Microsoft

Microsoft's Response to Request for Information

U.S. Department of Commerce, National Institute of Standards and Technology

Information on Current and Future States of Cybersecurity in the Digital Economy

I. Introduction

Microsoft Corporation (Microsoft) appreciates the opportunity to provide comments to the U.S. Department of Commerce (Commerce) and specifically the National Institute of Standards and Technology (NIST) in response to its request for information (RFI) on Current and Future States of Cybersecurity in the Digital Economy to inform Commission on Enhancing National Cybersecurity (the Commission).

Microsoft commends the Commission for leveraging numerous mechanisms, including open hearings across the country, and this RFI process to engage with public and private sector stakeholders as well as consumers to solicit input to help shape the Commission's thinking and recommendations. Our understanding is that the Commission is using this RFI to seek information on 10 broad topics, and specifically for each topic, on current and future challenges, promising and innovative approaches to address these, recommendations, and references to inform its work.

While the Commission's work and the RFI are appropriately wide ranging, Microsoft's response to the RFI focuses on five targeted recommendations. We believe these recommendations have the potential for the greatest overall impact. But we also recognize that moving from recommendation to reality will require considerable deliberation and specific, actionable, and often nuanced approaches in order to enable progress, as they are aligned with highly complex issues. Specifically, Microsoft believes that as part of its overall effort, the Commission should make the following recommendations:

- Create an effective national cybersecurity architecture to resolve competing equities and create clarity in governance;
- Advance and promote greater domestic, and in particular international, use of the Cybersecurity Framework to help advance both security and economic growth.
- Embrace innovation and stimulate the deployment of new technologies and knowledge, with a particular urgency to accelerate improvements in identity management and security of Internet of Things (IoT);
- Leverage the full range of incentives and disincentives available to catalyze cybersecurity improvements in the development and operation of technology, including to address areas where market forces fail or leave critical gaps; and
- Develop focused and effective programs for public awareness and education, to improve engagement and adoption of the best technologies and practices, and to expand the workforce.

We expand on each of these recommendations below.

II. Effective National Cybersecurity Architecture

One of the greatest challenges facing the U.S. Government, and in fact many governments and companies around the world, is how to integrate, and when necessary, create the organizations, structures, authorities, and processes needed to effectively manage cybersecurity. Collectively, we need to create an effective architecture for cybersecurity governance, spanning principles, roles, and responsibilities within the government and across the public and private sectors.

This challenge exists, in part, because there is incredible diversity in cybersecurity needs and capabilities across organizations in both the private and public sectors. Within the government, for example, different organizations have unique authorities and responsibilities to fight crime, protect federal agencies and critical infrastructure, support continuous innovation and economic opportunity, support education and housing, oversee internal revenue, support agriculture and land management, and take necessary actions to protect national security and public safety. This diversity means that on occasion, different responsibilities and priorities may be in tension and require balancing and reconciliation. Industry introduces even more diversity with different drivers, such as shareholder value, as well as different responsibilities and capabilities.

The need for improved approaches to governance is not new. It has been noted numerous times, including in the Cyberspace Policy Review and by the President's Review Group on surveillance. Indeed, there has been incremental progress on governance over the last few years, primarily via cross-agency collaboration and more "whole of government" efforts, which used traditional mechanisms like interagency coordination committees. Earlier this year, the Cybersecurity National Action Plan also attempted to address some of these issues, notably establishing a Federal Chief Information Security Officer.

While these efforts are laudable, they do not go far enough. Several examples demonstrate the need for more robust mechanisms to bring together differing interests and expertise (and in the case of government, authorities), and to enable collaboration to find balanced approaches. For example, during revisions to the Wassenaar Arrangement it became apparent that the combined expertise of the arms control, security, and civil liberties communities had not been leveraged to formulate a position that considered the interests of each. The encryption debate, while involving representatives with different perspectives, continues to struggle to find an acceptable conclusion. And finally, consistent reporting about the government's challenges in securing its operations and data shows that difficulties exist in how cyber risks are managed across the Federal enterprise.

There are at least two areas where tensions between competing responsibilities and priorities should be addressed in an effective architecture. First, in the governance of technology concerns broadly, involving the public and private sectors and civil society, and where there may be competing equities regarding national security, economic security, and civil liberties; and second in governance within the public sector, focused on responsibilities and authorities for technology and cyber risks. Each affects the other, hence why they should both be considered within a national architecture for cybersecurity. For example, if the government has greater clarity on how to work together internally, they will be better positioned to engage with industry and civil society to govern the broader set of issues. Similarly, greater clarity on how to govern competing equities associated with broad technology challenges should help simplify internal governmental efforts to engage and collaborate on those issues. We'll speak to each of these two areas below, and provide examples and recommendations for each.

Governing Competing Equities Across Public and Private Sectors and Civil Society

The US Government must continue to improve how it works with diverse stakeholders to manage competing equities associated with technology. A clear example of where a more robust discussion of competing equities and how to balance them is needed has to do with how government agencies discover, buy, and handle vulnerabilities. Governments have competing equities when it comes to the buying and handling of vulnerabilities: the priority to protect users and the government by reporting vulnerabilities to a vendor may conflict with a desire to hold and eventually use a vulnerability for other national security purposes. While the U.S. Government has made statements regarding its "vulnerabilities equities process" (VEP), those statements have been limited and are primarily in the form of a blog post and a redacted version of an internal policy document. Additionally, concerns have been raised that the current approach doesn't yet balance equities in a way that best advances the range of U.S. economic and security interests at play.

While the above example might be illuminating, it is just one of the many equity challenges created by technology. The challenge of balancing equities is relevant for almost all technology concerns - including in policy efforts to

define international norms of behavior, in procurement processes, in operational efforts to exchange risk management information to protect cyber infrastructure or to counter violent extremism, and in technical efforts to control access to computing resources. Since no single organization in the government or in industry has the needed expertise or authority to address the multifaceted nature and competing equities associated with technology, the development of a governance structure is fundamental to making progress on cybersecurity.

With that in mind, we urge the U.S. to continue to improve its approaches to governing and managing technology opportunities and risks with a goal of better addressing the complex interplay of national security, law enforcement, economic interests, and civil liberties. Importantly, this doesn't necessarily mean having more people involved, but rather having the right people with the right expertise involved for specific challenges. Nor does it require new groups, but rather challenges us to rethink how to get various groups to work together – both within the public sector and between government and industry. Finally, it doesn't necessarily mean there is a single entity in charge of resolving competing equities for all cases, rather an effective governance model will involve a set of organizations and participants - from government, industry, and civil society - and an orchestrated approach to integrating the expertise and capabilities of each.

This effort should be coordinated and managed from the Executive Office of the President (EOP). In structuring this model, there should be a few key priorities: 1) clearly defining roles and responsibilities not only for the individual participants, but also focusing on how those participants function relative to each other; 2) structuring, orchestrating, and incentivizing cross-group coordination and collaboration, but doing so in a way that is agile and doesn't require additional resources; and 3) focusing on and delivering against specific outcomes. Working on a more dynamic, effective, and inclusive model for governance is critical because technology will continually surface issues that have implications for national and economic security, private sector interests, and the interests of citizens, domestically and globally.

Broad transformational ideas are needed to truly govern competing equities in a more effective national cybersecurity architecture. That said, we urge the government to act on the recommendations below for a more immediate effect. These recommendations have been made previously, but have not yet fully been implemented. Also, while not defining a specific governance model, these will better position the Federal government to be able to collaborate with industry and civil society to develop and then implement a strong governance model for managing competing equities. Some of the near-term recommendations the Commission should make include:

- Create greater coordination between the National Security Council (NSC) and National Economic Council (NEC) at the White House, specifically addressing impediments that have hindered coordination to date;
- Better leverage the diversity of expertise and experience available through existing public private partnerships by focusing on more specific outcomes and involving Subject Matter Experts (SMEs) with the needed expertise for the challenge at hand; and
- Develop larger and more formalized programs and initiatives, beyond those that exist today, that help foster the development of a professional cybersecurity workforce in the U.S. Government with cross-agency and cross-domain expertise and experiences.

Governing Competing Equities within the U.S. Government

The US Government must also better govern how it works internally to develop, procure, integrate, and manage technology and cyber risks. As noted above, the various departments and agencies within the Federal government have different missions, unique authorities and responsibilities, and varying technology environments, face risks; this diversity can create both uncertainty and tension, and requires greater clarity and reconciliation.

These competing equities within government also play out across policy, operational, and technical efforts. In the operational space for example, certain agencies may have high volume, and high security transactions that need to be resilient (e.g., online filing of tax returns), while others may maintain large data sets used internally within the government but not available publicly (e.g., weather modeling). These organizations will have different technology, face different cyber threats, different resources, and different capabilities to manage risks.

In order to better manage competing equities within government related to technology and cybersecurity, and to be more efficient and secure, the Commission should encourage the Federal Government to build a more robust organization-wide model for cybersecurity, to increase agility in procurement and integration of technology, and to consistently measure how risk is being managed and drive continuous improvement. Each of the recommendations are discussed below in turn, with examples where relevant and proposed steps on which the Commission may elaborate.

- Build a more robust, organization-wide governance model for federal cybersecurity to enable more effective coordination and collaboration. In April, the Cybersecurity National Action Plan (CNAP) established a Federal Chief Information Security Officer (CISO) role, creating an opportunity to institute an operating model whereby agency CISOs regularly interact, coordinate, and collaborate with the Federal CISO and their agency counterparts. The Federal Government may consider creating an action-oriented executive branch-wide cybersecurity leadership team through which the new Federal CISO can regularly convene agency CISOs and oversee initiatives or decisions that affect multiple agencies. In that forum, CISOs may also consider opportunities to capitalize on security, cost, and personnel talent efficiencies by incentivizing the use of common platforms and shared security services, including commercial managed security services.[1] That council should also regularly confer with its Chief Information Officer (CIO) Council peers to establish joint priorities and proactively identify opportunities and challenges.
- Be more agile in procuring, integrating, and managing new and upgraded technologies, which incorporate the most advanced security capabilities and features, while retiring legacy systems that pose operations and maintenance burdens and security challenges. As the pace of technology development continues to accelerate, so too must the pace at which the government can assess, adopt, integrate, and manage those new technologies, ensuring that agencies can utilize the most up-to-date capabilities and features that are better suited to meet the security needs of a range of government scenarios. The need for increased agility is particularly acute in the context of cloud computing because new capabilities and features can be continuously added to existing services. While FedRAMP Accelerated helped to establish a faster initial authorization process, increased agility is still needed in continuous monitoring and as additional feature sets augment services with existing certifications.
- Regularly measure, compare, and drive improvement in agency implementation of cyber risk management. Many organizations find value in organizing their approach to risk management around the five functions—identify, protect, detect, respond, and recover—that are described in the National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* (2014). In March, the National Security Telecommunications Advisory Committee advised President Obama to utilize the *Framework* functions to "implement risk management in a prioritized, thorough,

[1] Attachment to the Letter to the President – Emerging Technologies Strategic Vision, https://www.dhs.gov/publication/2016-nstac-publications

and consistent way," articulating vital steps and considerations in the context of each function.[2] In particular, as part of the "protect" function, Federal CISOs should regularly review the extent to which agencies are fostering the necessary risk management culture for cybersecurity. This includes ensuring the necessary leadership, processes, and resourcing to manage basic cyber hygiene, including patch management, identity management, whitelisting, access control, and isolation/segmentation of environments.[3]

By creating greater clarity on the needs and capabilities of the public and private sectors and developing improved processes and structures for governance, the U.S. will be better positioned to understand and manage the right balance between various equities. In doing so, the U.S. will better integrate and balance the interests of stakeholders, including law enforcement, national security, civil liberties, and economic security, and will be able to procure and manage its own infrastructure in a way that advances its own innovation, productivity, and security.

III. International use of the Cybersecurity Framework.

A number of governments around the world are currently developing cybersecurity strategies, legislation, regulations, guidelines, and standards, many of which reference the need for security baselines – not only for the government, but also for critical infrastructure and information and communication technology providers. In Europe, for example, the Network and Information Security (NIS) Directive will require governments to establish security baselines for essential services and digital service providers.

How governments approach the development and implementation of security baselines will have profound effects on both security and economic development. Fragmented, inconsistent approaches will redirect limited resources from security to compliance. Alternatively, leveraging, building from, and further developing and promulgating existing best practices with demonstrated results would help to advance security and enable nations' economic opportunities.

There are currently no widely referenced policy guidelines that governments are consistently leveraging. Many are reinventing the wheel or on a path towards burdensome compliance regimes with minimal impact on security. In the U.S., the NIST Cybersecurity Framework has emerged as a leading best practice in cyber risk management. The structure of the Framework's Core facilitates communication within and between organizations. In addition, as it incorporates risk-based and outcome-focused principles, the Framework is highly adaptable. Many U.S. organizations have highlighted its value for their operational risk management, and the Canadian, Italian, and Japanese governments have translated and/or utilized it as well.

However, adoption by other governments in their policy efforts has still been quite limited, in part due to limited exposure and information as well as interest in leveraging international rather than other sovereign approaches. The U.S. government also has an opportunity to be a leader in establishing international best practices for cyber risk management public policy. Microsoft proposes the Commission recommend the U.S. Government:

- Develop and advance a cross agency strategy to deliberately drive global conversations about and raise the visibility of the Framework, the inclusive approach used to develop it, and the outcomes based approach. The U.S. Department of State should include training on the use of the Framework in all of its global cybersecurity capacity-building efforts. Likewise, the White House should highlight the Framework

[2] Attachment to the Letter to the President – Emerging Technologies Strategic Vision, https://www.dhs.gov/publication/2016-nstac-publications

[3] Attachment to the Letter to the President – Emerging Technologies Strategic Vision, https://www.dhs.gov/publication/2016-nstac-publications

in its strategic cybersecurity partnerships. As a globally respected government and industry partner, NIST should also continue to facilitate a range of conversations to support implementation of the Framework in the U.S. and beyond;

- Support efforts to establish international standards based on the Framework, to foster greater harmonization of cybersecurity practices on a global scale; and
- Utilize the Framework in procurement to drive adoption, including referencing the Framework in its Special Publications and positioning the Framework as a recommended requirement for U.S. government procurement. In addition, the Office of Management and Budget (OMB) should determine how best to align the Framework to Federal Information Security Management Act (FISMA) requirements and ensure that Framework best practices are included in procurement requirements. This OMB step may also require amending the relevant Federal Acquisition Regulations as appropriate.

Drawing international support and consensus for this Framework will require collaboration with multilateral organizations and partnerships with industry. We believe that this Commission has a unique opportunity to use the success of the NIST Cybersecurity Framework to promote consistent approaches to cyber risk management abroad. Such alignment of global approaches will not only support improved security and economic development but also facilitate increased coordination, collaboration, and trust among partner nations.

IV. Identity Management and Security of Internet of Things (IoT)

In addition to looking at federal governance structures as they pertain to cybersecurity, we recommend the Commission further explore the challenges and opportunities arising from the emerging IoT landscape. The growth of Internet enabled devices across virtually all sectors will complicate the operational landscape of ICT providers, customers, products, and services that defenders are working to protect every day. In this heterogeneous environment with countless different types of devices made by countless different vendors, and numerous operators involved in the delivery of services, identity management will become even more important than it is today.

For the purposes of this response, identity management should be seen as the ability to identify hardware, software, data, and, when appropriate, people, and to use those identities to manage access and security. As such, it already provides a core mechanism to manage access to confidential information, as well as the basis for managing operational environments. The latter is critically important and can include decisions underlying both cyber and physical operations and security for governmental and critical infrastructure functions, large-scale and small-scale transactions and management, as well as social interactions. As growth in IoT causes even greater proliferation of devices, software, services, and data, we must make progress on identity management to help manage access and security at scale and across environments.

Despite its importance, advancing identity management as a policy priority can be difficult for a variety of social, technical, economic, and political reasons. First, the different cultural perspectives on privacy, identity, security, and anonymity complicate progress and ability to reach agreement across international and cultural boundaries.

Secondly, from a technical perspective there are numerous different ways to manage identity, reflecting the diversity of the software, hardware, and services environment discussed above. Moreover, individuals and machines typically use dozens of credentials spread across multiple providers. It needs to be noted that significant effort is required to compile, exchange, and interpret the identities even in a single system, much less across different ones.

Thirdly, the lack of clear economic incentives has meant that there has only been limited progress in developing the necessary technologies and standards to enable federation between the different systems and approaches

used – although that has begun to emerge. For example, industry is collaborating on the technical challenges associated with federation through the Fast Identity Online (FIDO) Alliance[4], which is working towards improving identity management through standardization and improvements in technological capabilities. Moreover, numerous other standards, guidelines, and specifications for identity management have been created by multiple national and international standards development organizations.

Greater government support would help catalyze industry and global standards organizations to adopt and adapt existing security and privacy techniques, as well as research and adopt techniques relevant for IoT solutions. IoT solutions are built by a variety of stakeholders, often outside of the technology sector, that may not be familiar with information security practices and are optimizing more for cost and power efficiency. As a result, available IoT hardware platforms generally lack many of the security features taken for granted in personal computer platforms. For example, IoT often do not use secure software development techniques described in ISO/IEC 27034, and those needing higher levels of security rarely include support for the trusted platform module techniques described in ISO/IEC 11889 which, for example, help protect data at rest and enable cryptographic keys to be used for identity.

Based on the sheer number of IoT devices, (in some cases) their rudimentary user interface elements, and their likelihood to be deployed in physical locations or form factors that are not easily accessible, automated management and maintenance are critical for the lifecycle of the device. Government is in a unique position to act as a convener, facilitating industry cooperation in developing new technologies, standards, ways to integrate and build from existing technologies, and accelerating needed developments on critical issues, such as security and interoperability. Microsoft proposes the Commission recommend the U.S. Government:

- In partnership with industry, **engage more proactively to support international standards for identity management** that advance (a) levels of assurance, (b) interoperable security languages and taxonomies, (c) identity claims, (d) automated security assessment sharing, and (e) user privacy, especially for IoT. This should include support for standards and technical capabilities, such as those advanced by the FIDO Alliance, that enable federation between different systems and approaches used;
- **Initiate another series of pilot projects**, much like those managed under the National Strategies for Trusted Identities in Cyberspace, in order to establish the economic and security benefits of new identity management technologies and solutions, including those enabled by cloud computing, such as managing identities over a large scale;
- **Convene stakeholders to specifically focus on how best to align existing and emerging requirements** and conformance models across international borders, vital to enhancing interoperability and creating economies of scale; and
- **Assess areas where identity management techniques or policies have been developed and implemented outside the U.S. with a focus on learning from others**. Identity management policies and programs are emerging in various countries and regions around the world. The U.S. should both seek to lead by example, and continually learn from others to drive progress on this critical priority.

There are immediate and longer term benefits to accelerating improvements in identity management, especially as we move to secure emerging technologies. As highlighted above, Microsoft believes that the US Government can act as a catalyst for establishing common ground between the different stakeholders in this field and play a leadership role internationally, advancing not only the interests of the U.S. and industry, but also the security of the online ecosystem as a whole. As billions of devices become connected, the ability to manage those devices securely - irrespective of owners and vendors involved – will become critical. It is our view that our window of

[4] https://fidoalliance.org/

opportunity to ensure that the security lessons learnt by the ICT industry in the 1990s are not forgotten but built upon, is narrowing. We encourage the Government to take steps, as proposed above, to ensure that does not happen.

V. Incentives and Disincentives to Improve Cybersecurity

Most governments struggle with how to effectively drive improvements to security, while still enabling producers and users of technologies sufficient flexibility to address a dynamic risk landscape, compete in a global environment, and innovate new features and functionalities, including those that advance security. The diversity of business models across sectors means that not all organizations and individuals are equally incentivized by the same market forces to invest in their shared cybersecurity responsibilities commensurate with the risks they face. These diverse groups face very different threats, not only from opportunistic actors seeking financial gain, but also from determined adversaries with greater capabilities, more financial resources, and a multitude of complex geo-political and geo-economic objectives.

Identifying gaps between what the market can and should drive and what the risk environment requires is a crucial step towards determining when and how to leverage the range of incentives and disincentives available to improve security. Governments have numerous legal and policy mechanisms they can leverage to help incent and when necessary, require, producers and users of technologies to take particular actions to improve security, and to hold them accountable if those actions aren't taken – these mechanisms include developing standards, fostering insurance markets, creating tax incentives, using procurement preferences, establishing liability, and setting regulations. Legal and policy mechanisms can be (and in some cases already are) used by the private sector in their own procurement processes.

Against this background, the question of balance between voluntary "opt-in" frameworks versus regulations for improving cybersecurity posture of organizations becomes central; ultimately the scope of the various approaches put into effect will have a significant effect on national and economic security. Specifically, approaches that rely solely on voluntary opt-in mechanisms are unlikely to recognize that some national security threats exceed what is commercially reasonable to expect companies to do. An example often raised is whether it is reasonable to expect a rural electricity cooperative to defend itself and its customers against a sophisticated and determined nation state adversary. On the other hand, approaches which rely solely, or too heavily, on liability or regulation will have a negative effect on the economy and security, hindering innovation and redirecting limited resources from security to compliance. A good example here is the balance that needs to be struck when it comes to emerging technologies, such as IoT; there are security risks, but how might strict regulations affect innovation, especially for smaller players? Furthermore, it is important to remember that bad actors don't have to follow any rules, and that therefore unduly constraining good actors would only exacerbate the "offense beats defense" advantage.

Much of the conversation to date about when to use voluntary versus regulatory approaches to drive behavior to improve security has focused on how to better manage operational cyber risks to ICT systems and data – typically discussed as part of critical infrastructure protection efforts. This focus most often concentrates on the security roles and responsibilities of users of technology, and not necessarily the security approaches used by those who develop the technology.

The focus on improving operational risk management, and in particular "cyber hygiene" is and remains essential, and is a priority on which the Commission should make specific recommendations. At least 85% of the targeted cyber intrusions that the Australian Signals Directorate (ASD), for example responds to, could be prevented by following four mitigation strategies, including application whitelisting, patching applications, patching operating system vulnerabilities, and restricting administrative privileges to operating systems and applications based on

user duties.[5] That number is even higher in the Microsoft ecosystem; according to Matt Miller, a Principle Software Security Engineer in our Cloud and Enterprise organization, upwards of 90% of successful threats that use vulnerabilities are using ones for which an update is already available, but hasn't yet been deployed. As such, guidance on how to create an appropriate mix of incentives and disincentives to drive investment and action by technology users that improve operational risk management would be useful. It would also be helpful to have greater data on what challenges inhibit technology users from taking actions known to reduce risks, for example understanding the difficulties in applying updates in operational systems, as this might point to areas for greater research and development.

Concurrent with efforts to improve operational security, there are also increasing number of players in the public policy conversation that wonder about what the responsibilities of those who produce technology should be. Some express frustration about the continuing presence of security vulnerabilities in software products and services, and question whether and how to use business practices and policy tools to reduce the number and/or severity of vulnerabilities in software *before* the technology is deployed in operational environments.

Software vendors began taking action to improve the security of the code for products and services almost 15 years ago. This area of practice, typically described as software assurance, seeks to encourage developers to build more secure software and address security compliance requirements. Many producers of technology, in particular large scale vendors, developed, implemented, and are constantly refining their practices to improve software assurance. Many also have specific corporate policies, programs, training, and tooling that help improve the assurance of their code.

For example, Microsoft uses the Software Development Lifecycle (SDL) to ensure the software that underlies the service is designed, developed, and deployed with security in mind throughout its entire lifecycle.[6] Vendors also collaborate with each other to share and promulgate practices for software assurance. For example, the Software Assurance Forum for Excellence in Code (SAFECode) is a non-profit organization exclusively dedicated to increasing trust in ICT products and services through the advancement of effective software assurance methods.[7] There is also an international standard, ISO/IEC 27034, a process-based standard, which offers guidance on specifying, designing/selecting and implementing information security controls through a set of processes integrated throughout an organization's Systems Development Life Cycles (SDLC).

Ensuring that developers - regardless of size – have processes in place to receive vulnerability information from third party finders and respond when vulnerabilities are identified is an essential component of a software assurance strategy. Vulnerability handling involves having the ability to: communicate with third party finders; validate and triage vulnerabilities; develop and deploy an update (aka "patch") to mitigate the vulnerability; and apply issued updates to systems that are in operation. As with tools to improve the assurance of code, technology providers have invested in developing best practices for vulnerability disclosure and handling. There are two ISO standards, ISO 29147 and ISO 30111, that describe processes for receiving vulnerability information from third party finders, communicating with finders about reported issues, and investigating, triaging, and resolving vulnerabilities.

Efforts to improve software assurance and manage and respond to vulnerabilities once identified have demonstrably improved cybersecurity, and case studies demonstrate that it is both more effective and costs less to integrate security in the lifecycle of technology rather than "bolting" it on afterwards. Yet despite the availability

[5] http://www.asd.gov.au/infosec/mitigationstrategies.htm

[6] https://www.microsoft.com/en-us/sdl/default.aspx

[7] https://safecode.org/about-safecode/

of best practices, guidelines and tooling to improve software assurance and some vendors' efforts in this space, implementation lags considerably.

First, while most large scale technology vendors are taking actions to improve software assurance, not all software is developed or managed by those vendors. In fact, the number and types of non-IT companies (e.g. banks, car companies, toy and appliance manufacturers) that are producing and deploying software code is growing, and will only grow more rapidly as IoT and mobile application use expands across different sectors of the economy. These organizations often do not have experience or expertise in software development or security, and software assurance practices cannot necessarily be easily nor consistently applied in these relatively smaller scale development environments.

Second, open source is increasingly being used and shared across the ecosystem, including by the Federal government,[8] yet is often maintained by volunteers, without specific requirements or processes for secure development or clear accountability or funding to respond to security issues that do arise. Industry's collective effort to provide funds to critical elements of the global information infrastructure through the Core Infrastructure Initiative will help to address some challenges, however, as use of open source grows, there will need to be more consideration of how to similarly foster improvements to the assurance of it.

Third, implementation of software assurance also lags in no small part because many users, including not only consumers, but also enterprises, small and large, do not understand the impact of their technology purchasing decisions on their cybersecurity, do not have the necessary means to measure the impact of their investments in security, or simply do not have the resources to purchase new technology or implement new processes. The level of security needed varies, and is often unclear, which creates uncertainty and relatively low market demand for more secure ICT software and services.

There are a myriad of efforts underway to catalyze security improvements in the development and use of technology, for example by the Underwriter's Laboratories for IoT, and by numerous agencies including the Federal Communications Commission and the Federal Financial Institutions Examination Council, but greater work to leverage and create a mix of incentives and disincentives is needed. The Commission should explore and make specific recommendations to:

- Drive improvements to operational security, including by creating a more balanced mix of incentives and disincentives to drive investment and action by technology users. Identify areas where market forces fail or leave critical gaps, and leverage or create the necessary regulatory frameworks to address those gaps. Inventory specific challenges that inhibit technology users from taking actions known to reduce risks, for example, applying updates in operational systems, as these challenges should inform future research and development.
- Promote better software assurance, including by fostering more incentives, specifically procurement preferences generally, and the standards development, for example through the Underwriters Laboratories Cybersecurity Assurance Program, for non-traditional software producers.[9] Also initiate research to assess specific high risk scenarios, determine what level of security may be necessary, and recommend when disincentives may be necessary to address risks that exceed market expectations.

  In crafting this recommendation, the Commission should emphasize the importance of a risk-based approach to carefully define an appropriate scope for each of the legal and policy mechanisms available to drive behavior. While there are a small set of risk scenarios where liability or regulation may be appropriate, the level of security necessary and appropriate for various scenarios remains unclear. As a

[8] https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m_16_21.pdf

[9] http://www.ul.com/newsroom/pressreleases/ul-launches-cybersecurity-assurance-program/

result, broad policies seeking to leverage law or regulation are challenged. The majority of efforts to promote software assurance should focus on incentivizing the marketplace and with only very narrowly tailored disincentives, such as liability and regulatory mechanisms, targeted to address particularly high risk scenarios where market forces cannot address risk.

- Ensure that software assurance policies leverage international standards, such as IEC/ISO 27034, ISO 29147, and ISO 30111, and focus on the processes used to develop and fix software (i.e., how software is built and how vulnerabilities are mitigated) rather than the presence of vulnerabilities.
- Seek to foster greater awareness of the role that software assurance and technology purchases have on operational risk, including through public awareness and education. The Commission should also encourage government engagement to enable conversations between ICT buyers and suppliers about how security is managed in the development and management of technology products and services over time, and how best to demonstrate practices in these areas.
- Fund research and development to advance cybersecurity models. Many of the models informing cybersecurity today were developed in the 1970s and did not envision the diverse, heterogeneous, and rapidly changing technology landscape in which we operate even now; and tomorrow will be even more complex. The Commission should encourage the Government to perform research and development that truly advances our cybersecurity models and better accounts for the complexity and scale of tomorrow's challenges.

Discussions of where market forces fail or leave critical gaps in cybersecurity, both in the development and operation of technology, are complex and sensitive. Quite often, they tend to emphasize either incentives or disincentives rather than considering the full range of both available to catalyze improvements. There are numerous legal and policy mechanisms available - including developing standards, fostering insurance markets, creating tax incentives, using procurement preferences, establishing liability, and setting regulations – and effective approaches are likely to include a mix - carefully scoped to advance both national security, economic security, and innovation.

V. Public Awareness and Education

Technology and policy considerations often dominate discussions of cybersecurity, but the fundamental human element of the issue is equally important. Significant compromises can occur because of an event as trivial as an individual clicking on a link thought to be trusted, opening a file from a supposedly trustworthy source, or inserting a USB stick that contains malware into a computer. At the same time, given the prevalence of computing today, it is important that responsible, smart and safe behaviors are instilled, and computer science skills developed in our youth from an early age. As such, Microsoft strongly supports the Commission's focus on public awareness and education.

Increasing public awareness and having users to exercise behaviors that lead to improved online safety is easier said than done. Human behavioral change is difficult and does not happen in the same almost instantaneous time scale in which the Internet operates. Moreover, research shows a majority of individuals adopt safer online habits and practices only after something bad has happened to them. Not only are the vast majority of citizens not aware of the dangers online until it is too late, but also many knowingly choose convenience over actions that could protect them.

Microsoft has long believed in the power of the individual and that individuals are best placed to make decisions about their own digital freedom. As a result, we feel we have a responsibility to empower them to make smart, informed decisions about, and to shape their experiences in, life online. To that end, we provide a broad collection

of tools and resources to inform and equip citizens and prepare as they navigate life in our 21st century digital world.[10] At the same time, we know we cannot do it alone. Microsoft therefore encourages the Commission to take the following considerations into account, when developing recommendations on public awareness-raising and education:

- Fund research to advance internet safety. Research plays a critical role in identifying factors that increase online risks and dispel myths that can lead to misplaced efforts. Government funding is essential for both academic and market research in these areas.
- Increase access to computer science education. Microsoft appreciates that computer science education, particularly starting in primary and secondary school, is necessary to help build a tech talent pipeline that will spark new innovations for the future. We have invested in providing computer science education to young people, helping them gain the computational-thinking and problem-solving skills necessary for success in the future,[11] and believe the government must similarly invest in our future.
- Require online safety education in schools. Microsoft believes that online safety curricula should become an integral part of schools' efforts to achieve technological literacy for their students, and should include modules focusing on online safety, online security, and online ethics. Microsoft encourages government to partner with internet technology providers, online safety organizations, and school districts to help fill this need, using a range of available online safety curricula.
- Promote more informed choices. To promote more "informed choices" by people who might be exposed to illegal or harmful content or conduct, Microsoft encourages governments to explore partnerships with non-governmental organizations to promote public-service announcements with links to positive messaging and diverse references on sensitive topics.
- Continue dedicated awareness campaigns. Microsoft has played an active role in the National Cyber Security Alliance and in STOP. THINK. CONNECT. from the beginning. We believe these are important and effective tools for driving a single focus at a particular point in time and should be continued in partnership with a broad selection of stakeholders. We firmly believe that together – as industry, government, NGOs, child safety organizations, law enforcement agencies and others – we can accomplish more than any single entity or organization on its own.
- Strengthen resources for consumers. The FBI has been promoting increased awareness of ransomware and providing resources to consumers to learn more about protecting themselves from falling victim to ransomware incidents. The U.S. should continue to promote efforts like this – including awareness from the Federal Trade Commission and other agencies – to help continue to make resources and information available to consumers for knowledge of what to do before, during, and after an attack.
- Support public and private partnerships. Technology companies, governments, businesses, and consumers must work together to innovate, develop, and deploy effective solutions. Together, we help protect consumers through legal actions to stop cyber criminals, such as shutting down botnets, and through other efforts such as PhotoDNA, a technology that helps industry and government find and remove some of the worst images of child sexual abuse from the internet. Governments and industry must continue to work together to establish safety principles and adopt policies that enable technology

[10] http://www.microsoft.com/about/corporatecitizenship/en-us/youthspark/youthsparkhub/programs/onlinesafety/resources/

https://www.microsoft.com/about/philanthropies/youthspark/youthsparkhub/programs/onlinesafety/resources/

[11] https://www.microsoft.com/about/philanthropies/youthspark/youthsparkhub/

providers to determine the most effective means of implementation. This approach provides the flexibility needed to address the ever-changing online risk landscape.

The Government has a vital role to play in helping individuals understand how the decisions they make online affects themselves and the broader cyber ecosystem. Existing campaigns have gained recognition and have proven successful in generating awareness, and that momentum and support must continue to ensure we prepare our society for the cybersecurity challenges ahead. Microsoft is also a strong proponent of being more focused in programs for public awareness and education with greater consistency and specific targets for behavioral change, as it is clear that the majority of people do not understand their roles and continue to be implicated by their own behavior. Support for and investment in multi-generational awareness and education will have impact now and for years to come.

VI. Conclusion

Microsoft appreciates the opportunity to provide these comments to NIST and the Commission on Information on Current and Future States of Cybersecurity in the Digital Economy. The cybersecurity challenges facing the U.S. and the global economy are real and increasing; yet there are specific, practicable recommendations that should be actioned to position our government and businesses to effectively and efficiently manage cyber risks. Microsoft appreciates the government's outreach on these important issues and welcomes opportunities to work with NIST, the Department of Commerce, the Commission, and this and future administrations in considering how best to manage and improve cybersecurity.

Sincerely,

Paul Nicholas,

Senior Director, Global Security Strategy and Diplomacy

Microsoft