U.S. CHAMBER OF COMMERCE

Ann M. Beauchesne
Senior Vice President
National Security and Emergency Preparedness

1615 H Street, NW
Washington, DC 20062
202-463-3100

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 U.S. Chamber of Commerce welcomes the opportunity to respond to the National Institute of Standards and Technology's (NIST's) request for comments on the Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 Draft 2 (Draft 2 or the second draft).[1]

On December 5, 2017, NIST released Draft 2, which makes a number of enhancements, clarifications, and additions to Version 1.1 of the Framework, which was published in January 2017. Last April, the Chamber wrote to NIST saying that it largely supported, with some caveats, the proposed changes that NIST put forward in Version 1.1. The major amendments contained in Version 1.1 pertained to measures/metrics and the supply chain. The Chamber focused its comments on these two areas and provided thoughts on establishing metrics to deter malicious actors.[2]

The Chamber values the considerable effort that NIST put forth to update the Framework. In addition to meeting with the Chamber and many other groups, the agency's two-day workshop in May 2017 gave stakeholders an opportunity to hear from one another about how organizations make sense of the proposed changes to the Framework. The Chamber's goal, which NIST shares, is to make essential and practical amendments to the Framework while keeping the new version compatible with the original, especially on the subject of maintaining broad swaths of the business community's support.

## FRAMEWORK MEASUREMENT: BUSINESS SELF-ASSESSMENT EMPHASIZED

NIST made substantive changes to the measures/metrics section of Draft 2, which the Chamber welcomes. First, the second draft renames section 4.0 of Version 1.1 to *Self-Assessing* Cybersecurity Risk with the Framework [italics added] from Measuring and Demonstrating

Cybersecurity. The revised header emphasizes that organizations can assess their cyber risks, along with the costs and benefits of their information security strategies "*internally* or by seeking a third-party assessment" [italics added].[3] This tweak, while seemingly subtle, is significant. It should instruct third parties, whether public or private, that they cannot have access to data that a company generates when using the Framework without prior authorization by the business. In a similar vein, NIST should consider adding language to the Framework noting that there is no such thing as complying with the Framework. Such thinking reflects the consensus that regulatory compliance does not equal sound cyber risk management.

Second, the content underpinning section 4.2 of Version 1.1, Types of Cybersecurity Measurement, was moved to the Draft NIST Roadmap for Improving Critical Infrastructure Cybersecurity Version 1.1 (Roadmap) that accompanies Draft 2.[4] Measuring cybersecurity, including the practices, processes, management, and technical aspects of using the Framework, deserves more work before being embedded, if ever, in the Framework because there are no standard templates or universal solutions linked to evaluating cybersecurity. The Roadmap pragmatically recognizes that since the Framework's beginnings a few years ago, "measurement has been a recurrent area of interest and much discussion. . . . This is an under-developed topic, one in which there is not even a standard taxonomy for terms such as 'measurement' and 'metrics.'"[5]

The Roadmap goes on to say, "The development of reliable ways to measure risk and effectiveness would be a major advancement and contribution to the cybersecurity community." The Chamber agrees with NIST that utilizing measurement data can improve the security of multiple business networks and information systems while providing consistent, reasonably complete, and flexible data to a range of stakeholders. However, the Chamber strongly believes that industry actors should never be compelled formally (e.g., through statutory mandates) or informally to disclose measurement information to third parties. Analysts, investors, researchers, and regulators should not be given businesses' sensitive, security-related data unless the private entity agrees to publicly disclose them.

Indeed, it is valuable that Draft 2 summarizes the relevance and utility of measurement as a self-assessment exercise. The Chamber thinks that business officials should identify before engagements which entities will receive the results of cyber performance examinations and how the information will be used.[6] Thus, the second draft's combination of stressing business self-assessment of the Framework and setting aside further work on measurement for the Roadmap helps place constraints on third parties, ideally freeing up businesses to gauge and assign values to their cyber risks and steps taken to reduce risks to acceptable levels.

Businesses should not have to look over their shoulders at regulators when judging the Framework's utility to their cybersecurity. The better that businesses measure their risks, costs, and benefits of cyber strategies and operations, the more rational, effective, and valuable their investments in enterprise cybersecurity programs can be individually and for the nation's economic security.

## SUPPLY CHAIN RISK MANAGEMENT (SCRM): PROGRESS CONTINUES

Last April, the Chamber urged NIST to provide additional guidance to organizations concerning SCRM activities. The agency made good strides to accomplish this goal. Section 3.3 of both Version 1.1 and Draft 2, Communicating Cybersecurity Requirements with Stakeholders, provides advice to organizations on applying the Framework to manage cyber risks associated with external parties and vice versa.

In addition, the Chamber agrees with NIST's decision to remove detailed language in Version 1.1 pertaining to SCRM from the various Tiers.[7] Many businesses believe that keeping SCRM in the tiering structures, which range from Partial (Tier 1) to Adaptive (Tier 4), would sow confusion about how to use them, which is an outcome that neither industry nor NIST wants.[8]

The Roadmap notes that there are ongoing challenges to SCRM, particularly organizations' awareness of supply chain risks and potential mitigating actions. The Chamber will continue to promote the use of SCRM standards, guidelines, and practices in its national Cybersecurity Campaign, which is beginning its fourth year.[9] The Chamber pushes businesses to use the Framework when communicating with partners, vendors, and suppliers about the management of supply chain risks and threats. It is positive that NIST expects to continue its work on identifying, evaluating, and developing effective technologies, tools, and techniques to help secure organizations' supply chains.[10]

It is worth flagging that some organizations found Figure 3, Cyber Supply Chain Relationships, confusing. A company told the Chamber that while the figure is partially explained in section 3.3, the roles and connections among the various ecosystem parties are unclear. The company asked, "What is the difference between the 'Technology Buyer' and the 'Buyer'? Aren't the 'Organization' and the 'Buyer' the same? And what is the difference between 'Not Technology' and 'Technology?'" These questions could be addressed through additional clarity and dialogue with stakeholders.

## SHIFTING VULNERABILITY DISCLOSURE AND FEDERAL ALIGNMENT TO THE ROADMAP

**Coordinated Vulnerability Disclosure (CVD).** Draft 2 adds a new Analysis subcategory regarding CVD to the Respond Function of the Framework.[11] The Chamber urges businesses to collaborate with security researchers on vulnerability disclosure programs.[12] Yet some in industry hold that it is too early to endorse CVD as a part of the Framework, including owing to the fact that CVD was not an element in Version 1.1.

The Chamber recommends that NIST temporarily move this new concept to the Roadmap, which offers a helpful setting to discuss the advantages and disadvantages of CVD. While Draft 2 does not suggest a certain level of CVD rigor and sophistication for Framework users, it conveys the sense that organizations should have programs to "receive, analyze, and respond to vulnerabilities *disclosed to the organization* from internal and external sources"

[italics added]. However, there are multiple uncertainties (e.g., liability) and complications (e.g., expenses) tied to the structure and utility of CVD processes, and not all companies should be expected to have them.[13] Some readers of Draft 2 interpreted the new CVD subcategory language to mean that Framework users would need to report publicly on their enterprise's vulnerabilities, which the Chamber does not believe was NIST's intent.

Framework stakeholders ought to grapple further with the complexities surrounding CVD before it is integrated into the Framework. The Roadmap has historically offered cybersecurity stakeholders a means of pinpointing unresolved issues, such as CVD, for future "development, alignment, and collaboration" without absorbing them into the Framework prematurely.[14] Not all businesses will be able to finance, staff, and manage CVD programs, and the Chamber does not want to see companies dissuaded from using the Framework because of unreasonable expectations.

The Chamber agrees with participants at NIST's May Framework workshop who noted that CVD was an important topic in cyber risk management but were unsure how to incorporate it into the Framework. They cited the National Telecommunications and Information Administration's (NTIA's) leadership on a CVD multistakeholder effort, which the Chamber has engaged. According to NIST's July 2017 workshop summary, some participants suggested that Version 1.1 was an appropriate venue to introduce CVD, while others cautioned that more time is needed to "research the intersection between CVD and the Framework."[15] The Chamber concurs with the latter view. The Roadmap is a suitable place to continue the dialogue on how to shape vulnerability disclosure practices and ingest them into the Framework over time.

**Federal Alignment.** Section 3.7 of Version 1.1, Federal Alignment, was shifted to the Roadmap, which the Chamber supports. First, NIST does a good job explaining in the Roadmap what federal programs, including NIST-developed guidance, support agency heads and senior cyber leaders. The government should lead by example on improving U.S. cybersecurity, but the Framework does not need to feature a special section devoted to federal alignment, so Draft 2 gets things right.

Second, there is broad consensus in industry that the Framework is a sound baseline for businesses' cyber practices, including internationally. The Chamber communicated to the Obama and Trump administrations that it wants to sustain the view held by most businesses and policymakers that the Framework is a cornerstone for managing enterprise cybersecurity risks and threats globally. Maintaining the federal alignment language in the Framework would be confusing to international audiences.[16]

Third, section 1(c)(ii) of the administration's May 2017 Executive Order (EO) 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, says, "each agency head shall use the Framework. . . ."[17] The Chamber typically resists seeing the words "Framework" and "shall use" in a single sentence. Simply put, the Framework is supposed to be a *voluntary* tool. Both industry and many public-sector stakeholders do not want the Framework to become a regulatory lever in the hands of government authorities.

However, NIST and industry, which jointly developed the Framework, are pleased that the Framework is being identified as an ideal means to manage agencies' cyber risks. Tom Bossert, the White House homeland security and counterterrorism advisor noted at the time of the EO's release, "[The Framework] is something we have asked the private sector to implement and not forced upon ourselves. . . . From this point forward, departments and agencies shall practice what we preach."[18]

***

The Chamber appreciates the opportunity to offer its views to NIST concerning Draft 2 of the Framework. If you have any questions or need more information, please do not hesitate to contact me (abeauchesne@uschamber.com, 202-463-3100) or my colleague Matthew J. Eggers (meggers@uschamber.com, 202-463-5619).

Sincerely,

Ann M. Beauchesne
Senior Vice President

Matthew J. Eggers
Executive Director, Cybersecurity Policy

Endnotes

[1] See NIST documents and resources related to the Framework for Improving Critical Infrastructure Cybersecurity (Framework) via www.nist.gov/cybersecurity-framework ("Latest Updates").

[2] See the Chamber's April 10, 2017, letter to NIST regarding Version 1.1 of the Framework. www.nist.gov/sites/default/files/documents/2017/04/20/2017-04-10_-_u.s._chamber_of_commerce.pdf

[3] Draft 2, pg. 26.

[4] Draft NIST Roadmap for Improving Critical Infrastructure Cybersecurity Version 1.1, or the Roadmap, (December 5, 2017). www.nist.gov/sites/default/files/documents/2017/12/05/draft_roadmap-version-1-1.pdf

[5] Roadmap, pg. 14.

[6] Chamber's April 2017 letter to NIST.

[7] Compare Version 1.1 (January 10) pgs. 9–12 with Draft 2 (December 5) pgs. 11–15.

[8] See NIST's Initial Analysis of Responses to Request for Comment (RFC) on Cybersecurity Framework Version 1.1 Draft Update (May 15, 2017), pg. 15. www.nist.gov/sites/default/files/documents/2017/05/16/rfc2-response-initial-analysis-20170515.pdf

[9] The Chamber's first of several regional cyber education events of 2018 is on March 27 in Sioux Falls, South Dakota.

[10] Roadmap, pg. 8.

[11] Draft 2, pg. 49.

[12] See, for example, the Department of Justice's A Framework for a Vulnerability Disclosure Program for Online Systems (July 2017). www.justice.gov/criminal-ccips/page/file/983996/download

[13] The advent of cyber Internet of Things (IoT) legislation adds to the difficulties tied to coordinated vulnerability disclosure. www.uschamber.com/sites/default/files/final_uscc_feedback_s1691_federal_cyber_iot_bill_nov_13_2.pdf, https://oversight.house.gov/hearing/cybersecurity-internet-things, www.nist.gov/news-events/events/2017/10/iot-cybersecurity-colloquium

[14] Roadmap, pgs. 1–3.

[15] NIST's Cybersecurity Framework Workshop 2017 Summary (July 21, 2017), pgs. 5–6. www.nist.gov/sites/default/files/documents/2017/07/21/cybersecurity_framework_workshop_2017_summary_20170721_1.pdf

[16] See the joint Chamber-Sidley Transatlantic Cybersecurity report (January 2017). www.uschamber.com/TransatlanticCybersecurityReport

See, too, the Chamber-led March 2016 group letter to the European Commission. www.uschamber.com/sites/default/files/documents/files/industry_comment_ltr_to_european_commission_on_future_of_public_private_partnerships.pdf

[17] www.federalregister.gov/documents/2017/05/16/2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure

[18] "Trump signs cyber order," *FCW*, May 11, 2017. https://fcw.com/articles/2017/05/11/trump-signs-cyber-order.aspx