USCIB UNITED STATES COUNCIL FOR INTERNATIONAL BUSINESS

May 8, 2015

Mr. Allan Friedman
National Telecommunications & Information Administration
U.S. Department of Commerce
Washington, DC 20230

VIA ELECTRONIC TRANSMISSION

Re: Request for Comments – Stakeholder Engagement on Cybersecurity in the Digital Ecosystem (Federal Register Docket No. 1503122523-5253-01)

Dear Mr. Friedman:

The U.S. Council for International Business (USCIB) is pleased to respond to the Department of Commerce Internet Policy Task Force's (IPTF) March 19, 2015 request for comments to identify substantive cybersecurity issues that affect the digital ecosystem and digital economic growth where broad consensus, coordinated action, and the development of best practices could substantially improve security for organizations and consumers. USCIB is a trade association composed of more than 300 multinational companies, law firms, and business associations from every sector of the US economy, with operations in every region of the world. In particular, USCIB Members include a broad cross-section of the leading global companies in the information and communications technology (ICT) sectors. Thus, we welcome this opportunity to offer a multi-sectoral perspective on cybersecurity issues that affect the digital ecosystem.

General Comments

Importance of the Digital Economy and Commerce Leadership -- USCIB applauds the Commerce Department's initiative in launching this very important undertaking, the outcome of which will affect companies across the entire US economy. The digital economy essentially *is* the economy. Virtually all companies – digital content providers, software manufactures, ISPs, and digital platform providers as well as retailers, financial services and insurance providers, manufacturers, and delivery service providers, to name just a few – operate in the digital ecosystem and must contend with the evolving set of security challenges. The same holds for consumers and organizations who utilize online services to conduct business, purchase products, and engage with various communities. Thus, while the focus of this particular initiative is security-related, the broader issue at stake is the continued dynamism and innovative potential of the U.S. economy, which is solidly within the remit of the Commerce Department and requires its continued leadership.

Multistakeholder Model – In view of the breadth of stakeholders who rely on a stable, secure, and resilient digital environment, the Commerce Department is to be commended for conducting this new initiative in an open, transparent, and inclusive manner, enabling the participation of stakeholders from business, government, civil society, the technical community and academia. The successful development of the National Institute of Standards and Technology (NIST) "Framework for Improving Critical Infrastructure Cybersecurity" through a multistakeholder process serves as a testament to the effectiveness of this model in marshalling the breadth of expertise required to address the complexity of issues in an ever-changing digital ecosystem. This NIST process demonstrated that government cannot tackle cybersecurity challenges in a vacuum – be they focused on critical infrastructure or the broader economy. Government needs commercial and economic expertise of business, technical advice of the technical community, and social welfare and human rights-related acumen of civil society, consumer voices, and academia to produce a sound policy framework that addresses the intricacies and fluidity of safety and security in the digital environment.

Moreover, the Commerce Department's decision to (1) solicit multistakeholder inputs to shape this new initiative and (2) include all stakeholder groups in the subsequent discussions sends a strong signal to the global community that the United States will back up its words of support for the multistakeholder model with action. This comes at a critical juncture in the global community's assessment of whether multistakeholder forums have proved effective in extending the economic and societal benefits of a vibrant digital economy to larger segments of the world population as well as addressing cybersecurity, privacy, and a host of other Internet-related issues.

Globally Accepted Standards – The IPTF Request for Comments envisions a process that will result in development of best practices aimed at improving security for organizations and consumers. USCIB urges that any best practices resulting from this initiative should be based on *globally accepted standards* developed by organizations such as the International Standards Organization (ISO), the Internet Engineering Task Force (IETF), the Institute for Electrical and Electronics Engineers (IEEE), or other internationally recognized standards-setting organizations. This is important because these organizations have tested the standards to ensure their effectiveness. In addition, the global recognition and acceptance of the standards developed by these organizations better ensures interoperability of technology solutions.

Security is Context-Based – USCIB recommends that an overarching theme guiding the multistakeholder process should be that effective security is based on context; the totality of circumstances must be considered in developing cybersecurity best practices and frameworks.

Privacy -- USCIB appreciates the importance of considering the implications of cybersecurity activities on privacy and civil liberties. NTIA has existing efforts to address privacy-related issues such as through previous RFI processes. To the extent that privacy-related matters are pertinent to this effort, we recommend that NTIA consider the model employed by NIST during the development of the Cybersecurity Framework, where the approach was based on high-level processes proposed by industry to address privacy aspects of the practices in the Framework. The OECD's 2002 Security Guidelines and current efforts to revise those guidelines also present a high-level approach and may be relevant.

Commercial and Trade Implications -- USCIB notes the increasing trend of countries citing cybersecurity as a justification for new barriers to trade and investment, especially with respect to online products and services. We encourage NTIA to coordinate closely with other agencies focused on commercial and trade issues to ensure that the consistency of such measures with countries' international commitments is examined and considered, and that their economic effects are well understood.

Cybersecurity and the Internet of Things -- Addressing security issues in the Internet of Things (IoT) is an ever-more pressing issue as more devices are deployed and come online. Failures in security design or implementation can result in increased security risk, preventing IoT from achieving their potential in the growing digital economy. Security concerns need to be addressed in technology, policies and practices. While the IoT ecosystems are still developing, multistakeholder fora can play important roles in promoting enhanced security across all relevant stakeholders from policy-makers, to developers, to commercial entities, to users, each according to their role.

Addressing SME Audiences – Security-related best practices and frameworks should be drafted in a manner more readily understandable to SMEs, which often lack the resources to hire in-house security professionals. Whatever topics the Commerce-hosted multistakeholder process ultimately focuses on, efforts should be made to distill security best practices in a manner that is more user-friendly for non-security-focused business and government professionals. This could take the form of a specially tailored SME document or manual.

In addition, USCIB urges greater involvement of other “non-security” Federal agencies, such as the Small Business Administration (SBA), in promoting good cybersecurity practices in smaller enterprises. Specifically, Commerce and the SBA should highlight existing small business incentive programs that will be discussed through the multistakeholder process and may be linked to the adoption of basic APIs or protocols for securing SME websites, apps, and services. In addition, the SBA might include certain minimum cybersecurity requirements as a condition for the granting of loans.

NTIA-Led Cybersecurity Improvements – As a complement to the Commerce-led multistakeholder process, USCIB urges the National Telecommunications and Information Administration (NTIA) to play a leading role in the following areas:

- Work with 18F to switch all federal employees to computers connecting to the web through DNSSEC-compliant DNS servers; and
- Facilitate Commerce Department/18F engagement on fostering overseas gov programs that parallel the U.S. government’s deployment of HTTPS across all .gov websites.

Pre-Existing Organizations and Work Already Existing on Cybersecurity

It is important that the Commerce-hosted multistakeholder process not duplicate any of the considerable security-related work already underway in various standards-setting bodies and other global forums. Efforts should be made to consider how the multistakeholder process can effectively build upon such work—not replicate it. Toward this end, we identify the following organizations whose work should be considered in determining the scope of any work under the new process:

- Internet Engineering Task Force
- Worldwide Web Consortium
- IEEE
- ISO/IEC

- Wi-Fi Alliance
- Bluetooth SIG
- Consumer Electronics Association
- Telecommunications Industry Association
- 3GPP
- FCC Communications, Security, Reliability, and Interoperability Coucl
- INCITS/ANSI
- Linux Foundation
- Open Web Application Security Project
- PCI Security Standards Council
- RASA Security for Business Innovation Council
- IT Sector Coordinating Council
- IT-ISAC

Specific Issues Potentially Benefitting from Multistakeholder Consideration

Topics Already Subject to Extensive USG Work

1. Domain Name System (DNS), Border Gateway Protocol (BGP), and Transport Layer Security (TLS) Certificates
2. Trusted Downloads
3. Vulnerability Disclosure

USCIB notes that the U.S. Government (USG) already has done extensive work developing best practices and technical standards for the above three topics. We therefore would encourage the relevant Federal agencies involved in this work – NIST, the Department of Homeland Security (DHS), the National Science Foundation (NSF) – to share lessons learned about these topics with non-governmental stakeholders and guide discussions about next steps, particularly in terms of industry and government cooperation.

Botnet/Malware Mitigation -- Public attention often focuses on national security-related cyber attacks, but individual consumers continue to be subject to a range of cybersecurity issues that they are not able to effectively protect against entirely on their own. Full cooperation and active effort on all parts of the ecosystem are necessary to truly tackle the issue. Malware, botnets and viruses delivered to their devices through a range of vectors undermine trust in the ecosystem, impose costs on consumers, and damage efforts to expand digital commerce. The business community has made significant efforts to address the issues including through industry partnerships, internal business practices, and in educating users and making user tools available. There is, however, undoubtedly more that can be done.

Mitigating concerns related to malware and botnets is an issue that truly calls for collective action, including efforts from ISPs, security software providers, hosting providers, consumers and others. A Commerce-led multistakeholder process could help identify gaps in sector participation in these efforts and focus those sectors on how they can contribute to improvement. It could also bring user-focused stakeholders and other stakeholders together to jointly identify improvement opportunities.

This work could also build upon the work done previously by the Industry Botnet Group (IBG), which was initiated by the Department of Commerce in late 2011 to take collective action to address botnets. That group produced a set of principles, and the multistakeholder process could pick up where the IBG left off. The IBG principles included “Report Lessons Learned” and “educate users.” Accordingly, it would be appropriate for Commerce to study the lessons learned in the past three years of various stakeholders’ efforts to disrupt and clean-up botnets. The study could focus on, for example, what are the most effective ways to communicate security issues to consumers, what are the incentives to keep a device secure, and what are the available end-users tool to remove malware and any measures of success.

Lagging Security Efforts in the Public Sector – The Commerce-hosted multistakeholder process should examine the extent to which the public sector has been lagging behind the private sector in implementing cybersecurity best practices and frameworks. The goal of this aspect of the process would be to develop an expedited, prioritized timetable for Federal agencies to implement improved security frameworks, which would place some agencies (e.g. DHS, Commerce, State, Justice) on a faster-track than other “non-security” Federal agencies. The prioritized approach, in turn, would serve as a model for state, local, and municipal governments.

In addition, USCIB urges the multistakeholder process to consider a leadership role for NTIA in pursuing the following improvements:

- Work with US-CERT to publish quarterly report on high-risk HTTPS certificate authorities; and
- Host joint NIST/SBA National Software Update Day.

Implementing the Multistakeholder Process

As mentioned above, USCIB believes that the multistakeholder model best ensures that a diversity of expertise can be tapped to address the unique security, privacy, and other Internet governance issues generated by the dynamic and evolving digital ecosystem. We note, however, that some security issues, particularly highly technical issues, may be appropriate for a policy-focused group facilitated by NTIA and conducted in Washington, DC, composed of stakeholders who have worked actively in shaping the work of the standards-setting groups detailed in the General Comments section and possess in-depth technical expertise.

Structure and Mechanics -- In addition, we also underscore that a multistakeholder process for a topic as complex as security in the digital ecosystem typically is a time-consuming process. To be effective, this requires active and committed participation by representatives from each stakeholder group – over a significant period, which often extends beyond the period originally anticipated. Thus, the inclusive, participatory nature of the multistakeholder process will be compromised if one stakeholder group loses interest or lacks resources to see the process through to completion. The final output of the process, in turn, could be compromised. USCIB therefore recommends that the Commerce Department (as the principal host), establish realistic, perhaps overly conservative timeframes from the onset to enable potential stakeholder participants to thoroughly evaluate whether they can commit the requisite resources and personnel to the process.

Transparency of Process – USCIB proposes that NTIA develop an IETF Non-WG Mailing List to facilitate public discussion throughout the duration of the multistakeholder process. In addition, participants in the process and their affiliations should be disclosed.

Side Events or Workshops -- USCIB does not believe that special workshops or side events should developed to raise awareness or promote independent action on certain cybersecurity issues. Such events would detract from the focus of the multistakeholder process and risk creating confusion about priority issues for discussion.

Sincerely,

Barbara P. Wanner

Barbara P. Wanner
Vice President, ICT Policy

cc: Peter Robinson, President, U.S. Council for International Business
Rob Mulligan, Senior Vice President, Policy and Government Affairs,
U.S. Council for International Business
Eric Loeb, Vice President of International External Affairs, AT&T, & Chair,
U.S. Council for International Business ICT Policy Committee