INFORMATION TECHNOLOGY
IT SCC
SECTOR COORDINATING COUNCIL ™

January 19, 2018

Via cyberframework@nist.gov

Andrea Arbeleaz
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Subject: Cybersecurity Framework Version 1.1 Draft 2

Dear Ms. Arbeleaz:

The IT Sector Coordinating Council (IT SCC) generally supports the changes that NIST suggest in its December 2017 Cybersecurity Framework (CSF) Version 1.1, Draft 2. The major amendments that are contained in NIST's update pertain to (1) metrics and measurements, (2) supply chain risk management and small business education and prioritization, and (3) development of roadmap action items. ISA largely focuses it comments on these three areas.

CSF v1.1 Draft 2 Section 4.0 – Self-Assessing Cybersecurity Risk with the Framework

In the CSF v1.1 Draft 2, NIST correctly revises the metrics and measurement section that was inserted in v1.1 Draft 1 to refocus the metrics language to emphasize internal assessments. The IT SCC applauds this revision.

The IT SCC applauds NIST's insistence that the Framework remain a voluntary, non-regulatory tool. We want to stress to policymakers that the inclusion of metrics and SCRM in the CSF v1.1 Draft 2 should not alter this fact. Businesses need flexible and effective cyber solutions so that they can routinely adapt to the ever-changing tactics that illicit actors throw against network defenders. Pro-Framework stakeholders should push back vigorously against regulatory authorities that could leverage – subtly or overtly – metrics and SCRM considerations for their own unproductive purposes.

In the CSF v1.1 Draft 1, NIST included language in Section 4.0 calling for "external audit" or "conformity assessment." The IT SCC believes that was the wrong path for cyber-risk management. By revising this section, NIST clarifies its intent that metrics are to be used for measuring effective use of the Framework, highlighting uses of measurement that emphasize the role of metrics in self-assessment rather than outside assessment. Retitling this section from "Measuring and Demonstrating Cybersecurity" to "Self-Assessing Cybersecurity Risk with the Framework", as well as adding a Roadmap item on metrics to detail future work for advancing the measurements section, embraces stakeholder comments. Emphasizing "self-assessment" ensures NIST's intent is clear – that metrics should be developed and used for self-assessment in order to allow and encourage organizations to voluntarily use the Framework in line with their unique business goals and objectives.

We also support NIST's emphasis on the strategic nature of cybersecurity's effect on business results. In the revised Section 4.0, CSF v1.1 Draft 2 states, "To examine the effectiveness of investments, an organization must first have a clear understanding of its organizational objectives, the relationship between those objectives and supportive cybersecurity outcomes, and how those discrete cybersecurity outcomes are implemented and managed. While measurements of all those items is beyond the scope of the Framework, the cybersecurity outcomes of the Framework Core support self-assessment of investment effectiveness and cybersecurity activities."

In 2014, the National Association of Corporate Directors (NACD), published the Cyber-Risk Oversight Handbook for Corporate Directors (updated in 2017) that aims to teach boards more about cyber-risk management and contextualize cybersecurity within issues boards are comfortable with (mergers/acquisitions, PE rations, innovation, strategic partnerships). This Handbook encourages boards to approach cybersecurity through the perspective of making sound business decisions. More importantly, the positive impact of the Handbook on consensus security outcomes has been highlighted by PricewaterhouseCoopers (PWC) in their 2016 Global Information Security Survey report.

NIST's revision in v1.1 Draft 2 Section 4.0 adopts the same principles recommended not only in private sector comments to the CSF v1.1 Draft 1, but also those that PwC highlighted as increasing board participation in security discussions, better alignment of cybersecurity with overall risk management and business goals, improved security practices, increased budgets, and fostering an organizational culture of security. Again, we applaud NIST in adopting this recommendation.

CSF v1.1 Draft 2 Section 3.3 – Communicating Cybersecurity Requirements with Stakeholders

In the CSF v1.1 Draft 2, NIST added new language to help users better understand managing cybersecurity within supply chains, to help supply chains better understand managing cybersecurity, and to better incorporate that information into external participation under the Framework's core implementation tiers.

Refining the language around implementation tiers and enhancing guidance for applying the Framework to supply chain risk management (SCRM) is a step in the right direction. References to SCRM should explicitly take into consideration small business concerns. Draft 2 stresses the importance of communication between stakeholders up and down supply chains, calling them "complex, globally distributed, and interconnected set of resources and processes between multiple levels of organizations."

While Draft 2 Section 3.3 does not specifically mention small business concerns, adding small business considerations to the Roadmap for future development shows NIST's commitment to helping small businesses and supply chain operators understand cyber risk and effectively address it. In the accompanying Roadmap, NIST committed to embarking on a "listening tour" to hear first-hand from small business owners about their cybersecurity needs, followed by working with stakeholders to address gaps in cybersecurity resources. This will be used to craft "Starter" Framework profiles specific to small- and medium-sized businesses, tailored toward risk-management of business processes important to small business owners and reducing effort necessary to customize the Framework.

The IT SCC has long held that, if we want small companies to become more secure, we need to make cybersecurity easier and cheaper for them. By undertaking systematic testing of the Framework, small businesses can obtain the desperately needed prioritizations of cybersecurity controls they need.

NIST should leverage the existing system of public-private collaboration in order to prioritize the needs of small businesses. The IT SCC applauds NIST's commitment to a "listening tour" to hear from small- and medium-sized businesses about their cybersecurity concerns, as well as highlighting the need to prioritize the NIST Cybersecurity Framework for better adoption by small business owners.

CSF v1.1 Draft 2 Roadmap

In the CSF v1.1 Draft 2 Roadmap, NIST includes language on the "cyber-attack lifecycle," governance and enterprise risk management, referencing techniques for informative references, and small business awareness and resources, in addition to cybersecurity measurement. Specifically, the Roadmap states that, "Increasingly, senior executives are asking for a more accurate and quantitative portrayal of [estimated benefit and risk reduction] and how they might change. Providing more accurate and quantifiable answers to these questions requires an aligned, modular, and systemic approach to cybersecurity measurement, so that measurement at more technical levels is supportive of high-level decision making."

The development of reliable ways to measure risk and effectiveness would be a major advancement in helping organizations align cybersecurity with overall risk management and business goals. The IT SCC applauds NIST's decision to initiate a cybersecurity measurement program focused on aligning technical measures to determine effect on high-level organizational objectives, as well as "to support decision making by senior executives and oversight by boards of directors."

Recommended elements of the metrics process NIST should launch as part of CSF v1.1 should include examination of methods boards can use to determine how best to address the NACD principles and coordinate with senior management regarding their implementation. These principles are:

- Cybersecurity is not an "IT" issue;
- Boards must understand their unique legal obligations for cybersecurity;
- Boards must have access to appropriate levels of cybersecurity expertise;
- Boards must demand that management define a clear cybersecurity framework that they will follow;
- Boards must understand organizational cyber risk and what risks they are accepting, mitigating or transferring.

This proposed update to the Roadmap reflects a cultural shift within government on how to approach cybersecurity issues. NIST's proposal to help organizations integrate cybersecurity into their overall business decisions signifies a key, and critical shift in the current governmental approach to cybersecurity.

Thank you for the opportunity to provide feedback and we look forward to continued collaboration.

Sincerely,

Ola Sage,
Chair, IT Sector Coordinating Council