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

February 9, 2016

Via cyberframework@nist.gov

Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

**Subject: Views on the Framework for Improving Critical Infrastructure Cybersecurity**

Dear Ms. Honeycutt:

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 joint industry-National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* (the framework).[1]

The Chamber does not attempt to answer all 25 questions in the request for information (RFI). Instead, we focus on addressing aspects of the four main categories of inquiry—use of the framework, possible framework updates, sharing information on using the framework, and private sector involvement in the future governance of the framework—and related topics.[2]

**The Chamber and other industry organizations contributed significantly to the framework's development.**

The Chamber believes that the framework—which was released in February 2014—has been a notable success. The Chamber, sector-based coordinating councils and associations, companies, and other entities collaborated closely with NIST in creating the framework since the first workshop was held in April 2013. Critical infrastructure entities are very supportive of the framework. Indeed, crucial elements of U.S. industry are aware of the framework and are using it or similar risk management tools.

[1] www.federalregister.gov/articles/2015/12/11/2015-31217/views-on-the-framework-for-improving-critical-infrastructure-cybersecurity

[2] An appendix summarizes select points made in this letter.

The framework is a cost-effective mechanism for many private-sector organizations because NIST recommends a suite of standards, guidance, and best practices, but it avoids presuming to tell companies how to use them. Thus, a crucial strength of NIST's cybersecurity architecture is its flexibility regarding implementation.

The Chamber values the Obama administration's leadership on the voluntary framework, as well as the Department of Homeland Security (DHS) $C^3$ Voluntary Program, and urges the next administration to actively support it. The Chamber welcomes assessments of current and former White House officials who have remarked that industry's response to the framework has been "phenomenal" and has "exceeded expectations." Such recognition is positive and helps keep the private sector engaged in using the framework and promoting it with business partners.[3]

A May 2014 White House blog, *Assessing Cybersecurity Regulations*, set a meaningful tone for how the administration would view its role vis-à-vis the framework and industry. The blog sent businesses and other stakeholders an important message that the framework should remain collaborative, voluntary, and innovative over the long term.[4] In June 2014, the Chamber and nearly two dozen organizations sent a letter to Mr. Michael Daniel, special assistant to the president and cybersecurity coordinator, agreeing with him that businesses and government "must build equally agile and responsive capabilities not bound by outdated and inflexible rules and procedures."[5]

At the time, the Chamber called on policymakers to do two things: (1) enact cybersecurity information-sharing legislation and (2) press both executive branch agencies and departments and independent agencies—which are technically excluded from the prescriptions of the 2013 cybersecurity executive order (EO)—to adhere to the dynamic approach advocated by the administration and embodied in the nonregulatory framework.

The first job has been completed, but the second one remains an open question. In December 2015, the president signed into law cybersecurity information-sharing legislation that was contained in the omnibus spending measure (P.L. 114-113).[6] Yet in contrast to this constructive law, federal agencies and departments have yet to complete work on harmonizing preexisting regulations with the framework. Cybersecurity regulations should be compatible with the risk-based approach of the framework.

---

[3] The Chamber first noted its appreciation of administration officials' comments in an October 2014 letter (page 3) to the National Institute of Standards and Technology (NIST) concerning a previous RFI. It is available at http://csrc.nist.gov/cyberframework/rfi_comment_october_2014/20141010_uscc_eggers_rev1.pdf.

[4] www.whitehouse.gov/blog/2014/05/22/assessing-cybersecurity-regulations

[5] www.uschamber.com/sites/default/files/documents/files/11June14GroupLetterT-YReplytoDanielCyberBlog_Final_0.pdf

[6] www.congress.gov/bill/114th-congress/house-bill/2029/text

**Industry is enthusiastically using and promoting the framework.**

Much of industry's favorable reaction to the framework is owed in large part to NIST, which tackled the framework's development in ways that ought to serve as a model for other agencies and departments. Interestingly, increasing public attention 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]

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 members of the Alliance of Automobile Manufacturers and the Association of Global Automakers have established an automobile industry sector information-sharing and analysis center (Auto-ISAC) to facilitate the sharing of existing or potential threats to motor vehicle cybersecurity among members of the industry. In addition, members of the two associations have recently released a *Framework for Automotive Cybersecurity Best Practices* (the auto framework). The auto framework was developed in consultation with NIST. Building on the auto framework, the industry plans to begin developing automotive cybersecurity best practices and will continue to collaborate with external stakeholders and cybersecurity experts as appropriate.

- The American Chemistry Council (ACC) is developing sector-specific guidance based on the NIST cyber framework to further enhance and administer the council's Responsible Care® Security Code. ACC's Chemical Information Technology Center (ChemITC) is completing a pilot program to implement 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.

- 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.

[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/sector-initiatives.

- 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 serves as guidance for using the framework in the water and wastewater systems sector.

- The Automation Federation (the federation) is a nonprofit association made up of 16 member organizations and 7 working groups representing more than 500,000 automation and technology professionals worldwide. In 2013, the federation committed to working with the White House and NIST to help them develop the framework. With the launch of the framework in 2014, the federation conducted eight framework seminars throughout the United States and in London.

  These informational programs provided manufacturing and business leaders with the opportunity to learn more about the framework and the role it plays in addressing the cybersecurity threat against critical infrastructure.

  In 2015, the federation continued its commitment to instruct business professionals on how to implement the framework, and the organization recommended that certain automation security standards be incorporated as essential framework components. The federation is continuing its outreach efforts in 2016.

- The Communications Sector Coordinating Council (CSCC) is the primary venue for collaborative cybersecurity activities with the council's government partners and is made up of the broadcast, cable, satellite, wireless, and wireline industries. Council members have participated in multiple NIST and National Telecommunications and Information Administration (NTIA) engagements, have supported DHS' $C^3$ Voluntary Program to promote the framework, and, through their industry associations, have sponsored framework-related educational programs, webinars, and panels.

  The sector is implementing the recommendations and guidance set forth in the Federal Communication Commission's (FCC's) Communications Security Reliability and Interoperability Council's (CSRIC's) landmark adaptation of the framework—the *Cybersecurity Risk Management and Best Practices (Working Group 4)* report. Producing this report consumed the time of more than 100 cybersecurity professionals over the course of 12 months.

- 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's) Critical Infrastructure Protection Cybersecurity Standards.

- The financial services sector has incorporated the framework as the basis for its sector-wide *All-Hazards Crisis Response Playbook* (the playbook). Developed and maintained

by the Financial Services Information Sharing and Analysis Center (FS-ISAC), the playbook was trimmed from more than 70 pages to 10 pages and redesigned for cyber and business resiliency executives and crisis response teams. Industry exercises, such as the Quantum Dawn series and the Hamilton series, have repeatedly pointed to the need for a unified, useable playbook. Similar to the framework, the playbook was developed over a six-month period relying heavily on public and private feedback and recommendations.

The playbook puts into operations the framework's response and recovery controls at a critical sector level. It also provides a means for businesses to develop their cybersecurity programs over time. The language of the framework controls is identifiable in the five main playbook components: (1) Financial Sector (FS) crisis communication; (2) FS Crisis Response Coordination; (3) Government Crisis Response Coordination; (4) Associations, Regional, and Multi-Sector Crisis Coordination; and (5) Sector Contingency Plans and Event Closure.

The succinct structure of the playbook ensures ease of use when responding to crises. The response and recovery activities of both public and private groups are defined throughout the playbook so that crucial sector teams and individuals will know their roles, as well as the roles of government entities, other sectors, and third parties.

Supplementing the playbook is a library that features crisis resource guides, event-specific plans, and templates for use during exercises. For example, playbook templates provide a method for the sector to incorporate lessons learned and identify improvements for future incidents and exercises. The FS-ISAC maintains the library and makes updates based on exercises and real-world experiences. Financial sector leadership is expanding the 2016 sector exercise program to promote and make broader use of the playbook throughout industry.

- 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.

  ITI principals also spoke at a U.S.-European Union (EU) workshop in Brussels, comparing U.S. and EU policy approaches on cybersecurity and emphasizing the positive attributes of the framework and its development. In addition, ITI has conducted outreach regarding the framework in Germany, India, and China.

- The mutual fund industry, represented by the Investment Company Institute (ICI), regularly shares information on threats and mitigation strategies via meetings of its Chief Information Security Officer Advisory Committee. ICI hosts one-day Cybersecurity Forums involving ICI members, security vendors, consultants, and law enforcement entities in the United States and London. In addition, ICI developed a detailed cybersecurity survey for its members, which has shown that many firms' cybersecurity

programs are consistent with the framework and that most companies use an amalgam of standards and guidelines in developing and maintaining their information security programs.

Moreover, the survey results enable a firm to see how it compares with its peers and direct resources according to security priorities. Finally, the ICI hosted an open house in Washington, D.C., featuring the FBI and the Secret Service, so that ICI members could discuss the threat environment and personally engage law enforcement agents who have direct responsibility for cyber investigations in 40 field offices across the country.

- The National Restaurant Association (NRA) created and widely distributed last year the *Cybersecurity 101: A Toolkit for Restaurant Operators* guide that details the five functions of the framework in order to assist restaurant operators and executives in adopting an enterprisewide cybersecurity program. Further, the NRA has convened a working group of member companies to develop a cybersecurity framework for the restaurant industry, a sector-specific guidance based on the NIST framework for use by single-unit restaurant operators. More than 7 in 10 restaurants are single-unit operations. The NRA has also hosted NIST for presentations on the cyber framework during association events, including webinars and executive study groups.

- 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 an 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), 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 transportation sector has conducted a joint government-industry initiative to offer guidance to businesses on using the framework as a risk management tool. The Transportation Systems Sector Cybersecurity Working Group (TSSCWG)—made up of officials with the Transportation Security Administration (TSA), the Department of Transportation (DOT), the Coast Guard, and of representatives for each of the transportation modes—provided the forum for this cooperative effort. The working group's guidance has contributed substantially to common understandings of the

framework and to a broader use of the framework by entities in each mode of the transportation sector.

The TSSCWG produced flexible guidance to facilitate businesses' use of the framework in ways adaptable to the varying sizes, resource bases, and risk profiles of organizations across the transportation sector. A key element of this approach is the development of cyber threat intelligence priorities, which are submitted to DHS and reflect the needs of TSSCWG members. By pooling public-private intelligence requirements together, the goal is to produce an up-to-date cyber threat picture, which should better instruct organizations' use of the framework in mitigating cyber risks. The TSSCWG is launching a cooperative effort with DHS to hone the transportation sector's intelligence priorities.

- The U.S. Chamber launched its cybersecurity roundtable series in 2014. This national initiative recommends that businesses of all sizes and sectors adopt fundamental Internet security practices, including using the framework and similar risk management tools, engaging cybersecurity providers, and partnering with law enforcement before cyber incidents occur.

  The Chamber is in the third year of its cybersecurity campaign. Eight regional roundtables and two summits in Washington, D.C. have been held since 2014. More events are planned in 2016, including in Detroit, Michigan, on March 10.[8] Each roundtable typically features cybersecurity principals from the White House, DHS, NIST, and local FBI and Secret Service officials.

Clearly, private sector organizations are (1) using the framework, (2) creating new resources to help their constituencies reduce risks to their cybersecurity, and (3) sharing best practices through formal and informal means. Industry is also (4) working with government entities to strengthen their information networks and systems against malicious actors.

To continue this significant progress, the Chamber urges policymakers to help agencies and departments with *streamlining existing regulations with the framework and maintaining the framework's voluntary nature*. We are not arguing for the rollback of current cybersecurity regimes, such as the critical infrastructure protection reliability standards for the electric sector.[9]

---

[8] 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. Last year, our organization led roundtables in Atlanta, Georgia (July 15); Minneapolis, Minnesota (September 16); Las Vegas, Nevada (September 30); and Durham, North Carolina (December 15). The Chamber's *Fourth Annual Cybersecurity Summit* was held on October 26. Each event included approximately 200 attendees.

The Chamber could not conduct its educational outreach without business support. Leading member sponsors of the 2014–2015 campaign were American Express, Armor, Dell, Dell SecureWorks, Duke, Ridge Global, Southern Company, Splunk, and U.S. Bank. Additional sponsors were the American Gaming Association, the American Gas Association, AT&T, Boeing, ClearForce, the Edison Electric Institute, Exelon, Finsectech, HID Global, Liberty Group Ventures, Microsoft, Oracle, Pepco Holdings, Inc., and *The Wall Street Journal*.

[9] https://s3.amazonaws.com/public-inspection.federalregister.gov/2016-01505.pdf, http://www.eei.org/issuesandpolicy/cybersecurity/documents/cybersecurity_faq.pdf

Nevertheless, the Chamber opposes the creation of new or quasi cybersecurity regulations on industry, especially when government authorities have not taken affected entities' perspectives into account. The Chamber also strongly cautions policymakers against relying heavily on metrics related to framework use given the extraordinary pace of change in the cybersecurity field.

**Policymakers need to prioritize harmonizing domestic cybersecurity regulations with the framework.**

The Chamber appreciates NIST's question regarding streamlining existing regulations with the framework. NIST asks (question No. 9), "What steps should be taken to 'prevent duplication of regulatory processes and prevent conflict with or superseding of regulatory requirements, mandatory standards, and related processes' as required by the Cybersecurity Enhancement Act of 2014?" Policymakers have contemplated[10] the issue of regulatory harmonization, but work in this area is incomplete.

The Chamber holds that policymakers need to act more vigorously to reduce duplicative and overly burdensome cybersecurity requirements impacting regulated organizations, as called for under the cybersecurity EO and the Cybersecurity Enhancement Act of 2014.

**Identifying and Reducing the Regulatory Burden**

- **2013 cybersecurity executive order (EO), 13636—**First, section 10(a) of the EO directs executive branch departments and agencies with responsibility for regulating the security of private-sector critical infrastructure to assess the *sufficiency* of existing regulatory authority given current and projected risks.

  However, much critical infrastructure is regulated by independent regulators. Therefore, only a limited subset of CI regulators tied to the chemical, health, transportation, and water sectors submitted assessments to the White House by roughly May 2014. Independent regulatory agencies may engage in similar analyses but are not required to under this EO.

  Second, section 10(c) calls on executive branch agencies with regulatory authority over critical infrastructure to report within two years (February 2016) to the Office of Management and Budget (OMB) on any private entities subject to "*ineffective, conflicting, or excessively burdensome cybersecurity requirements*" [italics added].[11]

---

[10] For instance, an August 2013 White House blog says, "Agencies will continue to ensure that the Framework and the [DHS] Voluntary Program interact in an effective manner with existing regulatory structures. As the Framework and Voluntary Program are developed, agencies will recommend other areas that could help make compliance easier, for example: eliminating overlaps among existing laws and regulation, enabling equivalent adoption across regulatory structures, and reducing audit burdens." www.whitehouse.gov/blog/2013/08/06/incentives-support-adoption-cybersecurity-framework.

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

- **Cybersecurity Enhancement Act of 2014 (P.L. 113-274)—**Section 101 of the act calls on the director of NIST to engage the private sector and government agencies (federal, state, and local) to "prevent duplication of regulatory processes and prevent conflict with or superseding of regulatory requirements, mandatory standards, and related processes."[12]

The intent of the framework is to build agile and responsive cybersecurity capabilities not captured by outdated and inflexible rules and procedures. The Chamber believes that any relevant agency—not simply NIST—ought to recommend to the highest levels of government ways to make using the framework easier, such as eliminating overlaps among existing laws and regulation, enabling equivalent adoption across regulatory structures, and reducing audit burdens.

As the table below succinctly illustrates, some government entities are forming genuine partnerships with industry to enhance the security and resilience of critical infrastructure and the United States; some agencies are seemingly exploring ways to flex their regulatory muscles; and some federal bodies are apparently abandoning the spirit, if not the precepts, of the 2013 EO and the 2014 act, which call for modernizing cybersecurity rules. A single business organization should not be beset by multiple cybersecurity rules coming from many agencies, which are likely to be conflicting or duplicative in execution.[13]

(Continue to the next page.)

[12] www.congress.gov/bill/113th-congress/senate-bill/1353/text

[13] The framework is supposed to help cut down on myriad requirements that companies have to contend with at the federal, state, and local levels. Indeed, states are increasingly getting into the regulatory mix. For example, Connecticut is proposing a Public Utility Company Cybersecurity Oversight Program, which would give companies the "opportunity to demonstrate, through annual meetings with government stakeholders, that they are adequately defending against cyber attacks."

Some companies respectfully pushed back. One business expressed a willingness to participate in private meetings with state regulators but resisted participating in annual meetings with other state officials. The company told Connecticut officials that it is already required to provide such reports regularly to various regulatory bodies. But the company was concerned that if *every state and the 130-plus countries in which it operates* all required periodic review meetings, or more, such a requirement would be excessively burdensome. The Chamber strongly shares this view. As important from a security standpoint, such extensive regulation would displace businesses' limited resources, which are intended for strengthening cybersecurity, not battling red tape.
http://insidecybersecurity.com/daily-news/connecticut-regulators-push-ahead-cyber-plan-reject-industry-critique

| Government Entity (Select Examples) | Comment | Status | |
|---|---|---|---|
| | | Workable | TBD |
| DHS/Chemical Facilities Anti-Terrorism Standards (CFATS) program | In May 2014, DHS "determined that there were no significant gaps between CFATS and RBPS-8 [a cyber standard]"[14] and the framework."[15] | ✓ | |
| DHS/Coast Guard (CG) | The CG, a law enforcement and regulatory agency, has authority to regulate maritime transportation security under specific laws. In May 2014, the CG recommended promoting the voluntary adoption of the framework by the maritime industry.[16]<br><br>On December 31, 2015, the CG submitted cybersecurity recommendations tracking with its voluntary, risk management approach to assist a United Nations agency that is developing international shipping cybersecurity guidelines.[17] | ✓ | |
| DHS/Transportation Security Administration (TSA) | In May 2014, the TSA said that while it has authority to regulate cybersecurity in the transportation sector, the agency "has pursued collaborative and voluntary approaches with industry since 2010." | ✓ | |
| Environmental Protection Agency (EPA) | EPA is responsible for regulating the security of critical infrastructure in the water and wastewater systems sector. In May 2014, the EPA wrote to the White House, saying that it "believes that a voluntary partnership model is a proven approach that will be effective for managing cybersecurity risks."<br><br>But EPA warned, "If the voluntary partnership model is not successful in achieving widespread implementation of the Cybersecurity Framework or, if warranted by a changing cybersecurity risk profile, the EPA can revisit the option of | | ✓ |

[14] www.dhs.gov/xlibrary/assets/chemsec_cfats_riskbased_performance_standards.pdf

[15] http://www.dhs.gov/publication/eo-13636-improving-ci-cybersecurity

[16] http://www.dhs.gov/publication/eo-13636-improving-ci-cybersecurity

[17] http://insidecybersecurity.com/daily-news/coast-guard-promotes-cyber-strategy-un-maritime-standards-body

| | | | |
|---|---|---|---|
| | using general statutory authority to regulate cybersecurity in the Water and Wastewater Systems sector."[18] | | |
| Federal Communications Commission (FCC) | The public-private Communications Security, Reliability and Interoperability Council (CSRIC) IV approved in March 2015 the *Cybersecurity Risk Management and Best Practices (Working Group 4)* report. Among other things, the working group developed guidance to help communications providers use the framework.[19] | ✓ | |
| Federal Financial Institutions Examination Council (FFIEC) | In 2015, agencies of the FFIEC—including the Office of the Comptroller of the Currency (OCC), the Board of Governor of the Federal Reserve System (Board), the Federal Deposit Insurance Corporation (FDIC), and the National Credit Union Administration (NCUA)—announced the development of a Cybersecurity Assessment Tool (CAT) to help financial institutions of all sizes assess their inherent cybersecurity risks and their risk management capabilities.[20]<br><br>However, the FFIEC did not adequately collaborate with the business community when crafting the CAT. Organizations such as the Financial Services Sector Coordinating Council (FSSCC) have recently written to the council, urging agencies to closely partner with the sector to develop a second version of the assessment that uses the framework "as its visual base and foundation," among other priorities.[21] | | ✓ |
| Health and Human Services (HHS) | HHS reported to the White House in early 2014, concluding, "All of the regulatory programs identified [in the HHS Section 10(a) analysis] operate within particular segments of the [Healthcare and Public Health] Sector, due to their own distinct legislatively-defined jurisdictions and | | ✓ |

[18] http://insidecybersecurity.com/cyber-public-content/epa-finding-regulatory-authority-cybersecurity-aids-white-house-voluntary

[19] The report notes (page 4), "The sector's participation in CSRIC WG4 was seen as an opportunity to assume the leadership urged by FCC Chairman Tom Wheeler in a speech delivered to the American Enterprise Institute in June 2014." https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf

[20] https://federalregister.gov/a/2015-17907

[21] September 21, 2015, letter from the Financial Services Sector Coordinating Council (FSSCC) to the Federal Financial Institutions Coordinating Council (FFIEC) responding to the Paperwork Reduction Act notice and request for comment (July 22, 2015, *Federal Register*). See the forthcoming letter from the FSSCC to NIST responding to the current framework RFI (December 11, 2015, *Federal Register*). Also see http://insidecybersecurity.com/daily-news/financial-group-regulators-reorient-cyber-tool-around-nist-framework, http://insidecybersecurity.com/daily-news/nist-process-could-help-address-cyber-reg-concerns-finance-sector.

| | | | |
|---|---|---|---|
| | purposes. Expanding any or each of these authorities solely to address cybersecurity issues would not be appropriate or recommended."[22]<br><br>A joint government-industry group is examining a plan on applying the framework across the health sector under section 405 of the Cybersecurity Act of 2015 (P.L. 114-113).[23] | | |
| National Highway Traffic Safety Administration (NHTSA) | A NHTSA official said in December 2015 that the agency is following a voluntary approach to cybersecurity. "We [NHTSA] think voluntary standards are key going forward." NHTSA hosted a roundtable in January 2015 with auto industry leaders to examine "sufficient and clear guidance" for equipment manufacturers in the auto industry to implement cybersecurity measures.[24] | | ✓ |
| Securities and Exchange Commission (SEC) | The SEC's Division of Investment management issued in April 2015 updated *Cybersecurity Guidance* for registered investment companies and registered investment advisers.[25]<br><br>In July 2015, the SEC issued a "concept release," *Possible Revisions to Audit Committee Disclosures*. The release suggested the commission's consideration of new disclosure requirements for audit committees related to "cyber risks, information technology risks, or other areas."[26] | | ✓ |

The Chamber's bottom-line message is that the framework is a sound baseline for businesses' cybersecurity practices, and it has the added benefit of being accessible to nontechnical professionals. As framework stakeholders begin the yearlong transition from the Obama administration to the next one, we want to sustain the view held by most businesses and policymakers that the framework is a policy and political *cornerstone* for managing enterprise cybersecurity risks and threats.

---

[22] http://www.phe.gov/Preparedness/planning/cip/Pages/eo13636.aspx

[23] www.congress.gov/bill/114th-congress/house-bill/2029/text

[24] http://insidecybersecurity.com/daily-news/nhtsa-official-praises-automotive-industrys-proactive-cyber-work, http://insidecybersecurity.com/daily-news/automakers-cite-autonomous-car-security-efforts-amid-regulatory-push

[25] www.sec.gov/investment/im-guidance-2015-02.pdf

[26] http://www.sec.gov/rules/concept.shtml

The Chamber's disposition is to oppose top-down regulations coming from agencies and departments—but not for its own sake. If, over time, the framework is used by some government entities as fly paper to affix new mandates, then such actions are bound to drive companies from the framework process, which would be highly counterproductive. Our organization does not want this outcome, and certainly public officials should not want it either. To be sure, the Chamber cannot expect government agencies to get rid of "ineffective, conflicting, or excessively burdensome cybersecurity requirements" overnight, but we can push policymakers to refrain from proliferating new red tape, which is contrary to effective risk-based principles governing cybersecurity.

Businesses share the goal of mitigating cybersecurity risks and are committing billions of dollars to the security and resilience of their enterprises. Most observers agree that regulations cannot possibly keep pace with bad actors and would lead to check-the-box security mandates that are costly, time-consuming, and ineffective—thus pulling businesses' limited resources away from cybersecurity and toward compliance. Such an outcome would harm both the nimbleness needed by companies to respond to incidents and public safety—it's the exact opposite effect that the framework initiative is trying to achieve.

**The framework is widely supported by industry and does not require major revisions; additional areas are worthy of NIST's attention.**

In February 2014, NIST released a *Roadmap* to accompany the framework.[27] The *Roadmap* outlines further areas for possible "development, alignment, and collaboration [with particular sectors and standards-developing organizations]." The Chamber contends that the framework is backed by many industry sectors essentially as it is written and does not need significant updating at this time. Meanwhile, here are some key areas that the Chamber sees meriting attention as NIST prepares for its workshop in April:[28]

- **Aligning international cybersecurity regimes with the framework.** Many Chamber members operate globally. We appreciate that NIST has been actively meeting with foreign governments urging 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.

  The current administration and the next one 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 amended the preliminary framework prior to finalization and

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

[28] In September 2015, the Chamber made similar comments in a letter to NIST concerning NIST Interagency Report (NISTIR) 8074, the draft *Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity*, which we supported.

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. Relatedly, 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.[29] The Chamber does not believe that the privacy engineering objectives and a privacy risk model outlined in NIST's draft *Privacy Risk Management for Federal Information Systems* (NISTIR 8062) are sufficiently mature to warrant inclusion in the framework.[30]

- **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, our member organizations have urged businesses to use the framework when communicating with partners, vendors, and suppliers. 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. NIST should provide additional guidance in this area, which the agency recognizes.[31]

  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 written comments to GSA and the Joint Working Group on Improving Cybersecurity and Resilience Through Acquisition regarding section 8(e) of the cyber EO.[32]

---

[29] 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 believes that the United States' engagement strategy should refrain from causing confusion with the privacy methodology in the framework.

[30] http://csrc.nist.gov/publications/drafts/nistir-8062/nistir_8062_draft.pdf

[31] See NISTIR 8074, volume 1, page 8.

[32] See the May 13, 2013, *Federal Register*, via www.gpo.gov/fdsys/pkg/FR-2013-05-13/pdf/2013-11239.pdf. Section 8(e) of the 2013 cybersecurity executive order (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.

- **Integrating a cyber threat profile.** As a potential complement to the framework, a cyber threat analysis could help businesses discern trends in malicious activity and apply the insights gained from intelligence and law enforcement sources such as DHS and the FBI. The federal government has gleaned threat data from hundreds of site visits and virtual engagements with public and private entities. Cybersecurity threat data would help the business community prioritize its risk mitigation activities. Here are some topics that a cyber threat profile could address:

  - Tactics commonly employed to gain illicit access to networks and systems.

  - Vulnerabilities in targeted systems and networks that are frequently exploited.

  - Indicators of illicit cyber activities often noted in post-incident analyses that were inadvertently missed by security professionals.

  - Protective measures often found lacking or absent in systems or programs that could have led to better outcomes.

  The aim of integrating a cyber threat profile isn't to produce an exhaustive analytical report. Rather, the intent is to carefully select useable data that individual analysts and incident response teams are frequently seeing based on their experiences in monitoring

and countering cyber threat activity. The resulting tool could, for instance, feature a top-five overview of the most common incidences manifested in each of the four topics suggested directly above.

***

The Chamber welcomes the chance to provide feedback on NIST's RFI. The framework represents a prime example of public-private partnerships in action. NIST and stakeholders in the public and private sectors should have a great sense of accomplishment. But our joint work continues. Our organization believes that the private sector should eventually govern the framework, but NIST needs to keep one hand on the wheel. NIST must maintain a key role in collaborating with industry and engaging foreign organizations and governments.

At a time when agencies and departments are developing flexible plans or directives to structure public-private approaches to cybersecurity, NIST's positive role in developing the framework is significant to the U.S. business community's cybersecurity interests at home and abroad. The Chamber holds that the United States and other countries benefit when the private sector can shape, in close collaboration with public-sector stakeholders, the development and revision of cybersecurity programs that businesses use whether voluntarily or because of a law or a regulation.

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 J. Eggers (meggers@uschamber.com; 202-463-5619).

Sincerely,

Ann M. Beauchesne

**Appendix: Summary of select points in the letter**

- The Chamber has been actively promoting the joint industry-National Institute of Standards and Technology (NIST) cybersecurity framework (the framework) since it was released in 2014.

- Chamber members are using the framework and urging business partners to manage cybersecurity risks to their information networks and systems.

- Industry is working with government entities to strengthen their information networks and systems against malicious actors.

- The framework is a cost-effective mechanism for many private-sector organizations because NIST recommends a flexible suite of standards, guidance, and best practices, but it avoids presuming to tell companies how to use them.

- The framework is backed by many industry sectors and does not need significant updating at this time.

- The Chamber strongly cautions policymakers against relying on metrics related to framework use given the extraordinary pace of change in the cybersecurity field.

- The Chamber urges policymakers to help agencies and departments with streamlining existing regulations with the framework and maintaining the framework's voluntary nature.

- The Chamber opposes the creation of new or quasi cybersecurity regulations, especially when government authorities have not taken affected entities' perspectives into account.

- The private sector is pushing foreign governments to use the flexible, nonregulatory framework as a model for business-government collaboration—but much more needs to be done by the U.S. government and industry.

- The private sector should eventually govern the framework, but NIST needs to maintain a key role in collaborating with industry and engaging foreign organizations and governments.

- The Chamber values the Obama administration's leadership on the voluntary framework and urges the next administration to actively support it.