U.S. CHAMBER OF COMMERCE

Ann M. Beauchesne
Vice President
National Security and Emergency Preparedness

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

October 10, 2014

Via cyberframework@nist.gov

Ms. Diane Honeycutt
Secretary
Computer Security Division
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Dear Ms. Honeycutt:

The U.S. Chamber of Commerce, the world's largest business federation representing the interests of more than three 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, welcomes the opportunity to comment on the National Institute of Standards and Technology's (NIST's) request for information (RFI), *Experience With the Framework for Improving Critical Infrastructure Cybersecurity*.[1]

The Chamber does not attempt to answer each question in the RFI. We focus on the successful rollout of the framework and the positive collaboration that many businesses and government entities have developed over the past several months. Individual organizations are better equipped to provide detailed responses regarding their experiences using the framework.

The Chamber also highlights policy issues—information-sharing legislation being a top priority—that lawmakers and the administration need to diligently address. The information-sharing discussion puts too little emphasis on improving government-to-business sharing. The Chamber wants to expand government-to-business information sharing, which is progressing but needs improvement.[2]

[1] See www.federalregister.gov/articles/2014/08/26/2014-20315/experience-with-the-framework-for-improving-critical-infrastructure-cybersecurity or www.nist.gov/cyberframework.

[2] For example, the Department of Homeland Security's (DHS') Office of Inspector General has reported that the department needs to improve expanding the Enhanced Cybersecurity Services program to all 16 critical infrastructure sectors. See *Implementation Status of the Enhanced Cybersecurity Services Program* (OIG-14-119, July 2014), at www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-119_Jul14.pdf.

Companies tell us that they need more actionable and immediate threat data that only government entities have. The Chamber seeks to incent companies to share cyber threat data with appropriate industry peers and civilian government entities to bolster our critical infrastructure, lifeline, first responder, and business systems.

Critical Infrastructures' Awareness of the Framework Is Strong; Sector Activities Are Robust and Maturing

The Chamber believes that the release of the *Framework for Improving Critical Infrastructure Cybersecurity* (the framework) has been a remarkable success. The Chamber, sector-based coordinating councils and associations, companies, and other private and public entities collaborated closely with NIST in developing the framework since the first workshop was held in April 2013.

Critical infrastructure sectors are keenly aware of and supportive of the framework. The Chamber understands that critical infrastructures at "greatest risk" have been identified and engaged by administration officials under the terms of the cyber executive order (EO).[3] Government officials ought to ensure that all resources, particularly the latest cyber threat indicators, are available to these enterprises to counter increasing and advanced threats.

Further, important elements of U.S. industry are aware of the framework and are using it or similar risk-management tools. Indeed, the Chamber welcomed an assessment from Michael Daniel, White House special assistant to the president and cybersecurity coordinator, who remarked on September 23 at the Chamber's third cyber roundtable in Everett, Washington, that industry's response to the framework has been "phenomenal." A second White House official, Ari Schwartz, senior director for cybersecurity, noted on October 1 that business support for the framework has "exceeded expectations." Such recognition is constructive and helps keep the private sector engaged in using the framework and promoting it with business partners.[4]

Much of industry's favorable reaction is owed in large measure to NIST, which tackled the framework's development in ways that ought to serve as a model for other agencies and departments. In May, the administration sent the business community a powerful message, saying that the framework should remain collaborative, voluntary, and innovative over the long term.[5] Interestingly, public focus on the framework has created visibility into industry's

[3] Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity*, is available at www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

[4] See "At eight-month mark, industry praises framework and eyes next steps," *Inside Cybersecurity*, October 6, 2014, http://insidecybersecurity.com/Cyber-Daily-News/Daily-News/at-eight-month-mark-industry-praises-framework-and-eyes-next-steps/menu-id-1075.html.

[5] The Chamber agrees with Michael Daniel's May 22 blog, *Assessing Cybersecurity Regulations*, at www.whitehouse.gov/blog/2014/05/22/assessing-cybersecurity-regulations. The blog says that business and government "must build equally agile and responsive capabilities not bound by outdated and inflexible rules and procedures." The Chamber especially 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.

long-standing efforts to address cyber risks and threats—constant, dedicated, and (mostly) silent efforts that preceded the creation of the framework.[6]

Most notable, since the framework's release in February, industry has demonstrated its commitment to using it. Many associations are creating resources for their members and holding events across the country and taking other initiatives to promote cybersecurity education and awareness of the framework. Some examples are listed here. Associations are planning and exploring additional activities as well.

- The Alliance of Automobile Manufacturers and the Association of Global Automakers have initiated a process to establish an automobile industry sector information-sharing and analysis center (Auto-ISAC) to voluntarily collect and share information about existing or potential threats to the cybersecurity of motor vehicle electronics and in-vehicle networks.

- The American Chemistry Council (ACC) is developing sector-specific guidance based on the NIST cyber framework to further enhance and implement the council's Responsible Care® Security Code. ACC's Chemical Information Technology Center (ChemITC) is also piloting an ISAC for the chemical sector.

- The American Gas Association (AGA) has hosted a series of webinars on control system cybersecurity and is working with small utilities to develop robust cybersecurity programs. Among other activities, AGA has stood up the Downstream Natural Gas Information and Analysis Center (DNG–ISAC), an ISAC designed to help support the information-sharing interests of downstream natural gas utilities.

- The American Hotel & Lodging Association (AH&LA) has conducted a series of widely attended cyber and data security webinars to assist small, medium, and large hotel and lodging businesses with implementing key information security measures and risk assessments.

- The American Water Works Association (AWWA) has created cybersecurity guidance and a use-case tool to aid water and wastewater utilities' implementation of the framework. The guidance is cross-referenced to the framework. This tool is serving as implementation guidance for the framework in the water and wastewater systems sector.

- Members of the Communications Sector Coordinating Council (CSCC)—made up of broadcasting, cable, wireline, wireless, and satellite segments—have participated in multiple NIST, Department of Homeland Security (DHS), and industry association-sponsored programs, webinars, and panels with future events being planned.

  In addition, the communications sector has roughly 100 cybersecurity experts engaged in the Federal Communication Commission's (FCC's) voluntary Communications Security Reliability and Interoperability Council (CSRIC) to adapt the framework for the sector

[6] The online publication *Inside Cybersecurity* provides an excellent catalog of industry initiatives to implement data- and network-security best practices. See http://insidecybersecurity.com/Sectors/menu-id-1149.html.

segments, focusing on an understanding of shared responsibilities across the ecosystem, the impact on small and medium enterprises, evolving threats, and barriers to implementing specific risk-management capabilities.

- The Electricity Subsector Coordinating Council has worked with the Department of Energy (DOE) to develop sector-specific guidance for using the framework. The guidance leverages existing subsector-specific approaches to cybersecurity, including DOE's *Electricity Subsector Cybersecurity Risk Management Process Guideline*, the *Electricity Subsector Cybersecurity Capability Maturity Model*, NIST's *Guidelines for Smart Grid Cyber Security*, and the North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection Cybersecurity Standards.

- The mutual fund industry, represented by the Investment Company Institute (ICI), has added to its committee roster a Chief Information Security Officer Advisory Committee. The committee's mission is to collaborate on cybersecurity issues and information sharing in the financial services industry and provide a cyber-threat protection resource for ICI members.

- The Information Technology Industry Council (ITI) visited Korea and Japan and shared with these countries' governments and business leaders the benefits of a public-private partnership-based approach to developing globally workable cybersecurity policies. ITI highlighted the framework as an example of an effective policy developed in this manner, reflecting global standards and industry-driven practices.

- The National Association of Manufacturers (NAM) has spearheaded the D.A.T.A. (Driving the Agenda for Technology Advancement) Policy Center, providing manufacturers with a forum to understand the latest cybersecurity policy trends, threats, and best practices. The D.A.T.A. Center focuses on working with small and medium-size manufacturers to help them secure their assets.

- Through the American Petroleum Institute (API), the oil and natural gas sector has worked with DOE to complete the Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model (ONG-C2M2). The oil and natural gas sector in 2014 established a new Oil and Natural Gas Information Sharing and Analysis Center (ONG–ISAC) to provide shared intelligence on cyber incidents, threats, vulnerabilities, and responses throughout the industry.

- The Retail Industry Leaders Association (RILA), in partnership with the National Retail Federation (NRF), has created the Retail Cyber Intelligence Sharing Center (R–CISC), featuring information sharing, research, and education and training. This ISAC enables retailers to share threat data among themselves and receive threat information from government and law enforcement partners.

- The U.S. Chamber of Commerce has launched its national roundtable series, *Improving Today. Protecting Tomorrow*™, recommending that businesses of all sizes and sectors adopt fundamental Internet security practices.

The Chamber Is Conducting Extensive Outreach to Local Chambers; Policymakers Need to Focus on Passing Information-Sharing Legislation and Deterring Foreign Attackers
The new framework is designed to help organizations start a cybersecurity program or improve an existing one. The framework puts cybersecurity into a common language for organizations to better understand their cybersecurity posture, set goals for cybersecurity improvements, monitor their progress, and foster communications with internal and external stakeholders.

Looking ahead to 2015, the Chamber's cyber policy advocacy and framework education campaign intends to focus on several areas, including the following:

- **Organizing roundtables with local chambers and growing market solutions.** The Chamber is planning more cyber roundtables. In 2014, the Chamber organized roundtable events with state and local chambers in Chicago, Illinois (May 22); Austin, Texas (July 10); Everett, Washington (September 23); and Phoenix, Arizona (October 8) prior to the Chamber's Third Annual Cybersecurity Summit on October 28. Leading member sponsors of the campaign—*Improving Today. Protecting Tomorrow*™—are American Express, Dell, and Splunk. Other sponsors are Boeing, the Edison Electric Institute, HID, Microsoft, Oracle, and Pepco Holdings, Inc.

  The Chamber urges policymakers to commit greater resources over the next several years to growing awareness of the framework and risk-based solutions through a national education campaign. A broad-based campaign involving federal, state, and local governments and multiple sectors of the U.S. economy would spur greater awareness of cyber threats and aggregate demand for market-driven cyber solutions.

  The Chamber believes that government—particularly independent agencies—should devote their limited time and resources to assisting resource-strapped enterprises, not trying to flex their existing regulatory authority. After all, while businesses are working to detect, prevent, and mitigate cyberattacks originating from sophisticated criminal syndicates or foreign powers, they shouldn't have to worry about regulatory or legal sanctions.

- **Engaging law enforcement.** The Chamber plans to continue its close contact with the FBI and the U.S. Secret Service to build trusted public-private relationships, which are essential to confirming a crime and beginning criminal investigations. We are encouraging businesses to partner with law enforcement before, during, and after a cyber incident. FBI and U.S. Secret Service officials have participated in each of the Chamber's roundtables.

- **Passing information-sharing legislation.** The framework would be incomplete without enacting information-sharing legislation that removes legal and regulatory penalties to quickly exchange data about evolving threats to U.S. companies.

  Businesses want to participate in the online equivalent of a Neighborhood Watch program. Companies' security professionals seek to exchange cyber threat information and vulnerabilities with their peers and government, but they fear being penalized for doing the right thing. The Chamber strongly urges Congress to pass an information-sharing bill that contains strong protections related to lawsuits, public disclosure, regulations, and antitrust concerns and respects privacy.[7]

In addition, the cybersecurity EO elevates the importance of bidirectional information sharing and calls for expanding the public-private Enhanced Cybersecurity Services (ECS) program to critical infrastructure. The administration should give consideration to developing an ECS program that is affordable to small and midsize businesses (SMBs).

On the one hand, some businesses would be well equipped internally or in partnership with third-party providers to make use of cyber threat information. On the other hand, the Chamber believes that most SMBs, depending on their size and abilities, would need significant assistance with incorporating threat information into their organizations.

- **Harmonizing cybersecurity regulations.** Information-security requirements should not be cumulative. The Chamber believes it is valuable that agencies and departments are urged under the EO to report to the Office of Management and Budget any critical infrastructure subject to "ineffective, conflicting, or excessively burdensome cybersecurity requirements." We urge the administration and Congress to prioritize eliminating burdensome regulations on businesses. One solution could entail giving businesses credit for information security regimes that exist in their respective sectors that they have adopted.[8] It is positive that Michael Daniel, the administration's lead cyber official, has made harmonizing existing cyber regulations with the framework a priority.

- **Raising adversaries' costs through deterrence**. The Chamber is reviewing actions that businesses and government can take to deter nefarious actors that threaten to empty bank accounts, steal trade secrets, or damage vital infrastructures. While we have not formally endorsed the report, the U.S. Department of State's International Security Advisory Board (ISAB) issued in July draft recommendations regarding cooperation and deterrence in cyberspace.

  The ISAB's recommendations—including cooperating on crime as a first step, exploring global consensus on the rules of the road, enhancing governments' situational awareness through information sharing, combating IP theft, expanding education and capacity

[7] In an April 2013 letter to NIST regarding businesses' use of the framework and the role of incentives, the Chamber provides its views on extending liability protections related to information-sharing legislation, extending a safe harbor related to using the framework, extending SAFETY Act applicability to the framework, eliminating cybersecurity regulations, leveraging federal procurement, and making the research and development (R&D) tax credit permanent. The letter is available at www.ntia.doc.gov/files/ntia/29apr13_chamber_comments.pdf.

[8] The business community already complies with multiple information security rules. Among the regulatory requirements impacting businesses of all sizes are the Chemical Facilities Anti-Terrorism Standards (CFATS), the Federal Energy Regulatory Commission-North American Reliability Corporation Critical Information Protection (FERC-NERC CIP) standards, the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), and the Sarbanes-Oxley (SOX) Act. The Securities and Exchange Commission (SEC) issued guidance in October 2011 outlining how and when companies should report hacking incidents and cybersecurity risks. Corporations also comply with many non-U.S. requirements, which add to the regulatory mix.

building, promoting attribution and prosecution, and leading by example—are sensible and worthy of further review by cybersecurity stakeholders.[9]

The Chamber believes that the United States needs to coherently shift the costs associated with cyber attacks in ways that are legal, swift, and proportionate relative to the risks and threats. Policymakers need to help the law enforcement community, which is a key asset to the business community but numerically overmatched compared with illicit hackers.[10]

Roadmap for the Future of the Cybersecurity Framework

In February, NIST released a *Roadmap* to accompany the framework. The *Roadmap* outlines further areas for possible "development, alignment, and collaboration."[11] Here are some key areas that the Chamber sees as needing more attention:

- **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 believes that 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 industry-driven 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.[12]

  The administration should organize opportunities for stakeholders to participate in multinational discussions. The Chamber wants to encourage the federal government to work with international partners and believes that these discussions should be stakeholder driven and occurring on a routine basis.

- **Avoiding disruptions to the framework's privacy methodology.** The Chamber appreciates that NIST struck Appendix B of 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 believes that the privacy methodology must be consensus based and straightforward. A privacy methodology that would attempt to apply privacy principles to most features of the framework or to

[9] The ISAB report is available at www.state.gov/documents/organization/229235.pdf.

[10] The Chamber argues for a clear cyber deterrence strategy in its December 2013 letter to NIST on the framework. See http://csrc.nist.gov/cyberframework/framework_comments/20131213_ann_beauchesne_uschamber.pdf.

[11] The *Roadmap* is available at www.nist.gov/cyberframework/upload/roadmap-021214.pdf.

[12] 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 is best achieved when organizations follow voluntary global standards and industry-driven practices.

recommend burdensome practices would create significant disincentives to businesses' implementing the framework.[13]

The Chamber welcomes the outreach that NIST officials have had with us regarding its new privacy engineering initiative and wants 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 a standards-setting effort that first requires a multistakeholder process to articulate consensus policy goals. However, the Chamber is concerned that the privacy engineering initiative, as presently conceived, would endorse potential policy objectives prematurely, rather than integrate consensus-based and broadly adopted policies into a technical standard.

We strongly caution NIST against pursing a privacy engineering initiative that would (perhaps unintentionally) undermine the progress that industry and NIST have made in creating and launching 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 roundtable series, 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 and disruption. NIST should provide additional guidance in this area.

  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 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.[14]

[13] For more on this argument, see Harriet Pearson's December 5, 2013, letter to NIST on the preliminary framework at http://csrc.nist.gov/cyberframework/framework_comments/20131205_harriet_pearson_hoganlovells.pdf.

[14] See May 13, 2013, *Federal Register*, pp. 27966–27967, at 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."

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.

Let's Increase the Framework's Success by Improving Collaboration and Eliminating Barriers to Smart and Efficient Cybersecurity

NIST and multiple stakeholders produced a smart framework that participants can take pride in. But more work lies ahead. The Chamber looks forward to working with policymakers to ensure that preexisting regulations are harmonized with the collaborative and voluntary nature of the framework. Businesses also seek the enactment of information-sharing legislation to achieve timely and actionable situational awareness to improve our detection, mitigation, and response capabilities.

The Chamber is committed to protecting America's business community and enhancing the nation's resilience against an array of physical and cyber threats. Government and business entities need to continue leveraging the framework to strengthen collective resilience and security and make ongoing improvements. We look forward to working with NIST and policymakers to build on the progress that we—industry and government—have made together.

The Chamber appreciates the opportunity to answer questions related to the RFI. For further 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 Beauchesne

Ann M. Beauchesne