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

April 10, 2017

Via cyberframework@nist.gov

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

Subject: Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity

Dear Mr. Games:

The U.S. Chamber of Commerce, the world's largest business federation representing the interests of more than 3 million businesses of all sizes, sectors, and regions, as well as state and local chambers and industry associations, welcomes the opportunity to respond to the National Institute of Standards and Technology's (NIST's) request for comments on the proposed update to the *Framework for Improving Critical Infrastructure Cybersecurity*.[1]

The Chamber generally supports the changes that NIST suggests in its January framework draft version 1.1. The major amendments that are contained in NIST's update pertain to (1) metrics and measures—which are distinct concepts, but we combine them into metrics to simplify this letter—and (2) supply chain risk management (SCRM). The Chamber largely focuses its comments on these two areas. We also provide thoughts on establishing metrics on malicious actors.

VERSION 1.1 REVISIONS MAY REQUIRE MORE THAN ONE WORKSHOP TO CLARIFY AND ACHIEVE INDUSTRY CONSENSUS

The Chamber appreciates the work that NIST has done to update the framework. We want businesses to vigorously test the value of metrics in operating environments, which is a comparatively new field of research, and manage supply chain risk. However, the Chamber does not want businesses to fear that the framework could become a means of serving the prerogatives of regulators over the needs of the business community. Unauthorized third parties, whether public or private, should not have unfettered access to data that businesses generate when using the framework.

In addition, policymakers should not take advantage of the business community's support for the framework to forge prescriptive pathways to SCRM. Cyber defenses need to rely on industry best practices and reflect the efficient, decentralized architecture of companies' supply chains.

Version 1.1 seeks to clarify, refine, and enhance the framework. But the Chamber has heard from several members that the proposed changes—particularly with regard to metrics—are unclear and raise questions of interpretation. These members, who have considerable cybersecurity policy experience, were unsure about (1) the meaning of the prospective metrics text, (2) how the metrics could help businesses, and (3) what entities could lay claim to organizations' metrics data.

This should not come as a surprise. Metrics—which were contemplated as part of the "data analytics" component (section 4.5) in the 2014 Roadmap—and SCRM were not included in the framework because they provoked a wide range of competing reactions (e.g., technical, security, and policy) that could not be easily reconciled.[2] In a similar vein, metrics were sparingly considered in NIST's December 2015 request for information and its April 2016 workshop.[3]

Taken together, the framework should make clear that there are no one-size-fits-all methods to employing metrics and administering SCRM activities, including within sectors. NIST is not so much the intended audience here as are policymakers.

The Chamber believes that NIST's two-day workshop in May offers stakeholders a good opportunity to hear from one another about how organizations make sense of proposed metrics and SCRM text. Still, a single workshop may not allow enough time to get the language right. NIST may need to hold follow-up gatherings to work through any significant remaining issues.

The Chamber's goal, which NIST shares, is to make essential and practical changes 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. This should be achieved through a robust back-and-forth dialogue between agency officials and industry leaders.

GETTING METRICS RIGHT AND WITHHOLDING DATA FROM UNAUTHORIZED THIRD PARTIES

NIST proposes including a new section, Measuring and Demonstrating Cybersecurity (section 4.0), in version 1.1.[4] The Chamber urges companies to take advantage of tools like the framework to help them mitigate risks and threats to their security and resilience. Metrics can help organizations improve their cybersecurity over time with increasing accuracy. Nevertheless, the framework is as much a product of industry's efforts as it is of NIST's, and the Chamber is mindful of how it is used.

Some policymakers are calling for NIST to develop framework implementation metrics to quantify the effectiveness and benefits of the framework that could easily become rigid during the design and implementation phases. Such thinking is misguided, the Chamber believes, because there are no standard templates or universal solutions linked to cyber metrics.

Indeed, the Chamber recently pushed back on legislation that initially sought to require public and private initiatives to develop outcome-based metrics, models, and tools that quantify the effectiveness and benefits of the framework. We said that

metrics are being vigorously debated in cyber policy circles and should not be written into law.

The Chamber supports businesses using data to understand the status of their organizations' information security programs. Yet the data are held closely by a business and shared only protectively with trusted third parties.

The Chamber believes that industry actors should *never* be compelled formally or informally to disclose metrics to third parties. Businesses may want to restrict sensitive information to certain recipients. Analysts, investors, security researchers, and regulators should not be given metrics unless the business agrees to publicly disclose them. The Chamber thinks that business officials should identify before engagements which entities will receive the results of cyber performance examinations and how the data will be used.

The Chamber agrees with NIST that harvesting information from metrics can improve the security of multiple business networks and information systems while providing consistent, reasonably complete, and flexible data to a range of stakeholders. The metrics section in version 1.1 could fit this mold without difficulty. But, going forward, industry's greatest challenge may be managing the relationship between its generation and use of metrics and regulators' likely strong desire to access the metrics—which the Chamber will oppose without private organizations giving their consent.

COMMUNICATING SCRM OBJECTIVES WITH SUPPLIERS AND PARTNERS

As recently as September 2016, the Chamber urged NIST to provide additional guidance concerning SCRM, which version 1.1 does through the inclusion of new explanatory language in section 3.3.[5] The Chamber's national Cybersecurity Campaign urges businesses to use the framework when communicating with partners, vendors, and suppliers about SCRM activities. Businesses of all sizes find it challenging to identify their risks and prioritize their actions to reduce weak links vulnerable to penetration, theft, and disruption.

The Chamber supports many efforts to enhance the security of public and private information and communications technology (ICT) networks and systems. The revised framework features SCRM considerations throughout the document. However, the Chamber wants to put the SCRM language in context.

First, it is important to highlight that businesses are linked together through a global web of interconnected, predictable, and efficient supply chains. U.S. businesses rely on these supply chains—which feature physical and digital characteristics—to access international consumers and compete in the global marketplace. The Chamber urges NIST and policymakers to recognize the complexity of mitigating cyber supply chain risk without compromising the interconnectivity that helps ensure the trade flows, access to markets, and the competitiveness of U.S. businesses.[6]

Second, the Chamber urges policymakers to reject prescriptive and/or excessive SCRM programs that inject the United States or foreign governments directly into businesses' innovation and technology development processes, which are international

in scope. Version 1.1 does not call for such regimes, which is positive, and this should not change in future frameworks.

Ambitious public- and private-sector efforts are under way to manage cyber supply chain risk. The Chamber opposes government actions that would create U.S.-specific guidelines, set private sector security standards, or conflict with industry-led security programs. Instead, cybersecurity stakeholders should seek to leverage consensus-based international agreements that enable ICT manufacturers to build products once and sell them globally. The revised framework is constructively consistent with such a view.

Third, the Chamber has a fundamental concern about policies that could broadly apply restrictions on international commerce based on real or perceived threats to the cyber supply chain and ICT products' country of origin. ICT cybersecurity policy must be geared toward embracing globally recognized standards, facilitating trade, and managing risk. NIST understands industry's core apprehension in this area, but we want to draw the attention of Congress and agencies to industry's position.

ESTABLISHING METRICS ON DETERRING BAD ACTORS

The development and use of cyber metrics is a work in progress and is controversial. The Chamber believes that the call for metrics should not be limited to use of the framework, which is industry-centric. Policymakers should also create metrics to assess how successfully the United States is imposing consequences on malicious actors to deter cyberattacks.

It is valuable that the administration's pending executive order on cybersecurity is expected to feature language that calls on federal agencies with economic and national security responsibilities to "jointly submit a report to the President on the nation's strategic options for deterring adversaries and protecting the American people. . . ."[7]

The Chamber's recommendation for measurements on bad actors is technically outside the scope of NIST's open review of version 1.1, but the two sides of this coin—e.g., deterrence by denial (via businesses' using the framework) and deterrence through cost imposition (via the government penalizing illicit hackers)—should be considered jointly in the policymaking process.[8]

Three examples are worth taking into account:

- First, metrics could be used to better pinpoint the geographic origins of cyberattacks. While attribution is a challenge, it is far from impossible.[9] Prominent cyber authorities agree that certain foreign powers or their proxies represent high-end threats against the business community and the United States.[10] Among the goals worth pursing include reducing the number of safe havens from which malicious actors can launch attacks against American interests with impunity.

There is no disincentive to being a cybercriminal that attacks U.S. industry from certain countries around the world. Recalcitrant governments too frequently will not help the U.S. government round up bad actors and turn them over to the FBI and/or the Secret Service.[11]

- Second, metrics could help stakeholders understand the relationship between attacks that businesses report to the government and the number of attacks that are investigated, attributed, and prosecuted. A low ratio suggests that an inadequate amount of government resources are being devoted to disrupting bad actors, which the Chamber has communicated to the Cybersecurity Forum for Independent and Executive Branch Regulators, among others.[12]

- Third, the United States has issued several high-profile indictments against foreign hackers in recent years. For example, in March 2016, seven Iranians allegedly working on behalf of the Iranian government were indicted for a series of cybercrimes that cost U.S. financial institutions tens of millions of dollars and compromised critical controls of a New York dam, according to an FBI announcement.[13]

  It is unclear if the indicted individuals will ever be brought to justice. Metrics could demonstrate if deterrence—essentially dissuading bad actors from hacking businesses because they believe that the costs to them will exceed their expected benefit—is having the intended effect.[14]

  Deterrence and norms need to be part of a new U.S. cybersecurity strategy that policymakers discuss with the business community before, during, and after the strategy is written.[15]

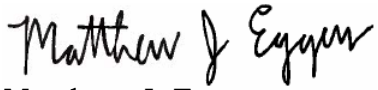
***

The Chamber 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 version 1.1 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 (abeauchesne@uschamber.com; 202-463-3100) or my colleague Matthew Eggers (meggers@uschamber.com; 202-463-5619).

Sincerely,

Ann M. Beauchesne
Senior Vice President



Matthew J. Eggers
Executive Director, Cybersecurity Policy

NOTES

[1] www.federalregister.gov/documents/2017/01/25/2017-01599/proposed-update-to-the-framework-for-improving-critical-infrastructure-cybersecurity

www.nist.gov/cyberframework/draft-version-11

[2] www.nist.gov/sites/default/files/documents/cyberframework/roadmap-021214.pdf

[3] www.nist.gov/sites/default/files/documents/cyberframework/RFI3_Response_Analysis_final.pdf

www.nist.gov/sites/default/files/documents/cyberframework/Workshop-Summary-2016.pdf

[4] http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=51292

[5] www.uschamber.com/sites/default/files/u.s._chamber_letter_nist-wh_cyber_commission_rfi_sept._9_final_v2.1.pdf

[6] www.uschamber.com/letter/letter-regarding-s-662-trade-facilitation-and-trade-enforcement-reauthorization-act-2013%E2%80%9D

https://energycommerce.house.gov/hearings-and-votes/hearings/cybersecurity-examination-communications-supply-chain

https://hsdl.org/?view&did=755497

[7] https://insidecybersecurity.com/daily-news/trumps-draft-cyber-order-drills-down-authorities-capabilities-protecting-critical-sectors

[8] www.lawfareblog.com/international-law-and-deterring-cyber-attacks

[9] www.lawfareblog.com/attribution-malicious-cyber-incidents-soup-nuts

[10] www.armed-services.senate.gov/imo/media/doc/DSB%20CD%20Report%202017-02-27-17_v18_Final-Cleared%20Security%20Review.pdf

[11] www.uschamber.com/sites/default/files/u.s._chamber_letter_nist-wh_cyber_commission_rfi_sept._9_final_v2.1.pdf

[12] www.uschamber.com/sites/default/files/u_s_chamber_letter_to_cyber_forum_july_8_final_2.pdf

[13] www.fbi.gov/news/stories/iranians-charged-with-hacking-us-financial-sector

[14] www.belfercenter.org/publication/deterrence-and-dissuasion-cyberspace

[15] www.uschamber.com/sites/default/files/u.s._chamber_cyber_priorities_2017_short_version_final_march_2017.pdf