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

December 13, 2013

Via csfcomments@nist.gov

Information Technology Laboratory
ATTN: Adam Sedgewick
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899-8930

Subject: *Preliminary Cybersecurity Framework* Comments

Dear Mr. Sedgewick:

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, appreciates the opportunity to comment on the National Institute of Standards and Technology's (NIST's) *Preliminary Cybersecurity Framework* (herein the Framework).[1]

For several years, the Chamber has advocated for legislation and policies that would build balanced and sustained relationships between business and government—unencumbered by legal and regulatory penalties—so that individuals could experiment freely and quickly counter extraordinarily fast-paced threats to the U.S. the business community.

We believe it is constructive that NIST has been given the responsibility to coordinate an environment where technical and security professionals come together to identify the most applicable and effective guidance throughout industry sectors and promote its implementation. The Chamber has valued NIST's involvement with developing the Framework. They have tackled a challenging assignment in ways that should serve as a model for other agencies and departments.

The Chamber is encouraged that administration officials have "heard a clear call on harmonization" regarding the regulatory aspects of the Framework, a topic that came up frequently at the November workshop in Raleigh, North Carolina. It was helpful to hear that

[1] www.nist.gov/itl/cyberframework.cfm; www.gpo.gov/fdsys/pkg/FR-2013-10-29/pdf/2013-25566.pdf; www.federalregister.gov/articles/2013/10/29/2013-25566/request-for-comments-on-the-preliminary-cybersecurity-framework

encouraging harmonization—and not creating new rules—is a top Department of Homeland Security (DHS) priority.[2] Similarly, a top DHS official noted last week that the goal of the Framework is "to create a market for performance goals," not a compliance market. "This is not a ruse to get regulation," the official stressed.[3] The Chamber urges other agencies and departments, not just DHS, to take a similarly nonregulatory approach to the Framework. We believe that the Framework must be collaborative, flexible, and innovative over the long term to genuinely help businesses counter cyber threats.

Four themes underpin the Chamber's letter:

- The Chamber believes that "adoption" of the Framework refers to a critical infrastructure *voluntarily using* the Framework as part of its risk management program.

- Appendix B of the current Framework is not a privacy methodology that the Chamber supports. However, we value good-faith efforts by administration and NIST officials to work with industry to produce a privacy methodology that is smart, targeted, and implementable. The overall Framework, which includes the privacy methodology, focuses fundamentally on critical infrastructure sectors; thus, the privacy methodology must not apply to commercial data activities outside of the Framework's narrow cybersecurity context. The Chamber urges NIST and the administration to produce a revised privacy methodology that industry can support prior to releasing the first version of the Framework in February 2014.

- With the launch of the Framework, the United States needs to strengthen its strategy to deter bad actors in cyberspace. Restraint needs to be a guiding principle. But the Chamber believes that the United States needs to redouble its efforts to shift the costs associated with cyber attacks on America's private sector to those responsible in ways that are timely, legal, and proportionate.

- The Chamber proposes collaborating with NIST after the February release of version 1.0 of the Framework to facilitate a lessons-learned venue to help businesses that use the Framework. We believe that NIST should continue playing a visible role, which lawmakers and the administration ought to support, in future efforts to update the Framework.

[2] http://insidecybersecurity.com/Cyber-Daily-News/Daily-News/officials-say-message-received-on-outstanding-cybersecurity-framework-issues/menu-id-1075.html

[3] http://insidecybersecurity.com/Cyber-Daily-News/Daily-News/dhs-officials-stress-need-to-focus-cybersecurity-framework-incentives-on-smaller-entities/menu-id-1075.html

NIST requests in their notice that stakeholders consider several questions.[4] The Chamber appreciates being able to provide the following perspectives:

1. **Does the Framework adequately define outcomes that strengthen cybersecurity and support business objectives?**

The Framework offers a road map for assisting a critical infrastructure to enhance its cybersecurity. Specifically, the Framework utilizes a linear profile mechanism, which entails comparing a business' "Current Profile" with its "Target Profile." A business is supposed to be able to sketch how it is managing cybersecurity risks and assess areas for improvement. Next, the Target Profile should guide how business and security professionals prioritize resources and measure progress toward their cybersecurity objectives.

It is positive that the Framework Profile tracks with the Chamber's recommendation in its April comments[5] urging NIST to use a cybersecurity capability maturity model as a means of reducing risks to critical infrastructure. In our view, key characteristics that a maturity model should offer businesses include:

- Enabling critical infrastructure owners and operators to evaluate and benchmark cybersecurity capabilities.

- Sharing best practices and other relevant information with industry partners as a means to improve cybersecurity capabilities.

- Assisting critical infrastructure owners and operators with prioritizing investments in cybersecurity.

2. **Does the Framework enable cost-effective implementation?**

It is too soon to say if the Framework enables cost-effective implementation. Complicating matters, many of the proposed incentives are not ready to support usage of the Framework.[6] However, the Chamber welcomes NIST's sensitivity to the issue of cost, since it is the owners and operators of critical infrastructure that must judge whether using the Framework is cost-effective relative to real or perceived gains in security. NIST appreciates that cybersecurity is just one of several costs related to managing risks and threats. Some organizations have relatively sufficient budgets to devote to human talent (in-house and external) and equipment; others do not.

The Framework should facilitate cost-effective implementation because so-called adoption is ostensibly voluntary and the usage of certain practices and controls is not mandatory.

---

[4] See p. i of the Framework, available at www.nist.gov/itl/upload/preliminary-cybersecurity-Framework.pdf, via www.nist.gov/itl/cyberFramework.cfm#.

[5] http://csrc.nist.gov/cyberframework/rfi_comments/040813_us_chamber_of_commerce.pdf; www.ntia.doc.gov/files/ntia/29apr13_chamber_comments.pdf

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

Helping with the cost factor, the Framework should allow organizations to use it and comply with an array of government information-security rules impacting a sector or an individual company.

A crucial variable to enabling efficiency is ensuring that using the Framework does not become a check-the-box exercise in which policymakers would have considerable influence. The Chamber believes that if lawmakers and agency and department leaders regulate in this space, the Framework would become bureaucratically sluggish over time and a barrier to Framework participation and enhanced security.

3. Does the Framework appropriately integrate cybersecurity risk management into business risk management?

The Chamber believes that the intended audience for the Framework is primarily critical infrastructure "at greatest risk," which is a relatively well-defined subset of critical infrastructure.[7] As such, the Framework is likely to be initially tested by entities that already have functioning enterprise risk management programs.

Several participants at the fifth Framework workshop debated the issue of what "adoption" of the Framework means.[8] The Chamber believes that adoption of the Framework refers to a critical infrastructure or any organization *voluntarily using* the Framework as part of its risk management processes. The bottom line is that voluntary usage of the Framework must allow for maximum flexibility in how an organization manages its cybersecurity risk and participates in the DHS Voluntary Program, which is called for under Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity*.

The Chamber welcomes NIST's position that adoption should not to be prescriptive, much less mandatory. According to NIST, *"An organization <u>adopts</u> the framework when it <u>uses</u> the Cybersecurity Framework as a key part of its systematic <u>process</u> for identifying, assessing, prioritizing, and/or communicating: cybersecurity risks, current approaches and efforts to address those risks, and steps needed to reduce cybersecurity risks as part of its management of the organization's broader risks and priorities"* [emphasis in original].[9]

---

[7] See section 9 of the February 2013 Executive Order (EO) 13636 titled *Improving Critical Infrastructure Cybersecurity*, which calls on the Homeland Security Secretary to identify critical infrastructure "at greatest risk"; it is available at www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

[8] www.nist.gov/itl/csd/5th-cybersecurity-framework-workshop-november-14-15-2013.cfm

[9] http://insidecybersecurity.com/iwpfile.html?file=pdf13%2Fcs12042013_nist_cybersecurity_framework_update.pdf; http://insidecybersecurity.com/Cyber-Daily-News/Daily-News/nist-works-on-adoption-definition-as-industry-groups-seek-recognition-of-cyber-efforts/menu-id-1075.html

4. Does the Framework provide the tools for senior executives and boards of directors to understand risks and mitigations at the appropriate level of detail?

The Chamber believes that NIST's inclusion of a *Message to Senior Executives on the Cybersecurity Framework* is helpful and concise.[10] Cybersecurity has emerged as a top priority for the Chamber. We believe that information security should be part of all businesses' risk management efforts.[11] In an interconnected world, economic security and national security are linked. The Chamber urges businesses to take the Framework out for a "test drive" to compare what activities the Framework calls for and what works in reality. The intent should be to improve the Framework by using it, including assisting boards and senior executives with prioritizing investments in cybersecurity. Indeed, the Chamber believes that the Framework needs to be developed and used in a manner that provides critical infrastructure owners and operators a return on their investments.

5. Does the Framework provide sufficient guidance and resources to aid businesses of all sizes while maintaining flexibility?

Some businesses may require assistance with implementing the Framework, particularly small and midsize companies. The Chamber thinks that certain companies could play a role in mentoring their business partners in setting up a cybersecurity program or strengthening one that is already in place.

While some businesses may need help in implementing the Framework, the Framework should not become prescriptive in nature, which is a message NIST and the administration have heard repeatedly from industry. Businesses are wary of the Framework becoming prescriptive over time, which speaks to agency or departmental rules and mandates. The Chamber anticipates that sector-specific organizations would play a role in contributing guidance and resources to facilitate industry's use of the Framework.

Crucial to maintaining flexibility, the Framework needs to state that using it is voluntary and that businesses do not need to undertake all the cybersecurity activities in the Framework core. Further, the Informative References are neither exhaustive nor mandatory. Businesses should freely implement other standards, guidelines, and best practices, which NIST acknowledges.

6. Does the Framework express existing practices in a manner that enables effective use?

It is too soon to say with accuracy whether the Framework expresses existing practices in a manner that enables effective use. Meanwhile, the Chamber would like to continue engaging NIST on how stakeholders can communicate cybersecurity practices in a manner that is accurate and consistent—but without sacrificing the flexibility businesses need to determine their own

---

[10] A draft, two-page letter to business leaders is available at www.nist.gov/itl/upload/discussion-draft_executive-overview-082813.pdf.

[11] See op-ed by Chamber president and CEO Thomas J. Donohue, *Cybersecurity = Economic Security*, which appeared in the September 30, 2013, editions of the *Washington Examiner* and the *Weekly Standard*.

"Current" and "Target" profiles.[12] For example, a critical infrastructure entity may recommend to an external business partner a Target Profile to convey important activities of the Framework core to prioritize. However, a key goal is for all stakeholders to communicate cybersecurity practices in a manner that compares "apples to apples" and "oranges to oranges" accurately, consistently, and flexibly.

7. Will the Framework be inclusive of, and not disruptive to, effective cybersecurity practices in use today, including widely used voluntary consensus standards that are not yet final?

NIST is commended for promoting the inclusion of industry-led, global cybersecurity standards and best practices developed by public-private standards development bodies. Each sector generally has a prioritized and flexible approach to cybersecurity that meets the requirements of its members. The cybersecurity Framework, in our view, should not duplicate or conflict with existing regulatory programs, such as the North American Electric Reliability Corporation (NERC) cybersecurity standards program. Similar programs exist in the banking, chemical and other sectors. All in all, it is too early to assess whether the Framework aligns with—and not interferes with—the cybersecurity practices utilized by critical infrastructure.

8. Will the Framework enable organizations to incorporate threat information?

The effective incorporation of cybersecurity threat information would probably vary from organization to organization, depending on its resources and sophistication. More to the point, the Chamber believes that the Framework would be incomplete without the enactment of information-sharing legislation that is supported by the business community. We welcome working with the administration and Congress toward this goal.

In our view, legislation is required to create a powerful sea change in the current information-sharing practices between government and the business community that reflects the conditions of an increasingly digital world.

The EO elevates the importance of bidirectional information sharing. This is a positive development that calls on government officials to produce timely, classified, and unclassified reports on cyber threats to specific targets, such as U.S. critical infrastructure. The Chamber urges the administration to support legislation that promotes the exchange of threat intelligence and protects companies that share this valuable information with appropriate government entities and industry peers.

9. Is the preliminary Framework presented at the right level of specificity?

This question is related to the fifth one, pertaining to the sufficiency of guidance and resources needed to adhere to the Framework. NIST has attempted to write an initial Framework that meets the needs of organizations of all sizes and sophistication. It is the Chamber's impression that the Framework would align initially with businesses that have mature cybersecurity operations. More specificity is not needed and would likely complicate a process that should be as straightforward and easy as possible. However, we urge NIST to continue working with industry to refine the Framework and its elements going forward.

---

[12] See section 3.3 of the preliminary Framework, *Communicating Cybersecurity Requirements with Stakeholders*, p. 12.

The last two questions deal with privacy and civil liberties and have been combined to streamline answering them.

10. Does the Framework provide the right level of specificity and guidance for mitigating the impact of cybersecurity measures on privacy and civil liberties?

and

11. Is the Framework sufficiently clear on how the privacy and civil liberties methodology [appendix B] is integrated with the Framework Core [appendix A]?

The Chamber, in its April 2013 letter to NIST regarding principles that should guide the development and implementation of the Framework, writes that our organization is committed to working with policymakers to ensure that the cybersecurity Framework includes protections related to personal privacy. The cyber EO directs NIST to include "methodologies . . . to protect individual privacy and civil liberties" in the Framework. Also, section 5 of the EO directs senior federal officials to base their agencies' protection of privacy and civil liberties on Fair Information Practice Principles (FIPPS).

The Chamber's interpretation of the EO and Framework concludes that protecting personal privacy is an important business consideration, but that such activity needs limiting to specific cybersecurity activities, which the administration has not yet articulated sufficiently. In addition, we believe that privacy-protection assessments should be weighed only in the context of the voluntary use of the Framework by critical infrastructure entities. The fundamental objective of the Framework is reducing cybersecurity risks that critical infrastructure entities face.[13]

The Framework's sprawling privacy methodology is troubling. The current draft contains broad-based privacy principles that do not have an obvious connection to the core Framework or cybersecurity. Most privacy advocates and security practitioners recognize that not all cybersecurity measures or controls have privacy implications. The Chamber believes that the privacy methodology overreaches and could be interpreted as applying FIPPS to virtually any public or private sector organization, particularly commercial data activities outside the narrow scope of cybersecurity activities conducted by critical infrastructure.

The Chamber urges the administration to make clear in the Framework that privacy protections are being contemplated only in the context of critical infrastructure cybersecurity activities, which we believe they recognize, and are not being used to establish broader privacy requirements for industry. One way that the administration can make clear that privacy protections are related strictly to critical infrastructure cybersecurity activities would be to strike appendix B altogether and include more tailored privacy statements into the Framework. An alternative privacy methodology has already been provided to NIST and the administration for

[13] The Chamber believes that the intended audience of the framework is mainly critical infrastructure "at greatest risk," a narrow field of critical infrastructure, which conforms to sound risk-management practices.

consideration.[14] The Chamber urges NIST and the administration to release a revised privacy methodology prior to issuing version 1.0 of the Framework in February 2014.

Deterring bad actors: The need to clarify and strengthen U.S. cybersecurity strategy

It is crucial to highlight that the Chamber views cybersecurity legislation and public policies favorably that answer the following two questions affirmatively:

- Do they help businesses counter threats to their computer systems and assets?

- Do they increase costs on nefarious actors, such as rogue hackers, criminal gangs, and groups carrying out cyber attacks at the behest of nation states?

The Chamber believes that the Framework has the potential to be a useful tool in assisting businesses with strengthening their cybersecurity. However, much more needs to be done to give businesses and government the implements they need to adequately increase costs on malicious cyber activity. The Framework, intentionally or not, is a tactic within the United States' strategy to counter serious threats to our nation's economic and national security. Despite the existence of written blueprints, such as ones related to global prosperity and defense,[15] the U.S. strategy is seemingly uncertain—both to many in the private sector and our adversaries alike. The Chamber believes that the United States needs to refocus national efforts toward heightening the costs on sophisticated attackers that would willfully hack America's private sector for illicit purposes.

Over the past several years, policy and legislation have tended to focus almost exclusively on regulating industry ("punishing the victim") or leveraging trade and investment measures in economically risky ways, which the Chamber views as a one-sided and losing proposition. Industry and government need to battle bad actors, not one another. Fortunately, due to NIST's work, the Framework should help create a more collaborative public-private approach to addressing cybersecurity threats, but the proof will be in the pudding.

We believe that the United States needs to coherently shift the costs associated with cyber attacks in ways that are timely, legal, and proportionate (relative to the risks and threats). Restraint needs to be the watchword, but nefarious actors that would attempt to empty bank accounts, steal intellectual property, or temporarily shut down vital infrastructure operations need to be held accountable. Policymakers need to help the law enforcement community, which is a key asset to the business community, but numerically overmatched compared to hackers.[16]

The Chamber believes that public and private sector stakeholders need to conduct a review of actions—including improved cyber defenses, which the Framework helps catalyze, and enhanced attribution capabilities—that can be appropriately and wisely taken by business

[14] http://csrc.nist.gov/cyberframework/preliminary_framework_comments.html

[15] www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (international) and www.defense.gov/news/d20110714cyber.pdf (defense)

[16] www.judiciary.senate.gov/pdf/5-8-13DemarestTestimony.pdf

and government to deter bad actors. In a global security environment that is characterized by asymmetric threats and risks, businesses are frequently left to their own devices. For deterrence to be effective, businesses should have a menu of legal options at their disposal, sending a credible message that cyber attacks on industry and government will not be tolerated.

Collaborating with NIST: Chamber proposes a lessons-learned forum to assist businesses and enhance Framework revisions

The Chamber appreciates the opportunity to offer our views on the preliminary Framework. NIST and administration officials have recognized that industry and government do not need to "reinvent the wheel" when it comes to cybersecurity standards. NIST officials have collaborated with the private sector and have not attempted to dictate preferred solutions. Agency officials have also listened to public criticisms of the preliminary Framework—negative and positive—since the very beginning, and they have incorporated industry feedback into the draft.

Much remains to be seen in terms of how the Framework is revised and implemented, especially the roles that regulatory agencies and departments would play. But the Chamber believes that a preferred outcome is one in which NIST's role is continued and elevated relative to other federal entities. NIST has played a positive role in helping critical infrastructure entities identify cybersecurity guidance, standards, and smart practices that are effective in improving their security and resilience.

Significantly, the Chamber would welcome collaborating with NIST after the February release of the Framework to offer a lessons-learned forum to help early users of the Framework maximize opportunities (e.g., identifying gaps in their cybersecurity processes) or minimize challenges (e.g., identifying gaps in the Framework itself and reducing regulations).[17] The goal would be to facilitate businesses helping one another and allow these interactions to inform revisions to the Framework.

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

Sincerely,

Ann M. Beauchesne

[17] http://insidecybersecurity.com/Cyber-Daily-News/Daily-News/nist-works-on-adoption-definition-as-industry-groups-seek-recognition-of-cyber-efforts/menu-id-1075.html