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 29, 2013

(Via cyberincentives@ntia.doc.gov)

Alfred Lee
Office of Policy Analysis and Development
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW, Room 4725
Washington, D.C. 20230

Dear Mr. Lee:

The U.S. Chamber of Commerce, the world's largest business federation representing the interests of more than three million businesses and organizations of every size, sector, and region, 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 U.S. Department of Commerce's notice *Incentives to Adopt Improved Cybersecurity Practices*.[1] It is constructive that the administration's executive order (EO) *Improving Critical Infrastructure Cybersecurity* calls for evaluating a program of incentives (section 8) to encourage critical infrastructure owners and operators to adopt the cybersecurity framework (section 7).[2] The Chamber urges the administration to continue its outreach to the private sector through the various presidential order working groups and other means.

Collaboration, Flexibility, and Cost Reduction Are the Main Qualities of an Attractive 'Voluntary' Cybersecurity Regime

The Chamber appreciates that the department is developing incentives that induce practical, "voluntary" participation by critical infrastructure entities in a cybersecurity program. However, the most important incentive that the administration and lawmakers could extend to companies is the *assurance* that the cybersecurity framework would remain collaborative, flexible, and innovative over the long term. The Chamber believes that the presence of these qualities, or the lack thereof, would be a key determinant to participation by U.S. critical infrastructure in a federal cybersecurity regime.

---

[1] *Federal Register*, pages 18954–18955 (March 28, 2013), available at https://federalregister.gov/a/2013-07234 or www.gpo.gov/fdsys/pkg/FR-2013-03-28/pdf/2013-07234.pdf.

[2] EO 13636, titled *Improving Critical Infrastructure Cybersecurity*, is available at www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

Businesses genuinely want government partners in the fight against organized criminals, hacktivists, and groups carrying out state-sponsored attacks.[3] It is clear to the Chamber that critical infrastructure entities are interested in engaging the National Institute of Standards and Technology (NIST) in developing and implementing the cybersecurity framework if they are allowed to manage risks smartly and effectively in a context that is nonbinding. Companies are less interested in getting a suite of incentives; instead, they are more interested in avoiding a program that is likely, later on, to become top heavy and rigid because of new rules or mandates.[4]

Indeed, any cybersecurity regime that industry believes would favor compliance and bureaucracy over creativity, speed, and innovation would almost certainly create a powerful *disincentive* to participation by critical infrastructure owners and operators. The Chamber believes that critical infrastructure entities need minimal structure (i.e., the cybersecurity framework) and maximum autonomy to counter—in partnership with government—rapidly changing cyber threats.[5] Incenting businesses to adopt a framework that ultimately becomes rigid and prescriptive (e.g., practices, technology) would distort the marketplace by driving private-sector investment toward compliance with lowest common-denominator solutions, thus making the United States less secure.

In addition, private firms must earn a qualitative and quantitative return on their investments. The cybersecurity program must focus on reducing businesses' costs (e.g., compliance, lawsuits) and fostering information sharing between government and the private sector. 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.

---

[3] The emerging cybersecurity framework 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.

[4] On April 8, the Chamber sent a letter to NIST arguing that the business community must lead the development of the cybersecurity framework, because a substantial amount of technical and standards-setting expertise resides in the private sector. The letter is available at http://csrc.nist.gov/cyberframework/rfi_comments.html; see http://csrc.nist.gov/cyberframework/rfi_comments/040813_us_chamber_of_commerce.pdf.

[5] In his book, *Yes to the Mess: Surprising Leadership Lessons from Jazz* (Boston, MA: Harvard Business Review Press, 2012), Frank J. Barrett, professor of management and global public policy at the Naval Postgraduate School, writes about the requisites for leadership, innovation, and learning in high-performing organizations. He argues (e.g., chapter four, "Minimal Structure–Maximal Autonomy") that dynamic organizations thrive on minimal constraints, learn from errors (without punishment), and collaborate through the evolution of ties between participants. In the Chamber's view, this is exactly what healthy cybersecurity partnerships do best.

Protected Information-Sharing is the No. 1 Tool to Combat Cyber Threats; Legislation Should Reduce Business Costs Related to Voluntary Sharing

At a time when the administration is rallying business support for developing and adopting the cybersecurity framework, the Chamber believes that its endorsement of industry-supported information-sharing legislation is tantamount to putting wind behind the sails of the presidential order.

The Chamber strongly supports legislation that would remove legal hurdles that currently prevent the private sector and government from rapidly sharing cyber threat information. An information-sharing bill needs to provide legal certainty to businesses that threat and vulnerability information voluntarily shared with each other and with the government would be provided safe harbor against the risk of costly litigation, would be exempt from public disclosure, and would not be used by officials to regulate other activities. Legislation also needs to include an exemption from antitrust laws, which limit exchanges of data and metadata between private entities, in order to prevent, investigate, and mitigate threats to cybersecurity.

Making Incentives Work

It is positive that the EO calls on policymakers to work with industry to assess the pros and cons of a mix of incentives. The Chamber is particularly interested in judging whether the incentives are weak or robust and if they would entail codifying the EO before it is shown to be smart and effective policy. Ultimately, the administration should meet with each identified critical infrastructure sector and discuss opportunities and issues of concern and what businesses need to adhere to the cybersecurity framework. The right incentives may be available or they may need to be created.

Here are some incentives that are frequently discussed by public and private sector stakeholders, which the Chamber is willing to consider:

- **Extending liability protections (information sharing).** Businesses seek to participate in the online equivalent of the "If You See Something, Say Something" campaign. Companies' security professionals want to exchange cyber threat information and vulnerabilities with their peers and government—but they fear being penalized for doing the right thing. Most importantly, the Chamber strongly urges Congress to pass an information-sharing bill with strong protections related to lawsuits, public disclosure, regulations, and antitrust concerns.

- **Extending liability protections (framework).** Congress is expected to consider extending liability protections to companies that "voluntarily" adopt the cybersecurity framework. This is a welcome option. However, our experience with S. 3414, the Cybersecurity Act of 2012, demonstrates that the level of protection authorized in the bill (i.e., against punitive damages sought in a lawsuit) was relatively weak. The bill provided insufficient protection to sway businesses' decision making in favor of the legislation.

- **Extending liability protections (SAFETY Act).** The administration and Congress are expected to assess how the Support Anti-terrorism by Fostering Effective Technologies Act of 2002 (SAFETY Act) could allow for legal liability protections for providers of qualified cybersecurity technologies to expand the development and commercialization of innovative products and services to mitigate significant cybersecurity incidents. This may require a review and possibly a modification of the events that would trigger SAFETY Act coverage and the types of technologies and services that would be covered. The Chamber's impression is that any legislative or policy changes to the SAFETY Act would not equate to codification of the EO.

- **Eliminating cybersecurity regulations.** Information-security requirements should not be cumulative. The Chamber believes it is positive that agencies and departments are urged, under the EO, to "report to OMB on any critical infrastructure subject to ineffective, conflicting, or excessively burdensome cybersecurity requirements." We urge the administration and Congress to prioritize eliminating burdensome regulations on businesses. One solution could entail giving owners and operators credit for information security regimes that exist in their respective sectors that they have adopted.[6]

  Likewise, the Chamber urges the OMB to rein in the inclination of agencies and departments other than NIST and the sector-specific agencies to become involved in the development and execution of the framework. In our view, 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.

- **Leveraging federal procurement.** The Chamber generally supports a government procurement process that rewards vendors that follow industry-recognized cybersecurity guidance.[7] However, we are concerned about unintended consequences of procurement incentives, such as a program that leads to one-size-fits-all outcomes or to artificially chosen technology winners and losers. The Chamber urges the administration to be mindful of how procurement incentives, however beneficial in the American context, could prompt foreign governments to emulate this policy, disingenuously, as a way of restricting U.S. companies' access to overseas markets.

---

[6] 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.

[7] See Government Accountability Office (GAO) report titled *Critical Infrastructure Protection: Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use* 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 standards, implementation guides and manuals, and best practices (p. 1).

The Chamber cautions against expanding the scope of the EO. The administration recognizes that it should not determine how companies design, develop, and manufacture their technology and products. There are well-established laws and policies on the books to ensure that government procurement processes leverage—rather than duplicate and weaken—industry-led, international technology standards and best practices.

- **Making the research and development (R&D) tax credit permanent.** Congress should make the R&D tax credit permanent to help businesses in adopting a multilayered cybersecurity program that matures over time in relation to risks. This is particularly important for small and midsize company owners and operators who typically lack the money and human talent to deploy a sophisticated program.

***

Robust cybersecurity is good for the business community and the United States. The Chamber appreciates the opportunity to comment on the department's notice, which seeks public input on an array of incentives that could help critical infrastructure adopt the cybersecurity framework through creating opportunities and reducing costs.

If you have any questions or need further information, please contact me (abeauchsene@uschamber.com; 202-463-3100) or my colleague Matthew Eggers (meggers@uschamber.com; 202-463-5619).

Sincerely,

Ann M. Beauchesne

cc: Michael Daniel, Special Assistant to the President and Cybersecurity Coordinator, the White House