST, and DHS so that we can actively support many of the strategic priorities outlined in the EO and PDD.

II. Scope of IT Sector Response to the NIST RFI

The IT Sector response to the NIST RFI primarily focuses on:

1) Guiding principles that should be included in the Framework to underpin national efforts to enhance cyber security;
2) Best practices to help assess and prioritize critical infrastructure cyber risks; and
3) Aggregate effect of private and public sector risk management on cyber security and resiliency of the nation's critical infrastructures.

The IT Sector response does not speak to nor is it intended to define what comprises "critical infrastructure" or "critical infrastructure at greatest risk," or provide guidance for individual organizations' risk management. Rather, our hope is that the Framework can shape national efforts to improve the cyber security of critical infrastructures, and create greater visibility and coerce government to share information that can inform and incent organizations' risk management activities consistent with the Framework's desired outcomes.

III. Guiding Principles for the Framework

The IT SCC believes the Framework must have defined specific security objectives; include a complete and repeatable risk-based approach, which considers consequences, vulnerabilities, and threats, 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.

<u>Defined Security Objectives.</u> Successful risk management efforts first begin with defining objectives the effort is seeks to achieve. In the context of improving the cyber security of critical infrastructure (i.e.,

that infrastructure which supports national and economic security, public health and safety), there are at least two distinct, but related, security objectives to consider:

- Advancing baseline cyber security, or "cyber security hygiene," broadly across all critical infrastructures; and
- Managing more significant, or "greatest" cyber risks presented by advanced threats with the intent to cause "catastrophic" effects.

It is impossible for individual organizations to defend against every possible threat or to account for every permutation of every possible vulnerability, particularly considering the dynamic nature of cyber threats. Government and private sector must have a clear and common view on the desired security objectives(s) the Framework is seeking to achieve, including the nature of the threats of concern, in order to structure risk assessment and management activities that most effectively leverage and optimize the impact of the capabilities and investments of each.

We must also understand that "greatest" cyber risks to critical infrastructure cannot be eliminated, only managed. Attempts by Government, sometimes working with industry, have been made and are currently underway to define the subset of critical infrastructure "at greatest risk" to a cyber incident. To date, these efforts have not been successful as stakeholders have struggled trying to apply traditional risk management approaches to a dynamic and interconnected infrastructure with rapidly evolving risks. Government needs to do better working with industry to perform an actual risk assessment to define the subset of critical infrastructure "at great risks", and section IV of this response provides the foundation for the approach that more appropriate for cyber risk management.

Risk-based. The basic formula for risk defines it as a function of threat, vulnerability, and consequence. Threat and vulnerability combined represent the likelihood that a vulnerability could be exploited successfully by a threat. The IT Sector believes that consequence is an appropriate initial factor to understand criticality, but that a complete risk-based assessment is required to identify critical infrastructure that could "reasonably result" in "catastrophic effects".

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 and the yet to be defined "critical infrastructure at greatest risk". Because limited resources exist to manage cyber risks, it is important that public and private sector security partners agree on how to best prioritize risks and apply resources. A complete risk-based approach will prioritize concerns, and help focus the individual and collective expertise and resources of government and industry where they will be most effective and complementary.

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. One-size fits all approaches fail to appreciate differences in unique business models, risk profiles, and resources and expertise between and within sectors. It also doesn't work for the dynamic nature of cyber threats; flexibility and agility are essential when managing cyber risks. On a practical level, this means 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. Specific controls and measures may face difficulty in cross-sector implementation and would be outpaced by cyber threats.

Domestic and International Relevance. The IT SCC has a unique, global perspective on potential impact of the Framework. Our sector is inherently international in nature, with customers, including small, medium, and large businesses, and operations located in nearly every country around the world. There is increasing interest among governments on improving cyber security, and we anticipate that the Framework will be studied closely by other countries seeking a template to develop similar measures.

As such, 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.

IV. Attributes of a Approach to Assess and Manage Critical Infrastructure Cyber Security

While risk management is a well understood discipline in some environments, managing cyber risks is dynamic and ever-evolving. Cyber risks are complex and changing, and efforts to improve security and resilience must not hinder innovation and agility. Risk management is the appropriate discipline with which to approach these challenges, but how that discipline is applied must evolve, leveraging insights gained through experience, to better address the unique nature of cyber risks.

Through our individual corporate risk management efforts and the sector's efforts managing cyber security, we have demonstrated that the following best practices are effective in guiding efforts to identify and prioritize cyber risks, and that such an approach can produce meaningful, actionable outcomes. We look forward to working with our colleagues in other sectors, who have also undertaken various efforts on this topic, as we work collectively to manage cyber risks.

- **Rely on Actual Subject Matter Experts**: The importance of private sector subject matter expertise to assess and management cyber risks using consistent, objective, and defined criteria cannot be overstated. Only with active engagement of the owners and operators who design, develop, implement, configure, manage, and maintain sectors' critical functions can any effort to identify or prioritize critical infrastructure cyber risk be valid.

- **Leverage Functions-based approach**: The highly diverse, virtual, interconnected, and international nature of cyberspace and the constantly evolving threat landscape limit the effectiveness of traditional asset-based approaches to critical infrastructure identification. In our experience, approaches that focus on understanding infrastructure functions (the full set of processes involved in transforming supply inputs into products and services) rather than cataloging physical fixed assets, to be more effective. For some sectors, particularly those with widely varying modalities (e.g., transportation) it may also be helpful to decompose critical functions into the component operations and processes (e.g., research and development [R&D], manufacturing, distribution, upgrades, and maintenance) that are part of the value chain for each function.

- **Assess and Prioritize Risks; criticality can be based on consequence, but risk includes likelihood**
  Functions' criticality can be assessed based on their potential impact on government or sectors' missions, *independent of any specific defined threat scenario*. A function's criticality depends on many factors, such as tolerable magnitude and duration of loss or degradation, resilience, and

the likelihood of cascading consequences, if other functions are highly dependent on the affected one. The purpose of utilizing a top-down approach to criticality is to identify those functions that meet a minimum consequence threshold based on these criteria. Resources can then be devoted to assessing cyber risks to nationally consequential functions and their supporting infrastructure.

Cyber risks result from a full spectrum of manmade (intentional and unintentional) and natural threats. Threat and vulnerability combined represent the likelihood that a vulnerability could be exploited successfully by a threat. While traditional threat analysis generally identifies an actor and the actor's intentions, motives, and capabilities to compromise a given target, such approaches typically rely on historical data, current intelligence, and analysts' speculation associated with a particular actor to predict threats.

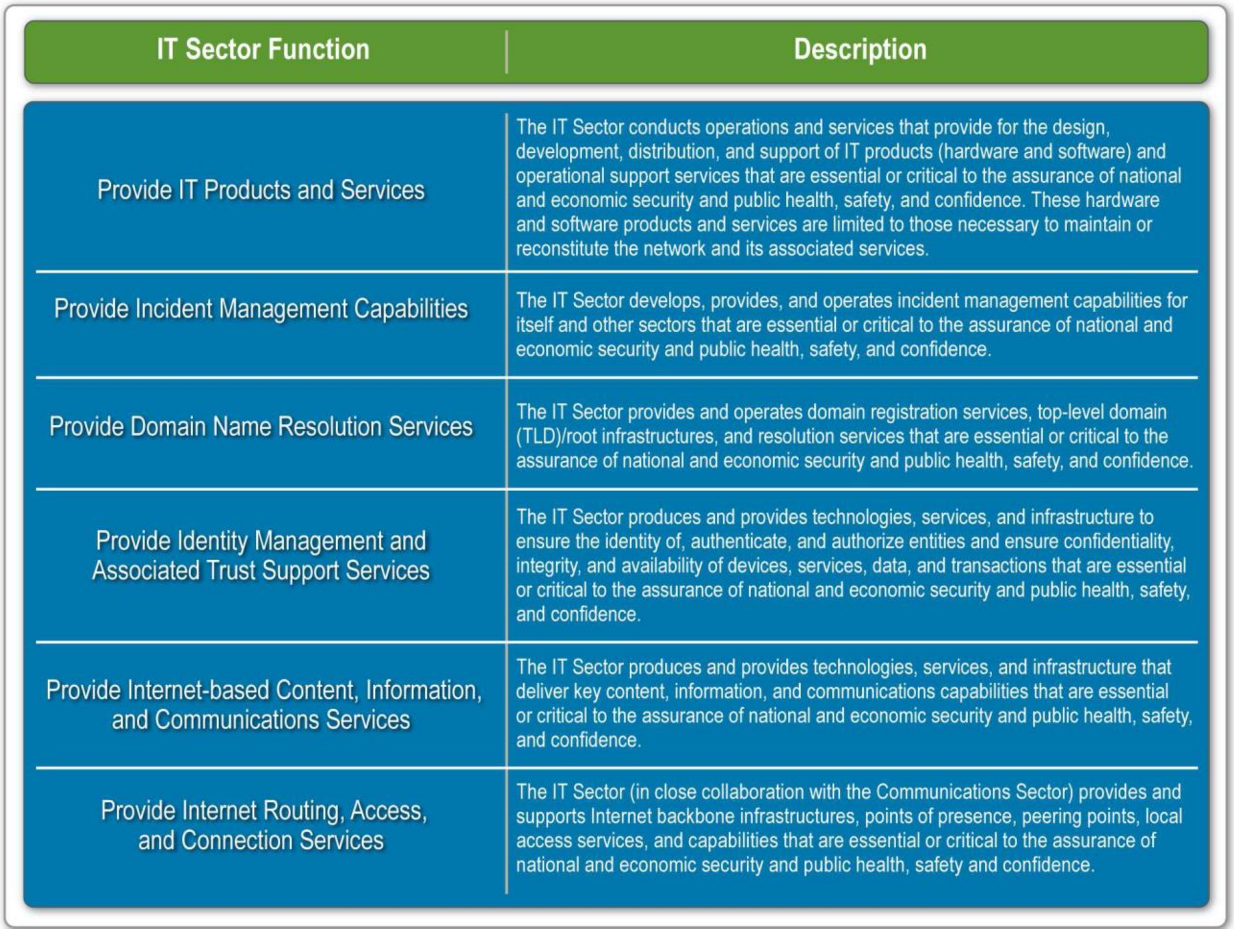
When analyzing cyber threats, this traditional approach alone is not sufficient because actors are not easily identifiable or traceable, and attacks—deliberate or unintentional—can go from conception to exploitation within hours. When considering cyber risk, we suggest complementing traditional threat assessment by including additional factors based on capabilities and intent independent of known actors to consider emerging non-traditional threats.

- **Account for Existing Mitigations:** Absolute risk typically refers the risk to a function if there were no mitigations in place, while residual risk is the risk that remains considering mitigations. Effective risk management requires a complete view of consequences, vulnerabilities, and threats, and includes identifying and assessing existing mitigations that may reduce those factors. Certain risks may be acceptable today, but threats and vulnerabilities often change quickly, and only a complete understanding of risk—both absolute and residual—provides opportunities to manage dynamically.

- **Optimize for Agility**: Understanding what critical infrastructure cyber security and the risks that infrastructure face is important to help apply and optimize the effectiveness of limited resources. We caution, however, that attempting to develop or maintain lists of critical cyber infrastructure and checklists of controls would be impractical and have little to no value. Specific systems and technologies change regularly and rapidly, as do the threats facing them, so by the time lists are developed and defined controls implemented, they would already be out-of-date and ineffective. Instead of trying to identify specific systems, their owners, or controls, an alternative and more effective approach would be to leverage the functions-based approach, value chain analysis, and consequence assessment to identify categories of systems that may be of interest, and then continue working with sector representatives to understand how those categories of systems support critical functions, and their risk profiles. Cyber risk management must also be dynamic, and regularly re-evaluated to account for the dynamic nature of both technologies and cyber threats.

Functions-based risk management in IT Sector

Six critical functions support the sector's ability to produce and provide high assurance IT products and services for various sectors. These functions are required to maintain or reconstitute networks (e.g., the Internet, local networks, and wide area networks) and their associated services. They represent consensus of the IT SCC and IT Government Coordinating Council (GCC) on critical functions vital to national and economic security and public health, safety, and confidence. These functions are distributed across a broad network of infrastructure, managed proactively, and therefore, can withstand and rapidly recover from most threats.



IT Sector Function	Description
Provide IT Products and Services	The IT Sector conducts operations and services that provide for the design, development, distribution, and support of IT products (hardware and software) and operational support services that are essential or critical to the assurance of national and economic security and public health, safety, and confidence. These hardware and software products and services are limited to those necessary to maintain or reconstitute the network and its associated services.
Provide Incident Management Capabilities	The IT Sector develops, provides, and operates incident management capabilities for itself and other sectors that are essential or critical to the assurance of national and economic security and public health, safety, and confidence.
Provide Domain Name Resolution Services	The IT Sector provides and operates domain registration services, top-level domain (TLD)/root infrastructures, and resolution services that are essential or critical to the assurance of national and economic security and public health, safety, and confidence.
Provide Identity Management and Associated Trust Support Services	The IT Sector produces and provides technologies, services, and infrastructure to ensure the identity of, authenticate, and authorize entities and ensure confidentiality, integrity, and availability of devices, services, data, and transactions that are essential or critical to the assurance of national and economic security and public health, safety, and confidence.
Provide Internet-based Content, Information, and Communications Services	The IT Sector produces and provides technologies, services, and infrastructure that deliver key content, information, and communications capabilities that are essential or critical to the assurance of national and economic security and public health, safety, and confidence.
Provide Internet Routing, Access, and Connection Services	The IT Sector (in close collaboration with the Communications Sector) provides and supports Internet backbone infrastructures, points of presence, peering points, local access services, and capabilities that are essential or critical to the assurance of national and economic security and public health, safety and confidence.

As noted earlier, the IT SCC and Government Coordinating Council completed the IT Sector Baseline Risk Assessment,[5] which characterized the risk profile of the six critical IT Sector functions using an analytic, criteria-based risk methodology, and provided a foundation for protective measures and R&D priorities. Concepts and lessons learned from the IT Sector risk methodology and assessment also became a foundation for DHS' Cyber Assessment Risk Management Approach, which has been applied successfully in other sectors. In 2011, the IT SCC published five risk management strategies,[6] which included policy,

[5] http://it-scc.org/documents/itscc/IT_Sector_Risk_Assessment_Report_Final.pdf

[6] http://it-scc.org/viewdocs/index.php

operational, and technical mitigations to help manage risks identified in the Baseline Assessment. In 2012, we updated the risk profile for the Domain Name Resolution Services function,[7] to consider how new Internet technologies, security standards, and governance practices have affected that function's risk profile.

Critical Infrastructure at Greatest Risk

As currently framed, DHS' efforts to identify critical infrastructure at greatest risk (associated with Section 9 of the EO) is improved relative to prior efforts. For example, officials leading the Cyber-Dependent Infrastructure Identification Working Group have begun to consider functions-based approaches, and understand that narrow threat-driven national planning scenarios must be augmented by additional threat analysis. Yet, the tendency to use more familiar, static approaches and traditional thinking—for example to focus on consequence only and "assume" both vulnerability and threat—jeopardizes the validity of the effort.

To identify critical infrastructure where a cyber incident could "reasonably result" in catastrophic effects, an assessment of both the consequences and likelihood of an event being successful and causing those effects must be considered. These efforts should start with a clear, shared understanding of the consequences that constitute catastrophic effects, but understanding these is only the first step; the process must then assess "reasonable" likelihood.

When considering likelihood, it may be defensible to assume vulnerability, since cyber security experts generally agree that a determined adversary with sufficient resources can almost always attack a system successfully, especially by using social engineering techniques. However, the factor that often elevates critical infrastructure to critical infrastructure at "greatest risk" is the threat presented by more advanced actors with more malicious intent (i.e., to affect national security or public safety). As such, assuming threat when trying to identify and manage critical infrastructure at greatest risk will not work.

The language in section 9 related to "commercial IT products and consumer services" is generating considerable discussion within the IT Sector and in other sectors, and interpretations vary. Regardless of interpretations, the IT Sector broadly agrees that that language in the EO does not mean IT Sector does not own or operate critical functions, as noted above, or have a role in helping to improve the cyber security of other critical infrastructures. As a sector, we also agree that critical infrastructure "at greatest risk" should be narrowly defined with particular consideration made to assure it does not hinder commercial innovation (in the IT Sector and in other sectors) or the open, global marketplace.

V. Private and Public Sector Risk Management

Risk management approaches used throughout the IT Sector are based on various philosophies, methodologies, and tools. Private sector entities typically base their approaches on business objectives, such as shareholder value, efficacy, and customer service. Enterprise-level risk management approaches usually involve cyber security initiatives and practices to maintain the health or "hygiene" of information security programs and infrastructures. Examples of these actions include physical vulnerability mitigation measures (e.g., physical access control and surveillance); human vulnerability mitigation measures (e.g., employee screening and security training and awareness); cybersecurity measures (e.g.,

[7] Provided upon request; please contact the SCC officers

encryption; behavior monitoring and management technologies; independent third-party security posture assessments); and business continuity planning.

As part of their individual risk management approaches, many IT Sector entities have designated focal points for risk management and/or security. Some have chosen to centralize this function within their organizations while others have chosen to have it distributed across their operations. In addition, IT Sector entities assess various types of risk (e.g., financial, human, supply chain, legal, and compliance) through multiple approaches (e.g., quantitative, qualitative, and modeling and simulation) leveraging both commercial and government off-the-shelf products and customized tools. These entities use a variety of common risk management frameworks to proactively manage steady-state risk.

Private sector entities implement a vast array of mitigations primarily based on their organizational objectives, whereas public sector interests are focused on assuring the sectors' functions to support the economy and national security. Individual risk management efforts are designed to support organizational objectives but—in aggregate—they also enhance the security and resilience of the critical infrastructure sectors. Understanding how existing public and private sector risk mitigations work together to address risks collectively and identifying additional capabilities is an essential component of the critical infrastructure cyber security. By increasing the awareness of national level concerns more broadly the organizations that provide these functions, the private and public sector can help enhance the security and resiliency

VI. Recommendations

NIST should consider the following recommendations to inform ongoing development of the Framework:

- Designate two IT Sector representatives, with subject matter expertise in cyber risk management, to the Framework Development Interagency Task Force
- Facilitate cross-work group collaboration between the integrated task forces groups leading cyber dependent infrastructure identification and Framework development, including to help define desired security objective(s) of the Framework and what constitutes "catastrophic effects", "reasonably result", and "at greatest risk", and to create clear alignment with how those terms apply to elements of the Framework
- Explore international standardization of a functions-based national cyber risk assessment methodology, building on the experience of the IT Sector and other sectors
- Facilitate as much substantive cross-sector interaction as possible, for example during the planned NIST RFI workshops, to help identify an appropriate cross-sector baseline approach for the Framework itself
- Develop sector specific and small and mid-size compendiums to Framework to account for differing risks and scalability between and within sectors, and to enable flexibility

NIST should include the following items in the Framework

- A clearly stated view on the desired security objectives(s) the Framework is seeking to achieve
- Approach for identification of critical infrastructure and critical infrastructure at greatest risk reasonably like to cause "catastrophic effects" that appropriately risk-based and builds on the work of the IT Sector and other sectors

- Desired security outcomes and potential globally relevant global standards that are cost-effective and may help to achieve those outcomes across sectors
- Approaches that help organizations to assess and manage cyber risks dynamically and encourages and enables them to modify or augment suggested standards as they deem necessary to manage dynamic cyber risks