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

April 8, 2013

(Via cyberframework@nist.gov)

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

Dear Ms. Honeycutt:

The U.S. Chamber of Commerce, the world's largest business federation representing the interests of more than 3 million businesses and organizations of every size, sector, and region, appreciates the opportunity to comment on the National Institute of Standards and Technology (NIST) notice titled "Developing a Framework to Improve Critical Infrastructure Cybersecurity."[1]

Administration leaders deserve credit for previewing the cybersecurity executive order (EO) with some in the business community, and the Chamber looks forward to continuing the engagement.[2] In the comments that follow, we do not attempt to answer the dozens of questions in the notice. Instead, the Chamber offers several principles that, in our opinion, should underpin the creation of the cybersecurity framework and guide its implementation.

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 U.S. national security. 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.

---

[1] NIST notice available at www.gpo.gov/fdsys/pkg/FR-2013-02-26/pdf/2013-04413.pdf; see February 26, 2013, *Federal Register*, pp. 13024–13028.

[2] EO 13636, titled *Improving Critical Infrastructure Cybersecurity*, is available at www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf (originally released by the White House on February 12, 2013); see February 19 *Federal Register*, pp. 11738–11744.

The Chamber strongly believes that critical infrastructure entities identified under the EO should be the primary voices behind the development of the cybersecurity framework. In turn, the administration has a unique opportunity to collaborate—rather than flex its regulatory authority—with the private sector as components of the EO are being developed and put into practice.[3]

Developing the framework is only one piece of the cybersecurity puzzle. 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.

Further, executive action, like legislation, must focus not only on strengthening U.S. critical infrastructure but on encouraging innovative cybersecurity practices. Policymakers need to help the law enforcement community increasingly shift the cost of cyber intrusions to nefarious actors, which the business community and government both confront daily.

(1) The business community needs to lead the development of the framework, because a substantial amount of technical and standards-setting expertise resides in the private sector.

The Chamber agrees with comments made by Patrick Gallagher, Under Secretary of Commerce for Standards and Technology at the Department of Commerce, who testified in March before Congress that a NIST-coordinated and industry-led framework would "draw on standards and best practices that industry is already involved in developing and adopting," and would "ensure a robust technical underpinning to the framework." He emphasized that a multistakeholder approach would take advantage of the strengths of the public and private sectors to develop solutions that both sides would find beneficial to security. Under Secretary Gallagher said that the "approach does not dictate solutions to industry, but rather facilitates industry coming together to offer and develop solutions that the private sector is best positioned to embrace."[4]

Industry activities include developing guides and road maps, standards, and innovative technologies to improve security, operational safety, and reliability. Indeed, the Government Accountability Office (GAO) has found that a wide variety of cybersecurity guidance is

[3] The Chamber has been a skeptic of legislation and policies that would almost certainly shift public-private partnerships toward regulation and away from collaboration. Mandates, in our view, are too static to keep pace with dynamic cyber threats.

[4] Under Secretary Gallagher's prepared testimony before a joint hearing of the Senate Homeland Security and Commerce committees is available at http://www.hsgac.senate.gov/hearings/the-cybersecurity-partnership-between-the-private-sector-and-our-government-protecting-our-national-and-economic-security (March 7, 2013).

available to critical infrastructure owners and operators.[5] GAO interviewed representatives of seven sectors—banking and financial services, communications, energy (electric, oil and natural gas), health care, information technology, nuclear, and water. The sectors provided a sampling of nearly 400 cybersecurity guidance documents applicable to their industries, and it is far from comprehensive.[6]

Most industry experts in cybersecurity argue that there is no "short list" of cyber standards. The ecosystem of cybersecurity guidance encompasses a variety of components, composing perhaps thousands of individual standards related to technologies, practices, and products that perform functions such as enabling interoperability and ensuring security policies and controls. Further, the guidance ecosystem is constantly evolving in response to cyber threats and risks, new technologies, and business models.[7]

The Chamber believes that NIST should play a constructive role in helping critical infrastructure entities identify the guidance that is "most effective and applicable in improving their security posture." In short, the process is set up so that industry and government "don't reinvent the wheel," which senior NIST leadership recognizes.[8]

---

[5] GAO report titled *Critical Infrastructure Protection: Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use* can be found at www.gao.gov/products/GAO-12-92 (December 2011, GAO-12-92). According to GAO, cybersecurity guidance, as used in the report, includes voluntary, consensus-based standards and mandatory or required standards, implementation guides and manuals, and best practices (p. 1). See, too, NIST notice, pp. 13025–13026.

In addition, it is worth noting that 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 that outlines how and when companies should report hacking incidents and cybersecurity risk. Also, corporations comply with many non-U.S. requirements, which only add to the multitude of regulations.

[6] See tables in appendix II of the GAO report, pp. 53–67. The breakdown of the cybersecurity guidance documents includes banking and financial services (136), communications (76), energy (72), health care (20), IT (40), nuclear (18), and water (18).

[7] GAO *Critical Infrastructure Protection* report, pp. 20–21.

[8] "[T]he framework is going to have a road map character to it where . . . we can use that to address those areas of overlap and see whether that's a problem or not. … So I think the process is specifically designed to make sure *we don't reinvent the wheel* [italics added]." Under Secretary Gallagher's remarks during Q&A at the March 7 combined hearing of the Senate Homeland Security and Commerce committees are available at http://homeland.cq.com/hs/display.do?docid=4233613 (March 7, 2013, *Congressional Quarterly* transcripts).

(2) The cybersecurity framework needs to be built upon existing voluntary consensus-based standards.

Under the EO, NIST shall be directed to coordinate the development of a cybersecurity framework that would focus on reducing cyber risks to critical infrastructure. The Chamber urges the administration to take the following actions:

- The U.S. government, through entities such as NIST, should take the lead in promoting the adoption of international cybersecurity standards and best practices developed by industry-led and public-private standards development bodies.

- The federal government should collaborate with the private sector to improve, expand, and implement the Common Criteria for Information Technology Security Evaluation, generally known as Common Criteria, which is the primary international standard (International Organization for Standardization, or ISO, 15408) for computer product assurance security certification. This international standard is recognized under a multilateral agreement (Common Criteria Recognition Arrangement) by more than 20 countries. Common Criteria is preferred by many in industry, rather than a collection of country-specific standards, rules, and required actions that could unintentionally balkanize cyberspace and security.

- NIST should continue to build its capacity to engage in international standards-setting efforts that are industry led. NIST may find it useful to leverage its resources by participating first at the national level. Then, through this participation, it would become a much more effective advocate of the voluntary, industry-driven position at the international level.[9]

(3) The cybersecurity framework needs to be risk based and performance based.

The EO states that the baseline cybersecurity framework should be risk based and performance based, which is fitting. Risk management is a foundational principle of homeland security.[10] The Chamber anticipates that the administration would incorporate performance standards, which have a well-established history in federal regulatory efforts, in the cybersecurity framework. Performance standards specify the outcome required but *leave the specific measures or techniques to achieve that outcome up to the discretion of the regulated entity* in partnership with federal entities.

The Chamber would strongly oppose attempts by government officials to mandate *preferred cybersecurity solutions*—whether a practice, a process, or an IT product or service—without the consent of affected owners and operators. Top-down approaches to instituting

[9] For more on the Chamber's views on the U.S. standards-setting process and cybersecurity, see our March 7, 2011, letter to NIST in response to the agency's 2010 notice titled "Effectiveness of Federal Agency Participation in Standardization in Select Technology Sectors for National Science and Technology Council's Subcommittee on Standardization."

[10] GAO report titled *Strengthening the Use of Risk Management Principles in Homeland Security* is available at www.gao.gov/products/GAO-08-627SP (April 15, 2008, GAO-08-627SP).

information security measures and controls should not have a place in a genuinely collaborative program.

(4) A cybersecurity capability maturity model should serve as part of the framework to manage risks to critical infrastructure.

Based on the text of the EO (section 8) and conversations with National Security Staff (NSS), the Chamber anticipates that the administration plans to use a cybersecurity capability maturity model as the overarching structure to reduce risks to critical infrastructure and to implement the "voluntary" cybersecurity program. NSS members have suggested that the Electricity Subsector Cybersecurity Capability Maturity Model, featuring some of the following objectives, could be applied to other sectors:

- 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.[11]

At present, using a maturity model seems like a constructive plan. However, the Chamber understands that a maturity model is not intended to be the only way to develop the framework. Indeed, each sector should be able to develop a prioritized and flexible approach to cybersecurity that meets the requirements of its members. Further, the Chamber believes that the cybersecurity framework should closely align with, not interfere with, the enterprise risk-management strategies of critical infrastructure. The cybersecurity framework, in our view, should not alter public-private partnerships, such as the North American Electric Reliability Corporation (NERC) cybersecurity standards program and similarly situated arrangements, without the mutual consent of both parties.

(5) The cybersecurity framework should not mandate third-party audits. Auditing procedures should be mutually agreed upon by critical infrastructure professionals and government officials.

The EO calls for "measuring the performance of an entity" in implementing the framework. It is unclear if metrics would entail auditing critical infrastructure, such as third-party audits. The Chamber is concerned about proposals that call on identified critical infrastructure to be evaluated by a third-party auditor. Complying with third-party assessments would be costly and time consuming, particularly for small and midsize businesses.

Many businesses already have processes in place for assessing and improving the strength of their networks and systems, so added mandates are unnecessary, if not misguided.

[11] See, for example, http://energy.gov/oe/articles/doe-releases-electricity-subsector-cybersecurity-risk-management-process-rmp-guideline, and http://energy.gov/oe/services/cybersecurity/electricity-subsector-cybersecurity-capability-maturity-model.

Owners and operators in the business community are concerned that the release of proprietary information to the government and third parties could create new security risks. Third-party audits should be optional, not mandatory.

(6) "Cost-effectiveness" needs to be a consistent theme throughout the development of the cybersecurity framework and program.

The language "cost-effective approach" is used only once in the EO. Cost-effectiveness should be a consistent theme throughout the cybersecurity framework and program. The issue of cost may not be an inhibiting factor for some critical infrastructure entities. However, the cost of complying with a "voluntary" cybersecurity framework and program could be a significant issue for some critical infrastructures. It should not be overlooked.

A cybersecurity framework and program should be able to measure a covered critical infrastructure's relative gain in security compared with its outlay of resources (e.g., capital, human talent). In other words, owners and operators need to get sufficient bang for the buck. Executive action must not focus solely on hardening U.S. critical infrastructure but on encouraging innovative cybersecurity practices. Policymakers need to shift the cost of cyber intrusions to bad actors, which the private sector and government both confront.

(7) The framework needs to be developed in a manner that provides critical infrastructure a return on investment.

Any cybersecurity program must afford businesses maximum input and flexibility with respect to implementing best cybersecurity practices. The Chamber is very concerned about a well-intended government program that would become slow, bureaucratic, and costly relative to businesses' need for a qualitative and quantitative return on investment (ROI).

Companies have spent millions to protect their IT assets and to enhance enterprise resilience. Any government cybersecurity program that puts claims on private sector resources must not weaken companies' efforts to keep pace with sophisticated threats. Moreover, a cybersecurity program must not divert companies' resources toward satisfying compliance mandates, instead of improving security. Cybersecurity program outcomes that fuel concerns about a lack of ROI would be viewed by the Chamber as unacceptable.

(8) The EO needs to include privacy and civil liberties safeguards.

Department of Homeland Security (DHS) privacy and civil rights officers shall assess annually the EO and recommend ways to minimize impacts on personal privacy. The program shall be evaluated against Fair Information Practice Principles and other privacy policies. The Chamber is committed to working with the administration and lawmakers to ensure that information sharing includes privacy and civil liberties safeguards. While personal privacy must be adequately guarded, improved information sharing should aim to enhance situational awareness to detect, prevent, mitigate, and respond to emerging and rapidly changing threats.

Importantly, enhancing the situational awareness of critical infrastructure owners and operators *would actually increase the security of personal information* that is maintained on company networks and systems. Improved information sharing would benefit individuals' privacy protections, *not detract* from them.

(9) The framework should be informed by a strategic assessment and prioritization of threats to U.S. cybersecurity, while maintaining robust flexibility.

The EO focuses on hardening U.S. critical infrastructure and encouraging innovative cybersecurity practices, which are essential steps for business and government to take together. However, the EO does not discuss the online threats to our national and economic security, and it does not prioritize or rank threats based on a strategic assessment. Government officials have almost certainly done these assessments, albeit discreetly.

The Chamber believes that the EO's framework should be informed by an assessment and prioritization of dangers posed to America's cybersecurity, including rogue individuals, organized criminal gangs, and groups carrying out state-sponsored economic espionage.[12] It is most important, though, that the framework remains *flexible*, so that it can accommodate the demands of many companies and sectors. The framework needs to evolve over time to help critical infrastructure owners and operators counter a diversity of cyber threats and risks to their enterprises.

(10) The cybersecurity framework would, and should, be open to public review and comment. However, the administration needs to explain how it plans to balance two competing and necessary goals—transparency and security.

The cybersecurity framework is expected to be open to public review and comment. Transparency is important—but wouldn't the administration be giving bad actors an advance look at the high-level contents of the cybersecurity framework? We urge the administration to communicate to stakeholders how it plans to balance two competing and necessary goals—openness and security. The Chamber's impression is that the administration plans to write the framework in a manner that is tantamount to saying, "You need a lock on your door, etc. But we won't disclose your security codes."

The Chamber appreciates the opportunity to offer several principles that our members believe should guide the establishment of the cybersecurity framework and its implementation. The administration deserves credit for previewing the cybersecurity EO with some in the business community prior to its release. The Chamber believes that NIST can, and should, play a principal role in helping critical infrastructure entities identify cybersecurity guidance, standards, and smart practices that are effective in improving their security and resilience.

[12] The *Administration's Strategy on Mitigating the Theft of U.S. Trade Secrets* is a welcome step in fighting against economic espionage and trade secret theft against the U.S. business community; see www.whitehouse.gov/blog/2013/02/19/launch-administration-s-strategy-mitigate-theft-us-trade-secrets (February 20, 2013).

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

cc: Patrick Gallagher, Under Secretary of Commerce for Standards and Technology, the Department of Commerce
Michael Daniel, Special Assistant to the President and Cybersecurity Coordinator, the White House