May 27, 2015

Mr. Allan Friedman
National Telecommunications and Information Administration (NTIA)
U.S. Department of Commerce
1401 Constitution Avenue, N.W., Room 4725
Washington, District of Columbia 20230

Submitted via electronic mail to securityRFC2015@ntia.doc.gov

Re: Stakeholder Engagement on Cybersecurity in the Digital Ecosystem,
Docket No. 150312253-5253-01

Dear Mr. Friedman,

Microsoft appreciates the opportunity to provide comments in response to NTIA's stakeholder engagement and to contribute to the identification of cybersecurity issues for which broad consensus, coordinated action, and the development of best practices could improve security for organizations and consumers. As we have stated in previous public comments, Microsoft is supportive of a reinvigorated Internet Policy Task Force (IPTF) playing "a more meaningful role in advancing the private sector's perspective in overall cybersecurity policy development."[1] In addition to cybersecurity's role in critical infrastructure protection, cybersecurity should be considered a key enabler of economic development. Advancing security supports economic development by increasing the reliability of and trust in the global digital economy.

As a global technology company, Microsoft has extensive experience developing cybersecurity best practices that enable growth in the digital economy. Microsoft developed and shares widely the Security Development Lifecycle (SDL), our software development security assurance process that is mandated across the company,[2] as well as Operational Security Assurance (OSA), which improves operational security across our cloud services.[3] Microsoft also helped to establish the Software Assurance Forum for Excellence in Code (SAFECode), a multi-company effort to advance industry best practices for software security and integrity. In addition, Microsoft is an industry leader in obtaining certifications that demonstrate our commitment to meeting the security needs of private and public sector organizations. Microsoft has received

[1] Response by Microsoft Corporation to Request for Information (2014), http://csrc.nist.gov/cyberframework/rfi_comment_october_2014/20141010_microsoft_kleiner.pdf.

[2] Security Development Lifecycle, MICROSOFT, http://www.microsoft.com/en-us/sdl/.

[3] Operational Security for Online Services Overview, MICROSOFT, https://www.microsoft.com/en-us/download/confirmation.aspx?id=40872.

multiple Federal Risk and Authorization Management Program (FedRAMP) certifications[4] and was the first major cloud service provider to adopt ISO 27018, the world's first international standard for cloud privacy.[5]

While Microsoft and many of our customers invest significantly in security development, trustworthy platforms, and other best practices, gaps still remain. Because a secure, resilient, and global Internet is vital to achieving the Commerce Department's broader objective of economic growth, Microsoft supports IPTF's role as a facilitator of initiatives to address those gaps. In choosing which cybersecurity issues to take on, we recommend that IPTF focus on issues that are most clearly situated within its remit, enabling IPTF to gain credibility and momentum. Below, in addition to describing which substantive cybersecurity issues are the most pressing and fitting for future work by IPTF, we introduce three issue categories that are intended to help IPTF to prioritize its efforts. We also suggest that, given its authority to bring together Commerce Department bureaus, IPTF choose issues that leverage the bureaus' vast expertise and ongoing efforts.[6]

Moreover, as it designs multi-stakeholder processes to address the cybersecurity issues on which it chooses to focus, we urge IPTF to build from the success of the Cybersecurity Framework development process, which NIST designed to be focused, time-bound, and action-oriented. In addition, to have the greatest impact in a diverse and globally-interdependent economy, we recommend that IPTF engage a broad group of stakeholders. To do so, we recommend that IPTF utilize partnerships to reach low-profile or reserved stakeholders, host geographically dispersed workshops around the United States, and ensure that best practices discussions extend beyond a national dialogue. Furthermore, to provide clarity as it convenes stakeholders, we recommend that IPTF revise its title to reflect its focus on cybersecurity in the digital economy.

Microsoft is committed to working with IPTF and other government and industry partners to build broad consensus, coordinated action, and the development of cybersecurity best practices that will improve security for organizations and consumers. We welcome the opportunity to have future conversations with NTIA, IPTF, and others on these topics.

Sincerely,

J. Paul Nicholas

[4] Microsoft Azure Trust Center, http://azure.microsoft.com/en-us/support/trust-center/compliance/ (explaining that Azure has been granted Provisional Authority to Operate by the FedRAMP JAB); Office 365 Trust Center, https://products.office.com/en-us/business/office-365-trust-center-cloud-computing-security (explaining that O365 has received FedRAMP Authority to Operate from the Department of Health and Human Services).

[5] *Microsoft adopts first international cloud privacy standard*, Microsoft on the Issues (Feb. 16, 2015), http://blogs.microsoft.com/on-the-issues/2015/02/16/microsoft-adopts-first-international-cloud-privacy-standard/.

[6] Department of Commerce Internet Policy Task Force (Aug. 24, 2011), http://www.osec.doc.gov/opog/dmp/doos/doo10_20.html.

Senior Director, Trustworthy Computing
Microsoft

Table of Contents

IPTF Should Focus Its Attention on Three Issue Categories

In its Request For Comments, IPTF proposed 13 substantive cybersecurity issues that impact the digital ecosystem and the potential for global economic growth.[7] To structure our understanding of the issues that IPTF has proposed and the valuable role to be played by the Commerce Department in the cybersecurity space, Microsoft has developed three categories: Information Infrastructure Protection; Cybersecurity for Economic Stability and Growth; and Cybersecurity for Future Prosperity and Progress.[8] These categories, which include each of the 13 issues proposed by IPTF except privacy, have helped Microsoft to evaluate which issues best fit within IPTF's remit and have the most potential to be positively impacted by a multi-stakeholder process. In addition, they provide a framing through which IPTF can define its scope of work and priorities.

We have specifically not included privacy in any of the three issue categories because, given the relationship between privacy and security, we contend that privacy should be treated as a horizontal rather than a discrete topic. As such, rather that convening a multi-stakeholder group specifically devoted to privacy, IPTF should promote privacy more broadly across all discussions about cybersecurity best practices. More specifically, IPTF should require each multi-stakeholder group to include appropriate privacy experts or consultations, assessing and integrating privacy considerations into their solutions or best practices from the outset. Meanwhile, we recognize the value of privacy-specific multi-stakeholder processes that have been convened by NTIA to address mobile app transparency and facial recognition technology.[9] In addition, we recognize that NIST is developing effective processes for privacy impact assessments.[10]

Issue Category	IPTF Proposed Issues	Microsoft Proposed Issues
Information Infrastructure Protection	• Trust and security in core Internet infrastructure • Domain Name System (DNS), Border Gateway Protocol (BGP), and Transport Layer Security (TLS) Certificates • Web security	• PKI, a narrowing of Trust and security in core Internet infrastructure and TLS Certificate issues
Cybersecurity for	• Malware mitigation	• Small and medium

[7] Request for Comment: Stakeholder Engagement on Cybersecurity in the Digital Ecosystem, Docket No. 150312253-5253-01, NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION (2015), at 7-10.

[8] We recognize that the RFC also proposed three categories for the 13 proposed cybersecurity issues: 1) Network and Infrastructure Security; 2) Web Security and Consumer Trust; and 3) Business Processes and Enabling Markets. We developed Information Infrastructure Protection, Cybersecurity for Economic Stability and Growth, and Cybersecurity for Future Prosperity and Progress as categories to highlight areas in which IPTF is particularly well-positioned to lead and that we recommend it prioritize.

[9] Summary Privacy Impact Assessment, NIST, http://www.nist.gov/director/oism/upload/NIST-Management-Resources.pdf.

[10] Privacy Multistakeholder Process: Mobile Application Technology, NTIA, http://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency; Privacy Multistakeholder Process: Facial Recognition Technology, NTIA, http://www.ntia.doc.gov/other-publication/2015/privacy-multistakeholder-process-facial-recognition-technology.

Economic Stability and Growth	• Malvertising • Managed security services • Open source assurance • Vulnerability disclosure • Botnet mitigation • Trusted downloads	enterprise (SME) security services, a broadening of managed security services
Cybersecurity for Future Prosperity and Progress	• Cybersecurity and the Internet of Things (IoT) • Security investment and metrics	• Cybersecurity insurance

First, the Information Infrastructure Protection category reflects the importance of protecting information infrastructure for the entire economy—not just for critical infrastructure. As such, issues within this category expand beyond the scope of but are a central pillar to IPTF's area of work, and the Commerce Department should help to convene stakeholders and contribute to but may rarely drive solutions. Second, the Cybersecurity for Economic Security and Growth category cuts across all sectors of the economy and market sizes, reflecting areas in which trust is needed but must be developed across borders and without the taint of national security. As such, the Commerce Department should own and IPTF should drive work in this category, convening stakeholders to develop solutions and best practices that will support stability and enable growth in the global digital economy. Third, the Cybersecurity for Future Prosperity and Growth category also cuts across all sectors of the economy and market sizes but includes longer-term issues for which precedent-setting best practices are needed. Because issues situated in this category are central to the future of the digital economy and ecosystem, the Commerce Department and IPTF should take initiative in bringing together stakeholders and shaping discussions.

Even with clearly scoped work and a defined set of objectives, though, IPTF must prioritize what to do first. Based on its role as a convener of dispersed stakeholders and need to effect demonstrable progress during a time-bound process, IPTF should apply greater resourcing and relative priority to the Cybersecurity for Economic Stability and Growth category at the outset. As it gains credibility as a convener, IPTF should next take on issues situated within the Cybersecurity for Future Prosperity and Progress category. Finally, narrowly defined issues situated within the Information Infrastructure Protection category should be taken on as they can be supported.

<u>Information Infrastructure Protection</u>

Within this category, Microsoft encourages IPTF to focus on increasing Public Key Infrastructure (PKI) trust, leveraging related work already being undertaken within the Commerce Department. Microsoft also includes within this issue category: trust and security in core Internet infrastructure; Domain Name System (DNS), Border Gateway Protocol (BGP), and Transport Layer Security (TLS) Certificates; and web security. Considering Commerce's position, within this issue category, Microsoft suggests that IPTF focus on PKI—which plays an essential role in e-commerce trust—so that it can build from existing Commerce efforts and best utilize a multi-stakeholder forum.

Cybersecurity for Economic Stability and Growth

Within this category, Microsoft encourages IPTF to focus on vulnerability disclosure, open source assurance, and small and medium enterprise (SME) security services—which, as explained below, is a slightly broader concept than the "managed security services" issue proposed by IPTF. Microsoft also includes within this issue category: malware mitigation; malvertising; botnet mitigation; and trusted downloads. As described above, developing cybersecurity best practices for economic stability and growth is squarely within IPTF's remit. As such, IPTF rightly proposed many topics that fall within this category. However, limited resources and stakeholder fatigue will require IPTF to focus on a narrower set issues. For the reasons outlined below, Microsoft suggests that vulnerability disclosure, open source assurance, and SME security services are the most fitting and important for IPTF to take on—and that developing best practices for coordinated vulnerability disclosure should be considered a priority.

Cybersecurity for Future Prosperity and Progress

Within this category, Microsoft encourages IPTF to focus on IoT and cybersecurity, security investment and metrics, and cybersecurity insurance, an additional issue proposed by Microsoft. Developing cybersecurity best practices that support ongoing innovation and incentivizing wider adoption of existing cybersecurity best practices will greatly impact how the digital economy continues to grow and support new industries. Therefore, IPTF is the right facilitator for longer-term issues situated within this category, and for the reasons outlined in the next section, Microsoft suggests that IPTF take on prioritized issues situated within it.

Key Issues in Information Infrastructure Protection

Within the category of information infrastructure protection, Microsoft encourages IPTF to focus on the public key infrastructure (PKI), an issue that cuts across the economy, affecting organizations of all sizes as well as consumers.[11] Trust in PKI is an important enabler for the digital economy, and IPTF's efforts could complement related work that is already being undertaken within the Commerce Department by the National Institute on Standards and Technology (NIST), an IPTF member.[12] In addition to developing the National Strategy on Trusted Identities in Cyberspace (NSTIC),[13] which may offer an alternative identity management solution to PKI-based infrastructure, NIST has been developing a draft Reference Certificate Policy standard (NISTIR 7924), the purpose of which is to "identify a baseline set of security controls and practices to support the secure issuance of certificates."[14] IPTF could leverage NIST's efforts on that Policy to produce a customized set of operational requirements for resource PKI (RPKI).

Much work needs to be done to fix the structural flaws in PKI and TLS/SSL, and while some solutions have been developed to mitigate those flaws, greater consensus around the right

[11] *In response to* RFC: Stakeholder Engagement on Cybersecurity in the Digital Ecosystem, at 7-8 (PKI and TLS).
[12] Department of Commerce Internet Policy Task Force (Aug. 24, 2011), http://www.osec.doc.gov/opog/dmp/doos/doo10_20.html.
[13] National Strategy for Trusted Identities in Cyberspace (NSTIC), http://www.nist.gov/nstic/.
[14] Harold Booth and Andrew Regenscheid, Second Draft NISTIR 7924: Reference Certificate Policy (2014), http://csrc.nist.gov/publications/drafts/nistir-7924/nistir_7924_2nd_draft.pdf.

solutions or coordination in developing new solutions would provide great value to the digital economy. Reliance on untrustworthy Certificate Authorities (CAs) is an important flaw on which IPTF could focus. Specifically, IPTF could work to build consensus on and spread the use of best practices that will help to increase trust in PKI certificates or reduce the need to trust CAs.

With respect to TLS certificates, the CA/Browser forum is continuously working to improve CA best practices, but the forum is limited by the lack of contact information available in WHOIS, so efforts to integrate DNS/WHOIS and TLS PKI would be helpful. In addition, work is needed to build consensus on how to remove untrustworthy CAs in an orderly fashion. Some applications and embedded devices do not have the capability to easily update their trusted set of root certificates, and many root CAs are "too big to fail" and cannot be removed without disabling many websites. The IPTF could also consider the use of TLS intercepting proxies to decrypt TLS traffic by employers using privately operated PKI. While there are many legitimate reasons for deploying this technology, privately operated PKI are often less secure, and enterprise TLS proxies can also interfere with the deployment of certificate pinning, which is discussed below.

Some potential PKI solutions already exist and could be used as a starting place for IPTF and participating stakeholders in a multi-stakeholder process. For instance, certificate pinning increases trust in certificates, leveraging an expected, pre-existing relationship between an application and an organization or service. Once a public key or certificate is known for a host, the public key or certificate is "pinned" to the host, eliminating the need to rely on a third party CA. In addition, Online Certificate Status Protocol (OCSP) increases trust by requiring CAs to provide responses to every client of a given certificate in real time, and OCSP stapling makes that process efficient by "stapling" time-stamped responses to the initial TLS/SSL handshake.

Key Issues in Cybersecurity for Economic Stability and Growth

Within the category of cybersecurity for economic stability and growth, Microsoft encourages IPTF to focus on vulnerability disclosure, open source assurance, and SME security services. These issues significantly impact and enable the digital economy, and consensus around best practices is needed and can be achieved. In addition, all three issues represent opportunities for broad industry engagement; organizations large and small are affected by the way in which vulnerabilities are disclosed, use open source software, and would benefit from improved security services throughout the digital economy. In addition, among the many other potential issues on which IPTF could focus within this issue category, Microsoft discourages IPTF from developing multi-stakeholder processes around trusted downloads and encourages IPTF to exercise caution in developing processes around botnet mitigation.

First, IPTF should facilitate a multi-stakeholder process focused on vulnerability disclosure,[15] an issue that should be considered a priority for the Commerce Department because it must be managed by a civilian agency and expands beyond context of critical infrastructure. While stakeholders are increasingly converging on support for responsible disclosure, security experts

[15] *In response to* RFC: Stakeholder Engagement on Cybersecurity in the Digital Ecosystem, at 10 (vulnerability disclosure).

and major technology companies have varying perspectives on how vulnerabilities should be disclosed, so developing consensus in a multi-stakeholder forum may be challenging. However, consensus in this area is vital for the digital economy, as consumers and organizations suffer and the economy is threatened by non-coordinated disclosure. In addition, as innovation is occurring more organically around the world and many more companies are becoming IT companies, IPTF should proactively spread best practices, foster greater convergence, and help to avoid a global relearning of those disclosure challenges that have been addressed. Moreover, IPTF should prioritize this issue because ISO 29147 provides a good starting place,[16] and the importance of a multi-stakeholder process is particularly elevated. To develop security and vulnerability disclosure strategies that prioritize the protection of consumers and organizations, the IT industry must work together.[17] Not only IT vendors but also security researchers are vital to this conversation and the developing of best practices around coordinated vulnerability disclosure.

Second, IPTF should consider facilitating a multi-stakeholder process devoted to open source assurance.[18] As software has become increasingly complex to maintain, lack of funding, developer support, and clear accountability for the security of critical open source software projects has resulted in vulnerabilities like that central to the Heartbleed crisis. Some existing industry efforts to improve open source software security exist; for instance, the Linux Foundation has developed the Core Infrastructure Initiative to identify and fund efforts to support critical open source software projects.[19] However, greater awareness and momentum are needed. IPTF could help to generate momentum and new solutions, facilitating discussions about secure development practices and responsible and equitable patch distribution.

Third, IPTF may also consider facilitating a multi-stakeholder process focused on developing, supporting, and promoting SME security services. Such a process would go beyond developing managed security services, also enabling SMEs themselves to build, support, and consume more secure and resilient apps and services. As such, a multi-stakeholder group might discuss APIs, SDKs, and the use of cloud services as well as managed security services.[20] Ultimately, this multi-stakeholder group would support broader cybersecurity education efforts in the U.S. government and private sector, offering a hands-on approach to SME cybersecurity education. In addition, SMEs would function as buying groups, providing economies of scale and reducing costs.

Fourth, within this area of cybersecurity for economic stability and growth, Microsoft discourages IPTF from focusing on trusted downloads.[21] Trusted downloads is too broadly scoped an issue to make meaningful progress within an IPTF multi-stakeholder process. In

[16] ISO/IEC 29147:2014, http://www.iso.org/iso/catalogue_detail.htm?csnumber=45170

[17] Chris Betz, *A Call for Better Coordinated Vulnerability Disclosure*, MSRC (Jan. 11, 2025), http://blogs.technet.com/b/msrc/archive/2015/01/11/a-call-for-better-coordinated-vulnerability-disclosure.aspx.

[18] *In response to* RFC: Stakeholder Engagement on Cybersecurity in the Digital Ecosystem, at 8 (open source assurance).

[19] Core Infrastructure Initiative FAQ, LINUX FOUNDATION, http://www.linuxfoundation.org/programs/core-infrastructure-initiative/faq; *see also* http://blogs.microsoft.com/cybertrust/2014/04/24/microsofts-commitment-to-the-core-infrastructure-initiative/.

[20] *In response to* RFC: Stakeholder Engagement on Cybersecurity in the Digital Ecosystem, at 10 (managed security services).

[21] *In response to* RFC: Stakeholder Engagement on Cybersecurity in the Digital Ecosystem, at 9 (trusted downloads).

addition, an IPTF process devoted to trusted downloads would be redundant; both industry and a nonprofit have developed and are working hard on solutions to the issue. For instance, Microsoft has developed the SmartScreen filter[22] and other technologies,[23] and StopBadware has been focused for years on the prevention of as well as mitigation and remediation measures for badware websites.

Fifth, botnet mitigation,[24] while important, is an area in which established collaboration among industry and international law enforcement is working successfully. For instance, Microsoft's Digital Crimes Unit (DCU) has worked with many industry partners and international law enforcement officials to successfully disrupt numerous botnets.[25] Specifically, botnet disruption operations require close coordination and operational security. As such, IPTF's proposed coordination of work on botnet mitigation is unnecessary and may cause industry confusion.

If, however, IPTF chooses to take on the issue of botnet mitigation, then we would urge IPTF and the multi-stakeholder group that ultimately forms to bring together a broad group of stakeholders and focus on areas in which activity is not already underway. For example, IPTF could engage hosting providers in addition to access and other service providers. Substantively, IPTF could commission research on legal impediments that hamper collaboration on botnet operations or on the economic impact of botnets on the American public and competitiveness, the results of which may encourage stakeholders who have not yet been involved to participate in mitigation and cleanup efforts. IPTF could also closely examine the system of incentives for consumers to maintain device security, including a study of the most effective practices for notifying victims of a botnet or distributing cleaning tools to botnet victims. Similarly, IPTF could consider the role of CERTs in the education and effective notification and remediation of infected computers.

Key Issues in Cybersecurity for Future Prosperity and Progress

Within the category of cybersecurity for future prosperity and progress, Microsoft encourages IPTF to consider focusing on IoT and cybersecurity, security investments and metrics, and cybersecurity insurance. All three issues have the potential to significantly shape future technologies and cybersecurity best practices, though IoT and cybersecurity is a particularly pressing issue. As last year's National Security Telecommunications Advisory Committee (NSTAC) report highlighted: "there is a small—and rapidly closing—window to ensure that IoT is adopted in a way that maximizes security and minimizes risk. If the country fails to do so, it will be coping with the consequences for generations."[26] The forecasted increase in the number of Internet-connected devices—from 13 billion in 2013 to 50 billion in 2020—will lead to a

[22] SmartScreen filter: frequently asked questions, MICROSOFT, http://windows.microsoft.com.
[23] How Microsoft antimalware products identify malware and unwanted software, MICROSOFT, http://www.microsoft.com.
[24] *In response to* RFC: Stakeholder Engagement on Cybersecurity in the Digital Ecosystem, at 7 (botnet mitigation).
[25] *See, e.g.*, Microsoft partners with Interpol, industry to disrupt global malware attack affecting more than 770,000 PCs in past six months (Apr. 12, 2015), http://blogs.technet.com.
[26] NSTAC Report to the President on the Internet of Things (Nov. 19, 2014), http://www.dhs.gov, at ES-1.

dramatic extension of the possible attack surface.[27] As such, we are currently at an inflection point and must make sure the necessary policies are in place before the attack surface multiplies.

Before beginning any new work in the area of IoT and cybersecurity,[28] Microsoft encourages IPTF to consider existing successful industry models for an IoT and cybersecurity working group, ensuring that IPTF is efficient, focused, and effective. For example, in late 2014, automakers representing over 90 percent of cars sold in the United States announced a set of Privacy Principles that they will follow for connected cars and data collected from them.[29] In addition, a new working group should leverage NIST's Cyber-Physical Systems (CPS) Public Working Group[30] as well as NIST's Global Cities Challenge, which is encouraging collaboration and the development of standards for smart devices and systems in the transportation, energy, manufacturing, and healthcare sectors.[31] Participating cities benefit from the experience of others to lower costs and improve efficiency in IoT standards development. By leveraging the Global Cities Challenge and CPS Public Working Group, IPTF can build from NIST's already assembled group of stakeholders as well as its standards development work.

IPTF could focus its IoT efforts on both the supply and demand sides of security challenges. For instance, to increase demand for scalable security solutions for IoT, IPTF could seek to catalyze the development of guidance and best practices for consumers and small business that are using IoT in their homes and workplaces. In addition, IPTF could convene leading IoT product and service providers to aggregate security best practices. The multi-stakeholder group could then look for ways to incentivize others in the industry to adopt these best practices to raise consumer security. Alternatively, because governments drive IoT investments for infrastructure like smart roads or buildings, an IPTF multi-stakeholder process could use its collective power to define security baselines and standards for those government investments in IoT infrastructure. No matter its ultimate focus, the multi-stakeholder group should focus on IoT devices and services that pose the greatest risks to consumer and enterprise productivity within the digital economy.

Second, IPTF could consider facilitating a multi-stakeholder process focused on security investments and metrics.[32] If IPTF chooses to do so, then Microsoft encourages the Task Force to narrow its scope of potential security investments and metrics topics by deciding to build on existing Commerce Department efforts. Specifically, Microsoft suggests that an IPTF multi-stakeholder process focus on security metrics that would enable stakeholders to measure the impact of NIST's Cybersecurity Framework. An IPTF multi-stakeholder process could study the

[27] *Is the Internet of Things strategic to the enterprise?* ZDNet, http://www.zdnet.com/.

[28] *In response to* RFC: Stakeholder Engagement on Cybersecurity in the Digital Ecosystem, at 9 (cybersecurity and IoT).

[29] *See* IoT Privacy Summit 2015, http://www.truste.com/events/iot/ (this session will review the Principles in detail, explain how they work in practice, and review the process by which they were adopted and socialized); *see also* https://www.globalautomakers.org/media/press-release/automakers-commit-to-privacy-principles-to-protect-vehicle-personal-data.

[30] Cyber-Physical Systems, NIST, http://www.nist.gov/cps/. The CPS PWG has been launched to bring together experts to help define and shape key aspects of CPS to accelerate its development and implementation across multiple industry sectors.

[31] Smart America: Global City Teams, NIST, http://www.nist.gov/cps/sagc.cfm.

[32] *In response to* RFC: Stakeholder Engagement on Cybersecurity in the Digital Ecosystem, at 10 (security investments and metrics).

costs of implementing the Framework or some other measure of economic impact (e.g., calculating how many of a certain kind of attack have been blocked), ultimately helping stakeholders to understand who is using the Framework, why they're using it, and what the associated return on investment is—which could support the business case for cybersecurity.

Third, Microsoft proposes that IPTF consider facilitating a multi-stakeholder process focused on cybersecurity insurance. As businesses consider various strategies to manage their cyber risk (i.e., mitigate, transfer, and accept), the insurance industry may accelerate investment in and demand for security products. Moreover, the White House lists cybersecurity insurance as one of the principle incentives for adoption of NIST's Cybersecurity Framework.[33] Relatedly, shortly after the release of the Framework, a representative from a global insurance broker observed that the Framework "will increase the need for insurance because it'll clarify a cybersecurity standard of care that more companies will have to fulfill."[34] Indeed, though it will take significant time to develop and mature, the cyber insurance market is already growing steadily.[35] In coordination with other U.S. government efforts,[36] IPTF could convene a multi-stakeholder group to look closely at the growing cyber insurance market and determine what additional steps might be taken to further stimulate growth of this important market.

IPTF Should Deliver White Papers for Prioritized Issues within 12 Months

Microsoft encourages IPTF to design multi-stakeholder processes that will be focused, time bound, and action oriented. As an active participant with NIST and other industry partners during the Cybersecurity Framework's development, we learned that being focused, time bound, and action oriented were critical to the Framework's successful development process. Specifically, Microsoft encourages IPTF to first focus on and learn from a small number of priority issues—including vulnerability disclosure—before considering whether and how to take on additional issues. In addition, to establish a clear agenda for the issues that it chooses to pursue, Microsoft encourages IPTF to launch multi-stakeholder processes for an initial period of 12 months, during which time each group of stakeholders would be able to discuss, develop, and publish a white paper. Through its white paper, each group would evaluate whether valuable and feasible work can be done by the group and, if so, outline the group's goals and plan of action going forward.

In addition, Microsoft encourages IPTF to design multi-stakeholder processes that encourage a broad and diverse stakeholder group to participate, collecting information from all stakeholders and producing outcomes that are scalable across geographies, industries, and market sizes. In developing the Cybersecurity Framework, NIST's decision to have geographically distributed

[33] Incentives to Support Adoption of the Cybersecurity Framework, WHITE HOUSE, https://m.whitehouse.gov/blog/2013/08/06/incentives-support-adoption-cybersecurity-framework.

[34] Judy Greenwald, *Cyber security framework unveiled*, BUSINESS INSURANCE (Mar. 2, 2014), businessinsurance.com.

[35] In 2014, the number of March & McLennan clients purchasing standalone cyber coverage increased by 32 percent over 2013. Benchmarking Trends: As Cyber Concerns Broaden, Insurance Purchases Rise, MARSH (2015).

[36] The Department of Homeland Security and the Treasury Department have begun to hold meeting with insurance and technology experts, seeking to examine the impacts of cyber insurance on the market and on security.

interaction opportunities with stakeholders resulted in a more diverse stakeholder group. As such, similarly, Microsoft encourages IPTF to host for each multi-stakeholder working group quarterly workshops around the country. Moreover, Microsoft encourages IPTF to leverage existing working groups and industry conveners to reach a broader audience.

To bring together and represent the expertise of the diverse community of cyber stakeholders across geographies, sectors, and market sizes, IPTF will need to explore and integrate into existing communities and demonstrate to them that their investment in participating will result in tangible benefits. For instance, gaining the support of and using space provided by existing groups like the Silicon Valley Leadership Group or venture capitalist firms may help IPTF to engage innovative small businesses and entrepreneurs. In addition, as it moves across geographies and industries, IPTF must customize its messaging and language to the various stakeholders or audiences that need to be engaged. In addition, to demonstrate progress and stakeholders' return on their investment in its processes, IPTF must show that it is agile and iterative.

IPTF Should Revise its Name and Consider Impacts of Cybersecurity on Trade

As IPTF prepares to stand up various multi-stakeholder processes, Microsoft encourages it to consider whether the Internet Policy Task Force's title should be revised to better reflect its focus on cybersecurity in the digital economy. Whereas an Internet policy group might focus on anything from Internet governance to intellectual property, a cybersecurity group has a clearer and more concentrated set of policy issues on which it is focused. Because it will be bringing together a vast array of stakeholders and ideally convening various regional workshops, IPTF should ensure that its mandate and goals are as clear as possible to potential participants.

We also note 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 IPTF to coordinate closely with its Commerce stakeholders as well as other agencies focused on commercial and trade issues. Doing so will ensure not only that the consistency of cybersecurity measures with countries' international commitments is examined and considered but also that the global economic effects of such measures are well understood.

Conclusion

Microsoft appreciates the opportunity to provide feedback to IPTF regarding its plan to stand up multi-stakeholder processes and develop much-needed cybersecurity best practices and standards. As it prepares to kick off an initial round of processes and working groups, we encourage IPTF to focus on a relatively narrow set of issues on which it can achieve measurable and important impact. In addition, Microsoft encourages IPTF to focus on issues that would enable it to leverage the existing efforts of its Commerce Department stakeholders.

Specifically, Microsoft encourages IPTF to focus on vulnerability disclosure. In addition, IPTF may consider developing multi-stakeholder processes for PKI trust, open source assurance, IoT and cybersecurity, cybersecurity investments and metrics, or cybersecurity insurance. Over a period of 12 months, multi-stakeholder processes devoted to such issues could assess whether and how they should attempt to fill an existing gap by: achieving consensus around coordinated vulnerability disclosure best practices; developing best practices or standards to improve PKI trust and open source software security; creating guidelines or best practices programs for secure IoT products or services; measuring the impact of the Cybersecurity Framework; and supporting growth of the cybersecurity insurance industry. To enable broad participation in the processes, we encourage IPTF to host quarterly workshops around the country and consider what a fitting title for the convening group or task force might be.

Microsoft looks forward to the opportunity to continue with IPTF the conversation that this RFC has initiated.