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

May 27, 2015

Via securityRFC2015@ntia.doc.gov

Allan Friedman, Ph.D.
Director of Cybersecurity Initiatives
National Telecommunications and Information Administration
Department of Commerce
1401 Constitution Avenue NW, Room 4725
Washington, D.C. 20230

Subject: Stakeholder Engagement on Cybersecurity in the Digital Ecosystem [Docket No. 150312253-5253-01]

Dear Dr. Friedman:

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 Department of Commerce Internet Policy Task Force's (IPTF's) notice requesting public feedback on *Stakeholder Engagement on Cybersecurity in the Digital Ecosystem*.[1]

The Chamber does not attempt to answer each question in the notice. We focus on future areas of work related to the cybersecurity framework, botnet and malware mitigation, and the domain name system. Individual organizations are better equipped to provide detailed responses to questions under the notice's three main areas—network and infrastructure security, Web security and consumer trust, and business processes and enabling markets.

Roadmap for the Future of the Cybersecurity Framework

In February 2014, the National Institute of Standards and Technology (NIST) released a *Roadmap* to accompany the cybersecurity framework. The *Roadmap* outlines further areas for

[1] www.ntia.doc.gov/federal-register-notice/2015/notice-comment-deadline-extension-stakeholder-engagement-cybersecurity-; www.gpo.gov/fdsys/pkg/FR-2015-03-19/pdf/2015-06344.pdf

possible "development, alignment, and collaboration."[2] Here are some key areas that the Chamber sees as needing attention by the IPTF and additional stakeholders:

- **Aligning international cybersecurity regimes with the framework.** Many Chamber members operate globally. We appreciate that NIST has been actively meeting with foreign governments to urge them to embrace the framework. Like NIST, the Chamber believes that efforts to improve the cybersecurity of the public and private sectors should reflect the borderless and interconnected nature of our digital environment.

  Standards, guidance, and best practices relevant to cybersecurity are typically industry driven and adopted on a voluntary basis; they are most effective when developed and recognized globally. Such an approach would avoid burdening multinational enterprises with the requirements of multiple and often conflicting jurisdictions.[3]

  The administration 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 occur on a routine basis.

- **Avoiding disruptions to the framework's privacy methodology.** The Chamber appreciates that NIST struck Appendix B of the preliminary framework and 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. A privacy methodology that would attempt to apply privacy principles to most features of the framework or recommend burdensome practices would create significant disincentives to businesses' implementing the framework.

  The Chamber welcomes the outreach that NIST officials have had with us regarding its new privacy engineering initiative and wants 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.

  NIST is well suited to contribute technical expertise to a standards-setting effort that first requires a multistakeholder process to articulate consensus policy goals. However, the Chamber is concerned that the privacy engineering initiative, as presently conceived,

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

[3] The Chamber sent a letter in September 2013 to Dr. Andreas Schwab, member of the European Parliament's Internal Market and Consumer Protection Committee, recommending amendments to the proposed European Union (EU) cybersecurity directive. We argue that cybersecurity and resilience are best achieved when organizations follow voluntary global standards and industry-driven practices.

would endorse potential policy objectives prematurely, rather than integrate consensus-based and broadly adopted policies into a technical standard.

We strongly caution NIST against pursing a privacy engineering initiative that would (perhaps unintentionally) undermine the progress that industry and NIST have made in creating and launching the framework.

- **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 roundtable series, our member organizations have urged businesses to use the framework when communicating with partners, vendors, and suppliers. Businesses of all sizes can find it challenging to identify their risks and prioritize their actions to reduce weak links vulnerable to penetration and disruption. NIST should provide additional guidance in this area.

  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 DHS, among others. In June 2013, the Chamber submitted comments to GSA and the Joint Working Group on Improving Cybersecurity and Resilience Through Acquisition regarding section 8(e) of the cyber EO.[4]

  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.

[4] See May 13, 2013, *Federal Register*, pp. 27966–27967, at www.gpo.gov/fdsys/pkg/FR-2013-05-13/pdf/2013-11239.pdf. Section 8(e) of the 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."

- 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.

Botnet and Malware Mitigation

One of those most tenacious threats to the global economy stems from the proliferation of botnets and malicious software (malware), which enables a single bad actor to control large networks of infected computers. Botnets, which are generally connected with criminal syndicates and the pilfering of personal information, can also be used for attacks by both state and nonstate actors against public and private networks.

Several public-private initiatives have tackled mitigating the proliferation of botnets and malware. Chamber members, including representatives of the communications and IT sectors, have been major contributors in blunting the impacts of botnets and malware.

- **Public-private efforts under way to control the spread of bot infections; further coordination worthwhile.** In March 2012, under the auspices of the Communications Security, Reliability, and Interoperability Council (CSRIC) III, an industry working group delivered the voluntary U.S. Anti-Bot Code of Conduct for Internet Service Providers (ISPs) (the Anti-Bot code) to address threats posed to residential broadband networks.

  Under the Anti-Bot code, ISPs agree to educate consumers about the botnet threat, take steps to detect botnet activity on their networks, make consumers aware of botnet infections on their computers, offer assistance to consumers whose computers are infected, and collaborate with other service providers that have also adopted the code. The council concluded that "constituents of the entire Internet ecosystem have important roles to play in addressing the botnet threat and that ISPs depend on support from the other parts in the ecosystem."[5]

  The Industry Botnet Group (IBG) is another example of communications providers playing a role in addressing botnet-related challenges. The IBG brought together stakeholders to address specific goals, including the development of principles to guide voluntary anti-botnet efforts throughout the digital ecosystem. In May 2012, the IBG presented at the White House its nine principles governing future engagement across the ecosystem.[6]

[5] https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-ReportFinal.pdf, and https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG7_Report_March_%202013.pdf

[6] http://www.industryweek.com/information-technology/nine-principles-boost-cybersecurity?page=2

A principal finding of the group was that addressing "botted" machines is a shared responsibility of many digital ecosystem stakeholders. These examples—the Anti-Bot code and the IBG—highlight efforts to constructively address botnet and malware mitigation issues.[7] The Commerce Department's IPTF could build on the momentum of this work to reduce the spread of botnets through further coordination of cybersecurity stakeholders.

Domain Name System

- **IPTF, industry engagement with Domain-based Message Authentication, Reporting and Conformance (DMARC):** The Chamber recommends that the IPTF raise awareness and encourage adoption of Domain-based Message Authentication, Reporting and Conformance (DMARC). DMARC is a method of email authentication that helps thwart malicious cyber actors' misuse of email to gain access to private networks.

  Individual organizations are responsible for configuring DMARC for their own information systems. Still, a greater benefit for the digital ecosystem is realized when DMARC is embraced by a large number of organizations. For this reason, DMARC is an ideal topic for the IPTF in that it is a multistakeholder process in need of increased coordination. Key goals are increasing confidence and trust in email sources while reducing successful phishing campaigns, which are a highly effective channel for propagating malicious code globally.[8]

***

The Chamber welcomes having the chance to provide feedback on the IPTF's notice requesting comment on cybersecurity issues that impact the digital ecosystem and economic growth.

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

Sincerely,

Ann Beauchesne

Ann M. Beauchesne

[7] www.m3aawg.org/dm3z/2014/10/20/new-m3aawg-bot-metrics-report-shares-network-operators%E2%80%99-perspective, and www.m3aawg.org/media_center/maawg-tackles-bots-with-new-isp-guidelines-for-restoring-infected-end-users-machines

[8] http://dmarc.org