Statement of the U.S. Chamber of Commerce

ON:	**Building a More Secure Cyber Future: Examining Private Sector Experience With the NIST Framework**
TO:	**Senate Commerce, Science, and Transportation Committee**
BY:	**Ann M. Beauchesne, Vice President, National Security and Emergency Preparedness**
DATE:	**Wednesday, February 4, 2015**

The Chamber's mission is to advance human progress through an economic, political, and social system based on individual freedom, incentive, initiative, opportunity, and responsibility.

Ann M. Beauchesne
Vice President, National Security and Emergency Preparedness, U.S. Chamber of Commerce
U.S. Senate Committee on Commerce, Science, and Transportation
Hearing entitled "Building a More Secure Cyber Future:
Examining Private Sector Experience With the NIST Framework"
Wednesday, February 4, 2015

Good morning, Chairman Thune, Ranking Member Nelson, and other distinguished members of the committee. My name is Ann Beauchesne, and I serve as vice president of the U.S. Chamber's National Security and Emergency Preparedness Department. On behalf of the Chamber, I welcome the opportunity to testify before the Senate Commerce committee regarding the business community's experience with the National Institute of Standards and Technology's (NIST's) *Framework for Improving Critical Infrastructure Cybersecurity* (the framework).[1]

The National Security and Emergency Preparedness Department was established in 2003 to develop and implement the Chamber's homeland and national security policies. The department works through the National Security Task Force, a policy committee composed of roughly 200 Chamber members representing practically every sector of the American economy. The task force's Cybersecurity Working Group identifies current and emerging issues, crafts policies and positions, and provides analysis and direct advocacy to government and business leaders.

The need to address increasingly sophisticated threats against U.S. and global businesses has gone from an IT issue to a top priority for the C-suite and the boardroom. Chamber President and CEO Thomas J. Donohue recently said, "In an interconnected world, economic security and national security are linked. To maintain a strong and resilient economy, we must protect against the threat of cyberattacks."

My statement focuses on the successful rollout of the framework and the positive collaboration that many businesses and government entities have developed over the past several months, including our new cybersecurity campaign—*Improving Today. Protecting Tomorrow*™. I am also going to highlight policy issues—information-sharing legislation being the top legislative 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]

The framework is a good start, but more work is needed to push back against skilled attackers. Most small and midsize businesses (SMBs) tend to lack the money and personnel to beat back highly advanced and nefarious actors, such as organized criminal gangs and groups carrying out state-sponsored attacks. No single strategy can prevent advanced and persistent threats—popularly known as APTs in cybersecurity jargon—from breaching an organization's cyber defenses.

[1] See www.nist.gov/cyberframework.

[2] The Chamber submitted in October 2014 similar comments to National Institute of Standards and Technology (NIST) related to businesses' awareness and use of the framework. See http://csrc.nist.gov/cyberframework/rfi_comments_10_2014.html.

Policymakers have not sufficiently acknowledged this expensive, practical reality. American companies should not be expected to shoulder the substantial costs of cyberattacks emanating from well-resourced bad actors such as criminal syndicates or nation-states—costs typically absorbed by national governments. Nation-states or their proxies and other sophisticated actors are apparently hacking businesses with impunity—and that has got to stop.

In addition to having policymakers acknowledge cost concerns, the Chamber would welcome working with the administration and Congress on establishing an intelligent and forceful deterrence strategy, which the United States currently lacks. U.S. policymakers need to focus on pushing back against illicit actors and not on blaming the victims of cybersecurity incidents.[3]

The Framework Is an Excellent Example of an Effective Public-Private Partnership; Critical Infrastructure Awareness of the Framework Is Strong, and Sector Activities Are Robust and Maturing

The Chamber believes that the framework—which was released last February—has been a success. The framework represents one of the best examples of public-private partnerships in action. NIST and stakeholders in the public and private sectors should have a great sense of accomplishment. The Chamber, sector-based coordinating councils and associations, companies, and other 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).[4] 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, 2014, 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, 2014, 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.[5]

---

[3] The Chamber submitted comments to the Department of Homeland Security (DHS) on cybersecurity solutions for small and midsize businesses (SMBs) in April 2014.

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

[5] 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.

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 2014, the administration sent the business community a powerful message, saying that the framework should remain collaborative, voluntary, and innovative over the long term.[6] Interestingly, public focus on the framework has created visibility into industry's long-standing efforts to address cyber risks and threats—constant, dedicated, and (mostly) silent efforts that preceded the creation of the framework.[7]

Most notable, since the framework's release, 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, is collaborating with small utilities to develop robust cybersecurity programs, and is working with companies to review and enhance their cybersecurity posture using the Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model (ONG-C2M2) from the Department of Energy (DOE). 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.

---

[6] 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 and industry partners especially urge independent agencies and Congress to adhere to the dynamic approach advocated by the administration and that is embodied in the nonregulatory, public-private framework. See June 11, 2014 letter, available at www.uschamber.com/sites/default/files/documents/files/11June14GroupLetterT-YReplytoDanielCyberBlog_Final_0.pdf.

[7] 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.

- 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. The sector is completing a year-long effort within the Federal Communication Commission's (FCC's) Communications Security Reliability and Interoperability Council (CSRIC) that involves more than 100 professionals who have worked to adapt the NIST framework to the sector segments and provide guidance to the industry.

- The Electricity Subsector Coordinating Council has worked with 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 in May 2014 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. ITI principals also spoke at a U.S.-European Union (EU) workshop in Brussels in November 2014, comparing U.S. and EU policy approaches to cybersecurity and highlighting the positive attributes of the framework and its development.

- 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 to 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's New Cybersecurity Campaign Enters Its Second Year; Policymakers Need to Focus on Passing Information-Sharing Legislation and Deterring Foreign Attackers

The NIST framework is designed to help s 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 cybersecurity 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 2015. Last year, 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 were American Express, Dell, and Splunk. Other sponsors were the American Gas Association, Boeing, the Edison Electric Institute, Exelon, HID Global, Microsoft, Oracle, and Pepco Holdings, Inc., and *The Wall Street Journal*.

  Each roundtable featured cybersecurity principals from the White House, DHS, NIST, and local FBI and U.S. Secret Service officials. The Chamber and our partners urged businesses to adopt fundamental Internet security practices to reduce network and system weaknesses and make the price of successful hacking increasingly steep. The Chamber also urged businesses to improve their cyber risk management processes. All businesses should understand common online threats that can lead them to become victims of cybercrime. Using the framework and similar risk management tools, such as the

Chamber's *Internet Security Essentials for Business 2.0* guidebook,[8] is ultimately about making your business more secure and resilient. The Chamber encouraged businesses to report cyber incidents. Perfect online security is unattainable, even for large businesses. Innovative solutions are regularly being brought to market because cyber threats are always changing. Businesses should report cyber incidents and online crime to their FBI or U.S. Secret Service field offices.

- **Increasing public awareness of the framework.** 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.

- **Improving information-sharing is job No. 1.** The framework would be incomplete without enacting information-sharing legislation that removes legal and regulatory penalties to quickly exchange data about threats to U.S. companies.

  - **Passing legislation this year.** Last week, 35 associations, including the Chamber, strongly urged the Senate to quickly pass a cybersecurity information-sharing bill.[9] The Senate Intelligence committee passed a smart and workable bill in July 2014, which earned broad bipartisan support. Recent cyber incidents underscore the need for legislation to help businesses improve their awareness of cyber threats and enhance their protection and response capabilities.

    Above all, the Chamber urges Congress to send a bill to the president that gives businesses legal certainty that they have safe harbor against frivolous lawsuits when voluntarily sharing and receiving threat indicators and countermeasures in real time and taking actions to mitigate cyberattacks. The legislation also needs to offer protections related to public disclosure, regulatory, and antitrust matters in order to increase the timely exchange of information among public and private entities.

[8] The booklet is available free for downloading at www.uschamber.com/issue-brief/internet-security-essentials-business-20.

[9] The coalition letter is available at www.uschamber.com/sites/default/files/150127_multi-association_cyber_info-sharing_legislation_senate.pdf.

The Chamber also believes that legislation needs to safeguard privacy and civil liberties and establish appropriate roles for civilian and intelligence agencies. The cybersecurity measure approved in July 2014 by the Senate Intelligence committee reflected practical compromises among many stakeholders on these issues.

Cyberattacks aimed at U.S. businesses and government entities are being launched from various sources, including sophisticated hackers, organized crime, and state-sponsored groups. These attacks are advancing in scope and complexity. Congressional action cannot come quickly enough.

- **Helping SMBs mitigate attacks.** 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 consider developing an ECS program that is affordable to 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, depending on their size and abilities, most SMBs would need significant guidance and perhaps additional assistance with incorporating threat information and risk management strategies into their organizations.

- **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.

- **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.[10] It is positive that Michael Daniel, the administration's lead cyber official, has made harmonizing existing cyber regulations with the framework a priority.

[10] 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.

- **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 building, promoting attribution and prosecution, and leading by example—are sensible and worthy of further review by cybersecurity stakeholders.[11]

  The Chamber believes that the United States needs to coherently shift the costs associated with cyberattacks 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.[12]

- **Making incentives work.** 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 (see p. 6 of this statement), 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.[13]

  The Chamber appreciates that the administration is assessing a mix of incentives that could induce businesses to use the framework.[14] However, in the Chamber's view, it is imperative that the administration, independent agencies, and lawmakers extend to companies the assurance that the cybersecurity framework and any actions taken in relation to it remain collaborative, flexible, and innovative over the long term. The Chamber believes that the presence of these qualities, or the lack thereof, would be a key determinant to use of the framework by U.S. critical infrastructure as well as businesses generally.

Roadmap for the Future of the Cybersecurity Framework

In February 2014, NIST released a *Roadmap* to accompany the framework. The *Roadmap* outlines further areas for possible "development, alignment, and collaboration."[15] The Chamber

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

[12] 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.

[13] The letter is available at www.ntia.doc.gov/files/ntia/29apr13_chamber_comments.pdf.

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

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

noted in an October 2014 letter to NIST some key areas that we see as needing more attention. The Chamber would highlight for the committee the importance of 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.[16] The administration should organize opportunities for stakeholders to participate in multinational discussions. The Chamber encourages the federal government to work with international partners and believes that these discussions should be stakeholder driven and occur on a routine basis.

The Public and Private Sectors Need to 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 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 Congress and the administration to build on the progress that we—industry and government—have made together.

---

[16] 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. The Chamber argues that cybersecurity and resilience are best achieved when organizations follow voluntary global standards and industry-driven practices.