From: **Christian Troncoso**
Date: Mon, Apr 10, 2017 at 5:31 PM
Subject: Comments on Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity
To: "cyberframework@nist.gov" <cyberframework@nist.gov>

On behalf of BSA | The Software Alliance, I am submitting the attached Comments on Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity.

Best,
Christian

Christian Troncoso
Director, Policy
BSA | The Software Alliance
W bsa.org

[Attachment Copied Below]

April 10, 2017

VIA EMAIL: cyberframework@nist.gov

Edwin Games
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Re: Comments on Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity

Dear Mr. Games,

BSA | The Software Alliance[1] appreciates the opportunity to respond to the National Institute of Standards and Technology's ("NIST") Request for Information about stakeholder views on the Framework for Improving Critical Infrastructure Cybersecurity ("Framework"). BSA is the leading advocate for the global software industry before governments and in the international marketplace. BSA members provide cloud services, data analytics, cybersecurity solutions, and other cutting-edge products and services to governments and businesses of all sizes across all industries.

As providers of technology that is the backbone of the global IT infrastructure and of cybersecurity products and services, BSA members have extensive experience working with governments and other stakeholders around the world on cybersecurity policy and standards. This experience has taught us the value of technology-neutral policies that provide guidance on managing cybersecurity risk while offering organizations the flexibility to deploy security measures that are tailored to their unique business drivers and to specific nature of the risks they face. BSA and its members are therefore very supportive of NIST's work to date in developing and overseeing the coordination of the Framework.

In issuing this Request for Comments on proposed updates to the Framework,[2] NIST has demonstrated yet again its commitment to ensuring the development and evolution of the Framework remains a transparent and collaborative exercise involving all stakeholders in government and the private sector. Because the Framework has been developed through a genuine public-private partnership, it has rightly earned tremendous legitimacy among policymakers and throughout industry. We applaud NIST for its continued commitment to the multi-stakeholder process and provide below our perspective on the proposed updates in Framework Version 1.1 as well as suggestions for encouraging further uptake of the Framework.

---

[1] BSA's members include: Adobe, ANSYS, Apple, Autodesk, Bentley Systems, CA Technologies, CNC/Mastercam, DataStax, IBM, Microsoft, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, Trimble Solutions Corporation, The MathWorks, Trend Micro and Workday.

[2] National Institute of Standards and Technology, *Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity; Notice and Request for Comments*, 82 Fed. Reg. 8408-09 (January 25, 2017).

Proposed Updates to the Framework – "Version 1.1"

Updating the Framework involves a delicate balance. On the one hand, it is critical that the Framework account for emerging threats and technological advances. On the other, it is important not to move too quickly in adding elements to the Framework that might not yet constitute "best practices" or that could deter adoption of the Framework by organizations with limited resources and/or familiarity with cutting edge risk management practices. Overall, BSA members are encouraged by the thoughtful and measured approach NIST has taken to updating the Framework and are generally supportive of the proposed revisions.

The proposed expansion of the Access Control Category to include guidance on Identity Management and Authentication is, in particular, a welcomed update. In the years since the publication of the Framework, the role that identity and access management plays in managing cybersecurity risks has grown in importance. The proliferation of IoT devices and the increasing adoption of "bring your own device" policies have made identity management and device authentication mechanisms a critical element of network security for enterprises of all sizes. The addition of guidance on Identity Management and Authentication to the pre-existing Access Control category in the Framework Core will help organizations better manage potential endpoint security risks associated with these developments.

BSA likewise appreciates NIST's effort to flesh out the guidance in Section 3.3 and Section 3.4 to better explain how stakeholders can use of the Framework to identify and communicate their supply chain risks with suppliers and partners. The addition of the Supply Chain Risk Management ("SCRM") category to the Framework Core will help organizations identify and manage their supply chain risks by reference to existing standards and best practices. However, because these standards and best practices continue to evolve, we have some concerns with NIST's proposal to add SCRM as a standalone criteria in the Framework Implementation Tiers. The existing Implementation Tier criteria (e.g. "risk management process" and "integrated risk management program") are holistic concepts that cut across the Framework functions and categories to "describe the degree to which an organization's cybersecurity risk management practices exhibit the characteristics defined in the Framework." In contrast, SCRM is itself a (newly proposed) Framework category. To avoid the risk of further confusing the role of Implementation Tiers, we recommend that NIST focus on providing SCRM guidance in the Framework Core and refrain from incorporating SCRM into the Tiers at this time.

Framework Version 1.1 also adds a new section on "Measuring and Demonstrating Cybersecurity," which introduces the concepts of "metrics" and "measures" to help organizations quantify the impact of specific cybersecurity practices. Rather than prescribing a specific set of metrics for measuring the cybersecurity impact of Framework adoption, NIST has wisely opted for a higher-level approach that provides guidance for organizations seeking to develop their own "measurement systems" that can account for their unique business requirements and available resources. While we welcome the high-level reference to the importance of understanding cybersecurity risk management as being grounded in business objectives, we are concerned that the highly conceptual guidance in newly proposed Section 4 might be premature for inclusion in the Framework Core. Because cybersecurity measurement is inherently context-dependent, a more useful approach would be for NIST to convene stakeholders to begin developing sector-specific guidance that can account for the unique needs of particular industries or communities, such as SMBs. Of course, such an approach would not be ripe for inclusion in the Framework. NIST should therefore consider building out such guidance in supplementary documents or through the development use cases that can be used as an addendum to the Framework. Such an approach would enable NIST to provide more concrete guidance while also accounting for organizations' varying operational contexts and accommodating the need for flexibility.

Promoting Domestic and International Adoption of the Framework

Updating the Framework to account for evolving threats and new technologies is critical to ensuring its long-term success. Equally important, however, are efforts to promote adoption of the Framework. In that regard, we are appreciative of NIST's efforts to promote adoption of the Framework by enterprises through participation at workshops and public events and by offering resources on its website that provide practical guidance and tools for implementing the Framework. These efforts are having a material impact on the overall uptake of the Framework[3] and NIST should continue to develop use cases and best practices that illustrate how the Framework can be implemented to improve cybersecurity risk management across a range different business sizes and industries.

We would also encourage NIST to work closely with other US government agencies to ensure there is a consistent, government-wide understanding of the Framework and the benefits of its risk management-based approach to promoting cybersecurity. A unified government approach to cybersecurity aligned around the Framework would reduce the compliance burden placed on regulated entities, allowing them to focus time and resources on risk management and improving security outcomes. For these reasons, the recent Presidential Commission on Enhancing National Cybersecurity identified regulatory harmonization with the Framework among its top recommendations.[4]

To promote international awareness of the Framework and encourage harmonization of international cybersecurity policies, we urge NIST to work closely with State Department's Office of the Coordinator for Cyber Issues ("S/CCI"). As the Administration's chief coordinator for global diplomatic engagement on cyber issues, the S/CCI is uniquely positioned to engage in norm building exercises with our international partners. As part of its capacity building exercises, the S/CCI should actively promote the Framework as a model for cybersecurity policy development. To that end, we would also encourage NIST's participation at the State Department's upcoming Global Training for Cyber Policy and Digital Economy Officers in Washington D.C. from May 8-12. The event will bring together more than 100 foreign service officers and could be a tremendous opportunity to ensure that US embassy and consulate personnel have the training needed to promote the Framework in their host countries. Finally, consistent with a recommendation from Commission on Enhancing National Cybersecurity, NIST should "promote the use of the Framework by actively working with industry to seek its acceptance in international standards bodies."[5] Recognition by a standards organization would bolster the Framework's credibility among international constituencies and help to ensure that other countries considering cybersecurity regulations opt for a standards-based approach.

---

[3] *See* Government Accountability Office, *Critical Infrastructure Protection: Measures Needed to Assess Agencies' Promotion of the Cybersecurity Framework*, 25 (Dec. 2015) ("Respondents to our survey who indicated they had been promoted to by NIST noted that they were encouraged to use the framework as a result. Specifically, 102 responses out of 132 indicated that NIST promotional activities were "very" or "somewhat" effective in encouraging the use of the framework.")

[4] Commission on Enhancing National Cybersecurity, *Report on Securing and Growing the Digital Economy,* December 1 2015, available at https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf ("Action Item 1.4.3: Regulatory agencies should harmonize existing and future regulations with the Cybersecurity Framework to focus on risk management – reducing industry's cost of complying with prescriptive or conflicting regulations that may not aid cybersecurity and may unintentionally discourage rather than incentivize innovation.").

[5] *Id.* (Action Item 6.1.5).

Thank you again for the opportunity to share our views on the development of the Framework.

Sincerely,

Christian Troncoso
Director, Policy