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

September 24, 2015

Via nistir8074@nist.gov (Comments on Draft NISTIR 8074)

Michael Hogan
Elaine Newton
National Institute of Standards and Technology
Attn: Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

**Subject: Draft *Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity***

Dear Mr. Hogan and Ms. Newton:

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, and dedicated to promoting, protecting, and defending America's free enterprise system, appreciates the opportunity to comment on the National Institute of Standards and Technology's (NIST's) draft *Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity* (the report). The report comes in two volumes.[1] The Chamber's letter comments on volume one of the strategy paper. We continue to review volume two, which is a relatively dense supplemental document.

The Chamber supported the enactment of the Cybersecurity Enhancement Act of 2014 (P.L. 113-274), which calls on NIST to produce the report. The act takes smart and practical steps to strengthen U.S. businesses' cybersecurity, including authorizing NIST to work closely with industry on an ongoing basis to develop voluntary guidelines and best practices to reduce cyber risks to U.S. critical infrastructure. We believe that public-private collaboration is essential to successfully countering highly adaptive cybersecurity threats, such as organized criminals, malicious individuals, and groups carrying out state-sponsored attacks.

[1] NIST Interagency Report (NISTIR) 8074, the draft *Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity*, is available at http://csrc.nist.gov/publications/PubsDrafts.html#NIST-IR-8074.

The act also focuses on supporting cybersecurity research and development, enhancing public awareness and preparedness, and increasing the number of professionals needed in the workplace to battle nefarious cyber actors and natural hazards. The act, in short, is narrowly tailored and industry focused.

Section 502 of the act requires the director of NIST to work with relevant federal agencies and departments to ensure interagency coordination in the development of international technical standards related to cybersecurity and develop and transmit to Congress a plan for ensuring such coordination within one year of enactment. The report serves as the basis of the mandated plan for advancing interagency coordination.[2]

> SEC. 502. International cybersecurity technical standards.
> (a) In general.—The Director [of NIST], in coordination with appropriate Federal authorities, shall—
> (1) as appropriate, *ensure coordination of Federal agencies engaged in the development of international technical standards related to information system security*; and
> (2) not later than 1 year after the date of enactment of this Act, develop and transmit to Congress a plan for ensuring such Federal agency coordination.
> (b) Consultation with the private sector.—In carrying out the activities specified in subsection (a)(1), the Director shall *ensure consultation with appropriate private sector stakeholders* [italics added].

**Cybersecurity Needs to Be Rooted in Global, Industry-Driven Standards and Practices**

In general, the Chamber agrees with the report's four strategic objectives, especially the importance of facilitating international trade and investment and promoting innovation and competitiveness, and eight recommendations. NIST's proposals—including instituting interagency coordination, collaborating with the private sector, and promoting agency participation in standards training—would provide valuable guidance from White House leadership to federal agencies.

Cybersecurity efforts are optimal when they reflect global standards and industry-driven practices. Efforts to improve the cybersecurity of the public and private sectors should reflect the borderless and interconnected nature of our digital environment. Standards, guidance, and best practices relevant to cybersecurity are typically led by the private sector and adopted on a voluntary basis; they are most effective when developed and recognized globally. Such an approach would avoid burdening multinational enterprises with the requirements of multiple, and often conflicting, jurisdictions.

The Chamber believes NIST realizes that government-directed or centrally coordinated standards, procurement, and regulatory regimes—which are common in other countries—are poor architectures for cybersecurity and would spread companies' information-security budgets much too thinly to meet the dictates of local magistrates.[3] Indeed, any cybersecurity

[2] www.congress.gov/113/bills/s1353/BILLS-113s1353es.pdf

[3] NISTIR 8074, volume 1, p. 3.

standardization processes that industry assumes would favor compliance and bureaucracy over creativity, speed, and innovation would almost certainly discourage buy-in by the private sector, which is crucial to the success or failure of most standards. The Chamber thinks that businesses need minimal structure and maximum autonomy to counter, in partnership with government, rapidly changing cyber threats.[4]

### *Roadmap* for the Future of the Cybersecurity Framework

The Chamber views the report largely through the lens of the *Framework for Improving Critical Infrastructure Cybersecurity* (the framework), which we view as a remarkable success because the business community has embraced it, and the companion *Roadmap*. In fact, the framework was written to be consistent with voluntary international standards.[5] Since the framework is based on global standards and is not country-specific, businesses operating in multiple countries can better align their facilities' cybersecurity efforts under a single umbrella.[6] The Chamber trusts that such a technically sound, cost-effective approach to cybersecurity underpins much of NIST's thinking in developing the report.

In February 2014, NIST released a *Roadmap* to accompany the framework.[7] The *Roadmap* outlines further areas for possible "development, alignment, and collaboration [with particular sectors and standards-developing organizations]." Here are some key areas that the Chamber sees as needing attention, which we urge NIST to consider in writing the final report:

- **Aligning international cybersecurity regimes with the framework.** Many Chamber members operate globally. We appreciate that NIST has been actively meeting with foreign governments to urge them to embrace the framework. Like NIST, the Chamber contends that efforts to improve the cybersecurity of the public and private sectors should reflect the borderless and interconnected nature of our digital environment.[8]

  The current administration and the next one should organize opportunities for stakeholders to participate in multinational discussions. The Chamber urges the federal

---

[4] In his book, *Yes to the Mess: Surprising Leadership Lessons from Jazz* (Boston, MA: Harvard Business Review Press, 2012), Frank J. Barrett, professor of management and global public policy at the Naval Postgraduate School, writes about the requisites for leadership, innovation, and learning in high-performing organizations. He argues (e.g., chapter four, "Minimal Structure-Maximal Autonomy") that dynamic organizations thrive on minimal constraints, learn from errors (without punishment), and collaborate through the evolution of ties between participants. In the Chamber's view, this is exactly what healthy cybersecurity standards-development processes facilitate.

[5] www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

[6] http://insidecybersecurity.com/daily-news/us-japanese-forces-bolster-cybersecurity-ties

[7] www.nist.gov/cyberframework/upload/roadmap-021214.pdf

[8] The Chamber sent a letter in September 2013 to Dr. Andreas Schwab, member of the European Parliament's Internal Market and Consumer Protection Committee, recommending amendments to the proposed European Union (EU) cybersecurity directive. We argue that cybersecurity and resilience are best achieved when organizations follow voluntary global standards and industry-driven practices.

government to work with international partners and holds that these discussions should be stakeholder driven and occurring routinely.

- **Avoiding disruptions to the framework's privacy methodology.** The report says, "Cybersecurity is an important component of protecting privacy, and many privacy standards address the protection of personal data by cross-referencing standards in the area of information security management systems."

  The Chamber appreciates that NIST amended the preliminary framework and included a more tailored privacy statement into version 1.0 of the framework. To encourage broad use of the framework, industry thinks that the privacy methodology must be consensus based and straightforward. We welcome the outreach that NIST officials have had with us regarding its international standardization and privacy engineering initiatives and want to continue the dialogue.

  Privacy engineering can offer tremendous value to businesses and consumers. Many Chamber companies leverage privacy engineering solutions as part of their "privacy by design" practices and internal information management programs. Refining and improving privacy engineering processes require a collaborative effort among an array of corporate resources—IT, compliance, legal, product development, marketing, and customer service.

  NIST is well suited to contribute technical expertise to an international standards-setting effort. But it should build on a multistakeholder process that is rooted in consensus policy goals. The Chamber is concerned that the international cybersecurity standardization initiative could endorse potential privacy policy objectives prematurely, rather than integrate consensus-based and broadly adopted policies into a technical standard. The essential point is the Chamber argues that the United States' engagement strategy should refrain from causing confusion with the privacy methodology in the framework.

- **Managing cyber supply chain risks.** The Chamber supports the attention that NIST has paid to supply chain risk management issues. As part of the Chamber's national cybersecurity education roundtable series,[9] our member organizations have urged businesses to use the framework when communicating with partners, vendors, and suppliers. Businesses of all sizes can find it challenging to identify their risks and prioritize their actions to reduce weak links vulnerable to penetration, theft, and disruption. NIST should provide additional guidance in this area, which the agency recognizes.[10]

[9] To date, cities visited on the Chamber's *Improving Today. Protecting Tomorrow*™ tour include Atlanta (July 2015), Austin (July 2014), Chicago (May 2014), Minneapolis (September 2015), Phoenix (October 2014), and Seattle (September 2014).

[10] NISTIR 8074, volume 1, p. 8.

Many companies and associations are participating in the Software and Supply Chain Assurance Forum, which is being led by the General Services Administration (GSA), the Department of Defense (DoD), and the Department of Homeland Security (DHS), among others. In June 2013, the Chamber submitted comments to GSA and the Joint Working Group on Improving Cybersecurity and Resilience Through Acquisition regarding section 8(e) of the cyber EO.[11]

Central points that the Chamber made in the letter remain applicable to the *Roadmap* and to NIST's activities concerning supply chain risk management:

- The Chamber supports efforts by policymakers to enhance the security of government information technology and communications (ICT) networks and systems, or the cyber supply chain. However, we urge policymakers to reject prescriptive supply chain or software assurance regimes that inject the United States or foreign governments directly into businesses' innovation and technology development processes, which are global in scope.

- 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, the government should seek to leverage mutually recognized international agreements that enable ICT manufacturers to build products once and sell them globally.

- The Chamber has a fundamental concern about policies that would 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.

**Harmonizing *Domestic* Cybersecurity Regulations—Still on Policymakers' To-Do List?**

NIST's report to Congress focuses on coordinating U.S. agencies in developing international standardization to promote cybersecurity and resilience. Still, the Chamber wants to remind policymakers that the February 2013 cybersecurity executive order calls on regulatory agencies with authority over critical infrastructure to report to the Office of Management and

[11] See May 13, 2013, *Federal Register*, pp. 27966–27967, via www.gpo.gov/fdsys/pkg/FR-2013-05-13/pdf/2013-11239.pdf. Section 8(e) of the EO says, "Within 120 days of the date of this order, the Secretary of Defense and the Administrator of General Services, in consultation with the Secretary and the Federal Acquisition Regulatory Council, shall make recommendations to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs, on the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration. The report shall address what steps can be taken to harmonize and make consistent existing procurement requirements related to cybersecurity."

Budget (OMB) any private entities subject to "ineffective, conflicting, or excessively burdensome cybersecurity requirements."[12] But work in this area is seemingly incomplete.

Agencies are expected to recommend ways to make using the framework easier, such as eliminating overlaps among existing laws and regulations, enabling equivalent adoption across regulatory structures, and reducing audit burdens.[13] The intent of the framework is to build agile and responsive cybersecurity capabilities not bound by outdated and inflexible rules and procedures. The Chamber urges independent agencies and Congress to adhere to the dynamic approach advocated by the administration and that is embodied in the nonregulatory, public-private framework.

Aside from offering the perspectives above for NIST's consideration, the Chamber has further questions and topics that we respectfully ask institute officials to address:

- The second of the report's four objectives pertains to ensuring that standards and assessment tools for the U.S. government are technically sound, which is logical. However, shouldn't NIST call out the "reasonable availability" of the underlying specifications necessary to implement standards as a factor for selecting them? (page 2, lines 67–81)

- The text on page 3 (line 116 and footnote No. 6) correctly calls out the obligation for agencies to follow the National Technology Transfer and Advance Act (NTTAA) and Office of Management and Budget (OMB) Circular A-119 Revised. Shouldn't recommendation No. 8 on page 13, related to using relevant international standards for cybersecurity, reference the NTTAA and the OMB member too, including the requirement to leverage voluntary consensus standards where available?[14]

- It is important for treaty-based international agreements to include a mechanism for private sector advice and input, given that that the U.S. government could be blocked from expressing its position because of disagreements among affected industries and other stakeholders. (page 9)

- When the United States is formulating its view through interagency coordination (see recommendation No. 1), a clear mechanism needs to exist for soliciting input from the business community, which seems absent from the report. (page 11, lines 445+)

- The reference(s) to U.S. government leadership in standards-development organizations strikes some in industry as a concern. Typically the government convenes, participates, and advises—which the Chamber strongly supports. But leadership or control of the standards-setting process is not a role that we would encourage. (e.g., see page 9)

---

[12] www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[13] www.whitehouse.gov/blog/2013/08/06/incentives-support-adoption-cybersecurity-framework

[14] www.whitehouse.gov/omb/circulars_a119

***

The Chamber welcomes the chance to provide feedback on NIST's draft report. At a time when governments are developing either flexible plans or top-down directives to structure public-private approaches to cybersecurity, NIST's positive role in international standards-setting is significant to America's engagement strategy and U.S. business interests at home and abroad.[15]

Industry benefits when the U.S. government can effectively influence—in close collaboration with private sector stakeholders—the development or revision of cybersecurity standards that businesses help craft and the market supports. Further, the smart and effective development of international standards for cybersecurity promotes U.S. commercial priorities by facilitating constructive outcomes like improved interoperability, higher confidence and trust in online and offline transactions, and strengthened competitiveness of American products and services.

If you have any questions or need more information, please do not hesitate to contact me (abeauchsene@uschamber.com; 202-463-3100) or my colleague Matthew Eggers (meggers@uschamber.com; 202-463-5619).

Sincerely,

Ann M. Beauchesne

[15] For example, the Chamber found quite helpful the January 2015 statement of cooperation between the United States and the United Kingdom that included a reference to the framework as a basis for international harmonization on industry best practices. See http://insidecybersecurity.com/daily-briefs/us-uk-cyber-pledge-cites-nist-framework-international-harmonization.