Billing Code 3510-60-P

DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration

[Docket No. 150312253-5253-01]

RIN 0660-XC018

Stakeholder Engagement on Cybersecurity in the Digital Ecosystem

AGENCY: National Telecommunications and Information Administration, U.S. Department of Commerce.

ACTION: Request for Public Comment.

SUMMARY: The Department of Commerce Internet Policy Task Force (IPTF) is requesting comment 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. The IPTF invites public comment on these issues from all stakeholders with an interest in cybersecurity, including the commercial, academic and civil society sectors, and from relevant federal, state, local, and tribal entities.

DATES: Comments are due on or before 5 p.m. Eastern Time on [insert date 60 days after publication in the *Federal Register*].

ADDRESSES: Written comments may be submitted by email to securityRFC2015@ntia.doc.gov. Comments submitted by email should be machine-searchable and should not be copy-protected. Written comments also may be submitted by mail to the National Telecommunications and Information Administration, U.S. Department of Commerce, 1401 Constitution Avenue, N.W., Room 4725, Attn: Cybersecurity RFC 2015, Washington, DC

20230. Responders should include the name of the person or organization filing the comment, as well as a page number, on each page of their submissions. All comments received are a part of the public record and will generally be posted to http://www.ntia.doc.gov/category/internet-policy-task-force without change. All personal identifying information (e.g., name, address) voluntarily submitted by the commenter may be publicly accessible. Do not submit Confidential Business Information or otherwise sensitive or protected information. NTIA will accept anonymous comments.

FOR FURTHER INFORMATION CONTACT: Allan Friedman, National Telecommunications and Information Administration, U.S. Department of Commerce, 1401 Constitution Avenue, N.W., Room 4725, Washington, DC 20230; Telephone: (202) 482–4281; Email: afriedman@ntia.doc.gov. Please direct media inquiries to NTIA's Office of Public Affairs: (202) 482–7002.

SUPPLEMENTARY INFORMATION:

Background: The Department of Commerce IPTF published a Notice of Inquiry (NOI) in 2010, focusing on the relationship between cybersecurity and the pace of innovation in the information economy.[1] Based on the comments received, the Department of Commerce published a Green Paper, *Cybersecurity, Innovation, and the Internet Economy*, in 2011.[2] The Green Paper focused on the sector of the economy that creates or uses the Internet or networking services and falls outside the classification of critical infrastructure, as defined by existing law and Administration policy. In that document, the IPTF focused on two themes. First, there are

[1] U.S. Department of Commerce, Internet Policy Task Force, Notice of Inquiry, *Cybersecurity, Innovation, and the Internet Economy*, Dkt. No. 100721305–0305–01, 75 Fed. Reg. 44216 (July 28, 2010), *available at:* http://www.ntia.doc.gov/federal-register-notices/2010/cybersecurity-innovation-and-internet-economy. Responses to the Notice of Inquiry are available at: http://www.nist.gov/itl/cybercomments.cfm.

[2] U.S. Department of Commerce, Internet Policy Task Force, *Cybersecurity, Innovation, and the Internet Economy* (June 2011) ("Green Paper"), *available at:* http://www.nist.gov/itl/upload/Cybersecurity_Green-Paper_FinalVersion.pdf.

real, evolving threats in cyberspace that not only put businesses and their online operations at risk, but threaten to undermine the trust on which much of the digital economy depends. Second, the pace of innovation in the highly dynamic digital ecosystem makes traditional regulation and compliance difficult and inefficient.

Stakeholder response to the Green Paper provided a roadmap for the IPTF to continue its cybersecurity policy work. In September 2011, the IPTF, in coordination with the Department of Homeland Security, issued a NOI on possible approaches to creating a voluntary industry code of conduct to address the detection, notification, and mitigation of botnets, which led to an industry-led working group.[3] In February 2013, the White House released Executive Order 13636 which called upon the Department of Commerce to work with industry to develop a framework for use by U.S. critical infrastructure to improve cybersecurity practices, and to undertake a study on incentives to encourage private sector adoption of cybersecurity protections.[4]

The Cybersecurity Framework was developed by the National Institute of Standards and Technology (NIST), an agency of the Department of Commerce, with the aid of broad stakeholder participation.[5] The Cybersecurity Framework offers organizations a guide for understanding and implementing appropriate cybersecurity protections, and has been applied by a range of organizations, including a number that fall "outside the orbit of critical infrastructure

---

[3] U.S. Department of Commerce and U.S. Department of Homeland Security, Notice of Inquiry, *Models To Advance Voluntary Corporate Notification to Consumers Regarding the Illicit Use of Computer Equipment by Botnets and Related Malware*, Dkt. No. 110829543–1541–01 , 76 Fed. Reg. 58466 (September 21, 2011), *available at*: http://www.ntia.doc.gov/files/ntia/publications/botnet_rfi.pdf.

[4] Exec. Order No. 14636, *Improving Critical Infrastructure Cybersecurity*, 78 Fed. Reg. 11739 (February 12, 2013), *available at* https://www.federalregister.gov/articles/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity.

[5] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity Version 1.0*, (February 12, 2014), *available at:* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

or key resources," the focus of the Green Paper effort.[6] Following launch of the Cybersecurity Framework, NIST published a Request for Information (RFI) in August 2014 asking for stakeholder feedback on Cybersecurity Framework awareness, use, and next steps.[7] In response to questions regarding next steps that could complement the Cybersecurity Framework process, stakeholders again identified the IPTF as a vehicle to facilitate further collaborative cybersecurity work, building on the models of multistakeholder participation initially discussed in the Green Paper.[8]

Accordingly, the IPTF proposes to facilitate one or more multistakeholder processes around key cybersecurity issues facing the digital ecosystem and economy. Multistakeholder processes, built on the principles of openness, transparency, and consensus, can generate collective guidance and foundations for coordinated voluntary action. Potential outcomes would vary by the issue discussed, but could include voluntary policy guidelines, procedures, or best practices. In the digital ecosystem, the rapid pace of innovation often outstrips the ability of regulators to effectively administer key policy questions. Open, voluntary, and consensus-driven processes can work to safeguard the interests of all stakeholders while still allowing the digital economy to thrive.

The focus of these processes is to address discrete security challenges in the digital ecosystem where collaborative voluntary action between diverse actors can substantially improve security for everyone. Each process will engage a wide range of participants to ensure that the

---

[6] Green Paper at ii.
[7] U.S. Department of Commerce, National Institute of Standards and Technology, Notice of Inquiry, *Experience With the Framework for Improving Critical Infrastructure Cybersecurity*, Dkt. No. 140721609-4609-01, 79 Fed. Reg. 50891 (August 26, 2014), *available at:* https://www.federalregister.gov/articles/2014/08/26/2014-20315/experience-with-the-framework-for-improving-critical-infrastructure-cybersecurity.
[8] *See, e.g.*, comments from the Information Technology Industry Council (ITI), US Telecom Association, and Microsoft on the Cybersecurity Framework RFI (August 2014), *available at:* http://csrc.nist.gov/cyberframework/rfi_comments_10_2014.html.

outcomes reflect the consensus of the relevant community, and are fair, voluntary, and stakeholder-driven.

These processes will be designed to complement, rather than duplicate existing initiatives, both inside and outside the government. They will be coordinated by the IPTF, under the leadership of the National Telecommunications and Information Administration (NTIA). Under its statutory authority, NTIA undertakes Internet policy initiatives that serve to protect, promote and reinforce an open, innovative Internet ecosystem and digital economy, and is the executive branch lead for promoting the multistakeholder approach to Internet policymaking.[9] In partnership with its IPTF partners, NTIA has addressed other key challenges in Internet policy through multistakeholder processes, including an ongoing set of initiatives around privacy and digital copyright.[10] These proposed cybersecurity processes will be coordinated with standards and technology work underway within the Department of Commerce focused on cybersecurity, including the Cybersecurity Framework, the National Cybersecurity Center of Excellence, and the National Strategy for Trusted Identities in Cyberspace.[11] Through the comprehensive scope of all these efforts, the Department of Commerce seeks to foster innovation and to better secure the ecosystem to ensure that businesses, organizations and individuals can expand their trust, investment and engagement in the digital economy, while also reinforcing the voluntary, multistakeholder approach to Internet policymaking.

---

[9] *See* 47 U.S.C. § 901(c) (describing NTIA's policy roles, including "[p]romoting the benefits of technological development in the United States for all users of telecommunications and information facilities;" "[f]ostering national safety and security, economic prosperity, and the delivery of critical social services through telecommunications;" and "[f]acilitating and contributing to the full development of competition, efficiency, and the free flow of commerce in domestic and international telecommunications.")

[10] More information about the IPTF's work on privacy and copyright initiatives, including multiple Requests for Comment, are *available at*: http://www.ntia.doc.gov/category/internet-policy-task-force.

[11] More information about the Cybersecurity Framework is available at: http://www.nist.gov/cyberframework; the National Cybersecurity Center of Excellence at: http://nccoe.nist.gov; and the National Strategy for Trusted Identities in Cyberspace at: http://www.nist.gov/nstic.

Request for Comment: IPTF plans to facilitate a series of discussions around key cybersecurity challenges that may be addressed through a better shared understanding of the nature of the problem, and where multistakeholder discussion can be a catalyst for self-coordination of cybersecurity activities. Outcomes would depend on the issues discussed, but may involve combinations of principles, practices, and the voluntary application of policies and existing standards. Initially, IPTF seeks to conduct a cybersecurity multistakeholder process focused on a definable area where consumers and organizations will achieve the greatest benefit and consensus in a reasonable timeframe. While IPTF will avoid duplicating existing work, areas where stakeholders have identified the problem or begun to seek consensus around specific practices could provide a useful starting point.

To identify potential cybersecurity topics that would benefit from a multistakeholder process, IPTF seeks comment from stakeholders on the following questions:

1. What security challenges could be best addressed by bringing together the relevant participants in an open, neutral forum to explore coordinated, voluntary action through principles, practices, and guidelines? For each issue, also provide comment on:
    i. Why this topic is a good fit for a multistakeholder process, and whether stakeholders might reasonably be expected to come to some consensus;
    ii. Why such a process would benefit the digital ecosystem as a whole;
    iii. How long a facilitated, participant-led process on this topic should take to come to consensus;
    iv. What form an actionable outcome might take; and
    v. What pre-existing organizations and work already exist on the topic.

2. Please comment on which of the following topics could result in actionable, collective progress by stakeholders in a multistakeholder setting. For each issue, also provide comment on:

   i. Why or why not this topic is a good fit for a multistakeholder process, and whether stakeholders might reasonably be expected to come to some consensus;

   ii. Why such a process would benefit the digital ecosystem as a whole;

   iii. How long a facilitated, participant-led process on this topic should take to come to consensus;

   iv. What form an actionable outcome might take; and

   v. What pre-existing organizations and work already exist on the topic.

Network and Infrastructure Security

a) **Botnet Mitigation**. Disrupting botnets requires coordinated action and transparency between ISPs, vendors, consumers, and the public sector, such as previous efforts of the voluntary public-private partnership between the U.S. Office of the Cybersecurity Coordinator and the U.S. Departments of Commerce and Homeland Security related to ISP codes of conduct. [12] What additional collective steps can be taken to support efforts to create awareness and manage the effects of botnets?

b) **Trust and Security in Core Internet Infrastructure: Naming, Routing, and Public Key Infrastructure**. Key aspects of the Internet's core infrastructure were designed and deployed without explicit security mechanisms (e.g., the Domain Name System (DNS) and Border Gateway Protocol (BGP)) and new threats have been

[12] U.S. Department of Commerce, Press Release, *White House Announces Public-Private Partnership Initiatives to Combat Botnets* (May 30, 2012), *available at:* http://www.commerce.gov/news/press-releases/2012/05/30/white-house-announces-public-private-partnership-initiatives-combat-b.

discovered in the Internet's Public-Key Infrastructure (i.e., PKIX). Technical solutions have been developed for many of these issues (e.g., DNSSEC, BGPSec and RPKI, DANE and certificate transparency) but uptake has been slow. What collective action can be taken to promote the voluntary adoption and diffusion of existing technical solutions to make the infrastructure more trustworthy?

c) **Domain Name System (DNS), Border Gateway Protocol (BGP), and Transport Layer Security (TLS) Certificates**. Key aspects of the Internet infrastructure have long been known to be vulnerable. While technical solutions exist for security vulnerabilities in routing, the domain name system and TLS certificates, uptake has been slow or is just beginning. What collective action can be taken to promote the voluntary adoption and diffusion of technical solutions, such as DNS Security (DNSSEC), to make the infrastructure more trustworthy?

d) **Open Source Assurance**. Many organizations depend on open source projects for a wide range of purposes across the digital economy. How can stakeholders better support improving the security of open source projects, and the distribution of patches?

e) **Malware Mitigation**. Disrupting and mitigating malware and malware networks can sometimes adversely impact consumers and stakeholders who may be inadvertently caught-up in the incident. How can existing models of mitigation and disruption better incorporate the needs and concerns of all relevant stakeholders?

<u>Web Security and Consumer Trust</u>

f) **Web Security**. Many consumers assume that their connections with websites are secure, and that the websites themselves are secure, when there is little guarantee that

safeguards are in place. What actions can improve web security and trust for consumers, including transport layer (Transport Layer Security, or TLS, often referred to as Secure Sockets Layer, or SSL) and web application security, potentially building on the success of existing stakeholder initiatives?[13]

g) **Malvertising**. Several popular websites have inadvertently spread malware through "malvertising," when malicious code is served from legitimate advertising networks. How can diverse stakeholders work together to limit this risk?

h) **Trusted Downloads**. Internet users often download content and applications online without clear assurance of the security of the site. Are there best practices and existing standards that providers of online applications and downloadable tools can adopt to ensure consumer protection without impacting innovation or business models?

i) **Cybersecurity and the Internet of Things**. As the Internet of Things matures and more systems integrate information technologies (IT) and operational technologies (OT), cybersecurity is enmeshed in a broader risk context that includes safety, reliability, and resilience. [14] How can we foster the emergence of voluntary policy frameworks, informed by market dynamics, that enable Internet of Things innovation while addressing the full spectrum of risks associated with cyber-physical systems?

j) **Privacy.** As noted in the Cybersecurity Framework, privacy and civil liberties implications may arise when personal information is used, collected, processed,

---

[13] *See, e.g.*, Open Web Application Security Project (OWASP), *Top 10 List (*"represent[ing] a broad consensus about the most critical web application security flaws"), *available at:* https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project.

[14] *See, e.g.*, NIST Cyber-Physical Systems Homepage, *available at:* http://www.nist.gov/cps; *see also*, FTC Staff, *Internet of Things: Privacy & Security in a Connected World* (January 2015), *available at:* http://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

maintained, or disclosed in connection with an organization's cybersecurity activities. How can risks to privacy or civil liberties arising from the application of cybersecurity measures or best practices be addressed in this process(es)?

Business Processes and Enabling Markets

k) **Managed Security Services: Requirements and Adoption**. Managed security services (MSS) allow many firms, particularly small- and medium-sized businesses, to secure themselves without acquiring expensive in-house expertise, yet there are obstacles preventing seamless market cooperation and accountability between clients and vendors. How can a common understanding of security needs by stakeholders enable faster and more efficient adoption to improve security without sacrificing accountability?

l) **Vulnerability Disclosure**. The security of the digital economy depends on a productive relationship between security vendors and researchers of all types who discover vulnerabilities in existing technology and systems, and the providers, owners, and operators of those systems. How can stakeholders build on existing work in this space to responsibly manage the vulnerability disclosure process without putting consumers at risk in the short run?[15]

m) **Security Investment and Metrics**. Market solutions for security require good information. What types of robust, practical, and actionable metrics can be used within organizations to understand security investment, and by consumers and clients to understand security practices and promote market demand for security?

[15] *See, e.g., Vulnerability Disclosure Overview*, ISO Standard 29147 (2014), *available at:* http://www.iso.org/iso/catalogue_detail.htm?csnumber=45170.

This list is not exhaustive. The IPTF welcomes comments on any of these topics, as well as descriptions of other topics that the IPTF and stakeholders should consider for the cybersecurity multistakeholder process. Note that comments are directly sought on which topics to address through the process, rather than the best solution to any given question.

3. Please comment on what factors should be considered in selecting the issues for multistakeholder processes.

IPTF also plans to draw on the Green Paper and earlier responses to past Requests for Public Comment; past respondents are invited to provide additional and updated viewpoints on IPTF efforts since those comments were provided.

Implementing the Multistakeholder Process: Commenters also may wish to provide their views on how stakeholder discussions of the proposed issue(s) should be structured to ensure openness, transparency, and consensus-building. Analogies to other Internet-related multistakeholder processes, whether they are concerned with policy or technical issues, could be especially valuable.

4. Please comment on the best structure and mechanics for the process(es). If different security issues will require different process structures, please offer guidance on how to best design an appropriate process for the issue selected.
5. How can the IPTF promote participation from a broad range of stakeholders, *i.e.*, from industry, civil society, academia, and international partners? In particular, how can we promote engagement from small and medium-sized enterprises (SME) that play key roles in the digital ecosystem? How critical is location for meetings, and what factors should be considered in determining where to host meetings?

6. What procedures and technologies can promote transparency of process, including promoting discussion between stakeholders and ensuring those outside the process can understand the decisions made?
7. What types of consensus outcomes can promote real security benefits without further adding to a compliance-oriented model of security?
8. Would certain cybersecurity issues be better served by a single workshop or other event to raise awareness and promote independent action, rather than a longer multistakeholder, consensus-building process?
9. How should evaluation of the processes be conducted to assess results and to ensure that recommendations and outcomes of the process remain actionable and current?

Response to this Request for Public Comment is voluntary. Commenters are free to address any or all of the issues identified above, as well as provide information on other topics that they think are relevant to promoting voluntary coordinated action to address cybersecurity risks through an open, transparent, voluntary, consensus-based process. Please note that the Government will not pay for response preparation or for the use of any information contained in the response.

Authority: 47 U.S.C. 901(c).

Dated: March 16, 2015.

/S/

_____

Angela Simpson,

Deputy Assistant Secretary for Communications and Information.