INTERNET SECURITY ALLIANCE
www.isalliance.org

January 19, 2018

Via cyberframework@nist.gov

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

RE: Cybersecurity Framework Versions 1.1 Draft 2

Dear Ms. Arbeleaz,

Thank you for the opportunity to provide commentary from the Internet Security Alliance on the second proposed version 1.1 update to the Framework for Improving Critical Infrastructure Cybersecurity.

The Internet Security Alliance (ISA) is a multi-sector trade association representing mainly the chief information security officers of Fortune 100 companies. ISA has a long-standing interest in seeing that the Framework achieves its objectives of better private-sector cybersecurity. ISA's Cybersecurity Social Contract, published in 2009, first called for the collaborative industry-government development of standards and practices suitable for voluntary adoption reinforced by market incentives that lead to Executive Order 13636 and the NIST Cybersecurity Framework (CSF). Since the CSF was unveiled in 2013, ISA has worked with the National Association of Corporate Directors (NACD) to integrate models, such as CSF, successfully into enterprise-wide risk management programs.

ISA has also been a longtime advocate for prioritizing and testing the Framework for effectiveness and cost-effectiveness, as called for in Executive Order 13636. The addition of language in the Framework's Executive Summary that states, "NIST must identify 'a prioritized, flexible, repeatable, performance-based, and cost-effective approach [to cyber risk management], including information security measures and controls that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risks,'" embodies ISA's stance – we need to fully implement Executive Order 13636 and prioritize cyber-risk management through a flexible, voluntary, cost-effective manner. In fact, in ISA's comments on CSF v1.1 Draft 1, we state that NIST should begin by addressing the effectiveness of CSF 1.0, and we applaud NIST for taking steps in this direction.

ISA generally supports the changes that NIST suggest in its December 2017 Cybersecurity Framework draft version 1.1. 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 its comments on these three areas.

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

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

In our comments on CSF v1.1 Draft 1, ISA recommended that NIST replace the language in Section 4.0 calling for "external audit" or "conformity assessment" as it suggested that the path to better cybersecurity metrics lies through audits or compliance assessments, and 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.

ISA also recommended NIST emphasize the strategic nature of cybersecurity's effect on business results. We again applaud NIST for adopting this recommendation. 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, ISA, in partnership with 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 ration, innovation, strategic partnerships, etc.). This Handbook encourages boards to approach cybersecurity through the perspective of making sound business decisions. The positive impact of the Handbook on consensus security outcomes has been highlighted by many of the leading professional services and law firms.

NIST's revision in CSF v1.1 Draft 2 Section 4.0 adopts the same principles ISA recommended not only in its comments to CSF v1.1 Draft 1, but also those related to 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.

INTERNET SECURITY ALLIANCE
www.isalliance.org

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

In 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. ISA recommended in its comments on CSF v1.1 Draft 1 that 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.

ISA 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. ISA suggested that NIST leverage the existing system of public-private collaboration in order to prioritize the needs of small businesses. ISA 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."

This circles back to ISA's work with NACD and corporate directors. 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. ISA 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."

ISA, in its comments on CSF v1.1 Draft 1, recommended that an element of the metrics process NIST should launch as part of CSF v1.1 includes examination of the 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. ISA has long advocated that cybersecurity is not just an IT issue, but an economic and enterprise-wide risk management issue, and it should be addressed as such. NIST's proposal to help organizations integrate cybersecurity into their overall business decisions signifies a key shift in the current governmental approach to cybersecurity.

***

ISA applauds NIST's insistence that the Framework is a voluntary, nonregulatory tool. We want to stress to policymakers that the inclusion of metrics and SCRM in 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.

If you have any questions or need more information, please do not hesitate to contact me (lclinton@isalliance.org; 703-907-7028). We look forward to continuing the effective public-private partnership with NIST and other pertinent stakeholders.

Sincerely,

Larry Clinton

www.isalliance.org

Larry Clinton
President/CEO
Internet Security Alliance