From: **Ola Sage**
Date: Mon, Apr 10, 2017 at 5:12 PM
Subject: IT Sector Coordinating Council Response to NIST Draft Cybersecurity Framework Version 1.1
To: "cyberframework@nist.gov" <cyberframework@nist.gov>

The IT Sector Coordinating Council is pleased to submit our response to Draft Version 1.1 of the Cybersecurity Framework.

Please contact me directly for questions or comments.

Kind regards,

Ola

Ola Sage, PMP®, CRISC
CEO, e-Management, CEO, CyberRx
Chair, IT Sector Coordinating Council

www.e-mcinc.com
www.cyber-rx.com
www.it-scc.org

[Attachment Copied Below]

Submitted by:
Ola Sage, Chair
Information Technology Sector Coordinating Council (IT SCC)
April 10, 2017

Introduction

The Information Technology Sector Coordinating Council (IT SCC) is pleased to submit our response to the National Institute of Standards and Technology's (NIST) Request for Comment (RFC) seeking feedback and input on the Cybersecurity Framework draft Version 1.1. The IT SCC commends NIST for its open and inclusive process, enabling a broad range of stakeholders to be involved in development efforts of the Cybersecurity Framework to date. Since its release in 2014, the Cybersecurity Framework has been used on a voluntary basis by organizations of all sizes and industries inside and outside the U.S. The Framework has also been positively received internationally by foreign governments such as Canada, the United Kingdom, Australia, and Italy to name a few.

The IT SCC welcomes the opportunity to provide input on the draft Version 1.1 that can help guide NIST's efforts in facilitating coordination with, "private sector personnel and entities, critical infrastructure owners and operators, and other relevant industry organizations" as directed by the Cybersecurity Enhancement Act of 2014. The following responses are informed by input from our IT SCC members who represent a broad base of owners, operators, associations, and other entities—both large and small.

IT SCC Comments

NIST Question #1) Are there any topics not addressed in the draft Framework Version 1.1 that could be addressed in the final?

IT SCC Comment: One of the main strengths of the CSF is the flexibility it offers organizations to determine what categories and subcategories are important within their organizations based on risk tolerance and cost effectiveness. Recognizing that successful implementation of the Cybersecurity Framework is ultimately based on achievement of outcomes described in an organization's target profile and not on Tier determination, there continues to be misperception and a lack of clarity about the use or value of implementation Tiers. The addition of Cyber Supply Chain Risk Management to the Tier descriptions adds complexity to Tier designation. Added complexity risks organizations moving away from making decisions based on a risk management approach to a compliance-based checklist application of Tiers based on a maturity model, such as CMMI. NIST might consider removing implementation Tiers as a "core" component of the Framework, leaving it to each organization to apply Tier-like requirements to their individual or industry Framework Profiles.

NIST Question #2) How do the changes made in the draft Version 1.1 impact the cybersecurity ecosystem?

IT SCC Comment: The IT SCC believes that at a macro level, the improvements and additions (e.g., supply chain, metrics, measures, access control) in Version 1.1 are necessary and timely; however maintaining flexibility in the application for organizations will be critical to continued use and

adoption of the Framework. The proposed changes could significantly impact the cybersecurity ecosystem primarily through the introduction of supply chain risk. This risk extends the scope beyond most organization's field of sight. While larger organizations are most likely already addressing this risk and have that ability due to their size and budgets, many small organizations may not have the resources to explore those risks.

The changes could also impact the ecosystem through the usage of cybersecurity measurements. The newly introduced concepts of metrics and measurements can help organizations better define improvements they would like to make to their cyber programs. Additionally, it can help them communicate these improvements throughout their enterprise, which would help extend the security message to other areas of any organization. The IT SCC cautions that it is important for organizations to preserve flexibility in the application of any metrics/measurements. Different organizations face unique threat environments and have different assets, risk tolerances, resources and business priorities. They will weigh individual Framework subcategories outcomes differently, which should be reflected in metrics/measurements.

NIST Question #3) For those using Version 1.0, would the proposed changes impact your current use of the Framework? If so, how?

IT SCC Comment: IT SCC members are using the Framework in a variety of ways and in some cases have published use cases describing how the Framework is being implemented within their organizations. Depending on how organizations define their current and target profiles, it is possible that the introduction of the proposed changes in Version 1.1, particularly around supply chain risk management and metrics/measurement could require additional resources to appropriately address the increased scope. For small and mid-size businesses (SMBs) the complexity may be an added deterrent as these organizations may not have the resources to address those types of issues.

NIST Question #4) For those not currently using Version 1.0, does the draft Version 1.1 affect your decision to use the Framework? If so, how?

IT SCC Comment: The IT SCC does not currently have objective data on members who are not using Version 1.0. However, as part of a joint IT Sector initiative with the Department of Homeland Security, the IT SCC will be conducting a survey of small and mid-size companies to learn if companies are using the Framework or not, and if not, why not. Data from this survey will be important to understanding how future versions of the Framework may be accepted or used by the SMB community, as well as shedding light on whether the Framework is cost-effective.

NIST Question #5) Does this proposed update adequately reflect advances made in the Roadmap areas?

IT SCC Comment: While not all of the Roadmap areas were addressed in Version 1.1, and some were addressed more than others, the proposed updates do advance several key areas that have been of significant interest to critical infrastructure owners and operators, such as supply chain, access control, and measurement. The IT SCC appreciates that NIST has already scheduled a Cybersecurity Framework Workshop in May 2017 to continue the dialogue on these areas.

NIST Question #6) Is there a better label than "Version 1.1" for this update?

IT SCC Comment: The label "Version 1.1" is adequate, but we suggest removing "Critical Infrastructure" from the title "Framework for Improving Critical Infrastructure Cybersecurity" and titling the document simply, "The Cybersecurity Framework." While we understand the name's origins come from Executive Order 13636, which initiated its creation, the use and value of the Framework stretches beyond critical infrastructure owners and operators. The short, straightforward "The Cybersecurity Framework" is memorable, rolls off the tongue well, and captures the broad scope.

NIST Question #7) Based on this update, activities in Roadmap areas, and activities in the cybersecurity ecosystem, are there additional areas that should be added to the Roadmap?

IT SCC Comment: We would like to provide the following suggestions.

● The introduction and use of case studies. IT SCC suggests that a series of case studies be developed as a supplement to the Framework. Each case study should be based on real world examples and reflect the efforts to implement the Framework for small, medium and large companies.

● Increased promotion of the Framework. To strengthen common foundation introduced by the Framework, it should be offered and promoted internationally as well as domestically. It should be actively shared with international governments, standards organizations, and industry sectors.

● Inclusion of newer technologies. Technology changes rapidly and newer ones need a way to be addressed, such the Internet of Things (IoT) and UAV/Drones. The technologies can be expected to influence current security models and their traditional defenses, requiring new approaches.

● Cybersecurity Framework for SMBs. We suggest that NIST consider introducing a simplified version of the Framework that is more accessible to very small companies. This approach would be analogous to the way OCTAVE-Allegro and OCTAVE-S were developed to simplify OCTAVE.

● More separation of duties. IT SCC suggests segregating functional areas that belong to Senior Management to those held by Operations. The added clarify could help avoid confusion and strengthen the meaning of several areas within the document.

● Clarification of labeling and use of key terms. Examples include: ○ Figure 2 on page 13 of the Framework clearly depicts two types of assessments that work in a feedback loop to/from senior management. At the top level there is a standard vulnerability stoplight/heatmap on the left side making its way up from a low-level analysis, and a true *Strategic Risk Assessment* on the right which articulates risk appetite, priorities, and budgets. The left side represents a *Vulnerability Assessment*, but that is not how it is labeled. The right side represents a *Strategic Risk Assessment*. The rest of the NIST Framework uses the term *Risk Assessment* to reference both, which is confusing.

> ○ A board, or executive team, works with very high-level asset categories. Think balance sheet items like physical assets, intangible assets, and financial assets. It does not delve into specific assets (e.g., software/hardware), threats (e.g., individual exploits), or vulnerabilities (e.g., patch levels). It keeps everything at a very high level. A *Strategic Risk Assessment* evaluates these high-level assets against a handful of equally high-level threat categories (e.g., Verizon DBIR threat categories). The results provide a top-line financial picture against

which to set priorities, budgets and risk appetite. Mitigation costs (derived from a *Vulnerability Assessment*) can then be evaluated against the risk appetite, with a standard cost-benefit analysis. *Vulnerability Assessments* may also drive/influence the statistical models that are also integral to a *Strategic Risk Assessment*.

○ The *Vulnerability Assessment* (audit, pen-test, inventory of known CVE vulnerabilities, patch levels, etc.) is a low-level, technical analysis performed by operations (IT staff/vendors). Stoplight/heatmap rankings are determined based on a CVSS score, industry best practices, or some other external point of reference. Among other uses, a *Vulnerability Assessment* articulates, to senior management, where mitigation-controls are weakest. When evaluated in the context of a *Strategic Risk Assessment* the cost/benefit of fixing vulnerabilities can be examined.

○ Organizations need both types of assessments, each serving a different function and a different audience. The NIST Framework does not really distinguishing between them, mostly because it uses Risk Assessment generically.

NIST Question #8) Are there any areas that should be removed from the Roadmap?

IT SCC Comment: Not at this time. The IT SCC appreciates the opportunity to provide feedback on Version 1.1 and looks forward to continued dialogue and engagement with NIST as the Cybersecurity Framework matures.