MICROSOFT RESPONSE TO THE DEPARTMENT OF COMMERCE GREEN PAPER ON CYBERSECURITY, INNOVATION, AND THE INTERNET ECONOMY

Docket No.: 110527305-1303-02

Dated: September 21, 2011

Microsoft Corporation (Microsoft) files these comments in response to the Green Paper on Cybersecurity, Innovation, and The Internet Economy ("Green Paper") published by the Department of Commerce, through the Office of the Secretary, the National Institute of Standards and Technology, the International Trade Administration, and the National Telecommunications and Information Administration, (collectively, "Commerce" or "Department") dated June 8, 2011. Microsoft provides these comments to supplement our initial response submitted on August 1, 2011.

Microsoft appreciates this opportunity to provide additional input on the Department's proposal for a new "Internet and Information Innovation Sector" (I3S) and a proposed set of public policies intended to help improve the cyber security of infrastructures within that sector. The proposal is inherently complex and raises a number of significant and challenging questions, in part because the proposal has intersections with other existing legal authorities and with ongoing legislative proposals from the Administration aimed at improving cyber security in critical infrastructures.

In responding to the proposals in the Green Paper, we offer a set of three themes to help constructively guide the Administration's policy efforts to increase security and foster innovation across infrastructures – both critical and non-critical. The new sector proposed in the Green Paper is called the Internet and Information Innovations Sector or the "I3S"; the themes we offer in our response similarly reference three I's—Innovation, Interoperability and Incentives, which we believe are central to "improving the overall cyber security posture of private sector infrastructure owners and operators, software and service providers." Our exploration of these themes also provoked a series of questions we believe require further consideration by both government and industry.

1) *Improving security without stifling innovation requires innovation*: DHS and the private sector must work together with Commerce to define a more nuanced and innovative approach to designating and managing cyber risks for Information Technology infrastructures – those critical for national security, public safety, and economic security, and those that fall outside of the Critical Infrastructure Key Resource – and ensure that methods designed to encourage companies that operate critical infrastructure to improve the security do not compromise their ability to deliver innovative technologies to the market. We believe the following questions require additional consideration in order to achieve the appropriate balance between security and innovation for critical and non-critical infrastructures:
    a. What are reasonable security goals and objectives for infrastructure that is critical but does not meet the criteria to be covered critical infrastructure?
    b. How can government and industry work together to address risks associated with the challenging decisions of how to utilize limited resources?

   c. At what point does infrastructure become so critical to economic security that it becomes a national security concern?

2) *Interoperability eases implementation*: Infrastructure risks are constantly evolving and challenging to precisely define. Infrastructure that may be designated as Covered Critical Infrastructure (CCI) and infrastructure which is critical but not CCI (i.e., National Information Infrastructure (NII)) are inherently interdependent on each other, and such designations as CCI and NII may change over time as the use of technologies change. As such, proposals intended to improve security for NII must also be considered with other related cyber security legislative proposals. While mechanisms to drive security improvements for both the CCI and NII may be different, they must also be fundamentally related because the approaches to enhance cyber security should be consistently risk-based, the interdependency between infrastructures, and the dynamic nature of the risks. These approaches should, to the greatest extent possible, be risk-based, prioritized, compatible, and interoperable so that the overarching security principles and voluntary behavior intended to create a security baseline for NII would become the foundation for any requirements for CCI imposed through regulation. We believe the following questions require further consideration as the Department considers how to drive security enhancements across infrastructures:
   a. How can government and industry define an interoperable framework that can accommodate the dynamic nature of infrastructure risks and the shift between CCI and NII infrastructures?
   b. How can DHS and Commerce work together and with the private sector to enhance security without stifling innovation?
3) *Commitment and Leadership as Incentives*: The clearest way to demonstrate the importance and value of codes of conduct is for government to lead by example through incorporating them into government operations, requiring their adoption in procurement decisions, and promoting them internationally to help define a set of global norms of behavior.
   a. How can government procurement practices be updated to make decisions based on best value and security so we leverage the market power of government to enhance security?
   b. How can Commerce, working in partnership with DHS, work with industry to promote similar Code of Conduct on an international basis to foster a secure and cohesive global marketplace?

We offer the following comments to help structure an approach by which companies can achieve their primary functions – developing products and services for the benefit of their customers – while supporting the important goal of stronger security.

Introduction

As one of the world's largest software company and a leader in the development of innovative, Internet-based information products and services, Microsoft is committed to helping our customers realize their full potential. In the Information Age, governments, industries, and consumers around the world rely on globally connected networks and cyber systems, and create and store volumes of sensitive data electronically. At the same time, we find both ourselves and our customers facing a rapidly changing threat landscape driven by malicious actors who develop attacks that can have impacts at machine-speed, motivated by competitive or strategic advantage, or financial gain. The fundamental challenge put forth by the Green Paper is about excelling in the Information Age—how to enhance the cyber security of consumers, businesses, and the Internet infrastructure to protect the tremendous economic and social value of the Internet without stifling innovation.

In responding to the proposals in the Green Paper, we organized our response and mapped the associated questions from the Green Paper using the three key themes—Innovation, Interoperability, and Incentives—we believe will help constructively guide the Administration's policy efforts to increase security and foster innovation across infrastructures.

Improving security through innovation

Defining and designating infrastructure[1]

Microsoft recognizes and appreciates there may be infrastructures that, while critical, do not have the potential to impact national security or public health and safety in the same way as the infrastructure that may be designated as CCI. We also support the notion that government has some role, albeit a very narrow one, to work with industry to define reasonable security objectives and to promote and incentivize private-sector efforts to improve cyber security for infrastructures that are not CCI. We do not, however, believe that the designation of a new sector is either an accurate representation of the economy, or necessary to promote the behavior Commerce wants to see occur.

Microsoft believes that the concept of an Information Technology (IT) Sector, as originally defined in the National Infrastructure Protection Plan (NIPP), as "an aggregate of primarily virtual and distributed functions…that provide hardware, software, IT systems, and services," remains an accurate representation of the segment of the economy driven by IT Sector companies. More importantly, the NIPP framework is designed to accommodate the risk environment of the IT Sector, recognizing that it

[1] *The relevant questions from the Green Paper addressed in this response include: How should the Internet and Information Innovation Sector be defined? What kinds of entities should be included or excluded? How can its functions and services be clearly distinguished from critical infrastructure; Should I3S companies that also offer functions and services to covered critical infrastructure be treated differently than other members of I3S? Is Commerce's focus on an Internet and Information Innovation Sector the right one to target the most serious cyber security threats to the Nation's economic and social well-being related to non-critical infrastructure? What are the most serious cyber security threats facing the NII as currently defined? Are there other sectors not considered critical infrastructure where similar approaches may be appropriate?*

highly diverse, virtual, interconnected, and international, with a constantly changing threat landscape, and interdependencies within the IT Sector and between the IT Sector and other critical infrastructure sectors.

We have observed that traditional “sector-based” approaches to managing risks have inherent limitations when applied to the IT Sector. Traditional approaches tend to apply a “one-size fits all” approach to managing risks, yet with infrastructure that is so diverse, risks that are so dynamic, and interdependences that are so complex, a more nuanced and risk-based approach is needed for the IT Sector. Such an approach could help drive security enhancements and create a healthier ecosystem, while enabling companies to focus on their primary function— creating new products and services.

Rather than defining a new sector, Microsoft recommends that Commerce work with the Department of Homeland Security (DHS) to understand the parameters of the IT Sector established under the NIPP, and then work with DHS and the IT Sector to leverage the existing partnership framework and identify any infrastructure that “would fall outside the classification of covered critical infrastructure as defined by existing law and Administration policy”(i.e., National Information Infrastructure (NII).

Defining this portion of the IT Sector is challenging for many reasons. First, there is a bit of a sequencing challenge, i.e., defining what is *not* CCI and how to improve its cyber security is more complicated when policy makers and industry are still struggling to define what *is* CCI and how to improve its security. Moreover, while we believe such an effort should start with the six critical functions as defined by the IT Sector under the NIPP, that definition was designed to be fairly open and adaptable to accommodate the evolving nature of IT products and services, and wasn’t created with the consideration that further segmentation of the Sector would be necessary. Thus, any actions in this space should be done in partnership with DHS to ensure that the framework and risk-based approaches outlined in the NIPP are not adversely impacted.

Thinking Through CCI and NII

Despite these challenges, we believe that there can be an innovative approach for designating IT Sector infrastructure as either CCI or as NII (i.e., infrastructure that is critical but may not have sufficient national security and public safety risks to be covered by the pending policy proposals intended to regulate some critical infrastructures). Microsoft does not take a position on what infrastructure comprise CCI and NII – rather, this discussion is offered only to help think through the challenges associated with such a delineation. In our internal discussions of the definition of the NII, we created a graphic (Figure 1 below) to help articulate the distinction between CCI and NII based on the risks that could result for a disruption, failure, or compromise.

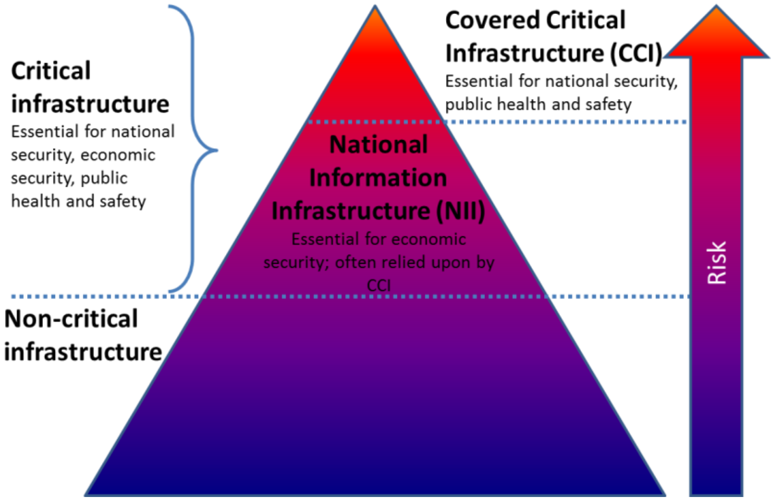
Critical infrastructure
Essential for national security, economic security, public health and safety
Non-critical infrastructure
National Information Infrastructure (NII)
Essential for economic security; often relied upon by CCI
Covered Critical Infrastructure (CCI)
Essential for national security, public health and safety
Risk

Figure 1: Categorizing IT infrastructure based on risk

Microsoft does not support different processes or criteria for the designation, but rather for a unified, risk-based process that will create cohesive, interoperable efforts to enhance cyber security for both CCI and NII. Such a process must be collaborative and include meaningful investment from key government agencies and from private sector stakeholders. The process should have the following characteristics:

- *Infrastructure- (not Entity) Focused*: Designation of infrastructure and the associated risk management activities, whether as CCI or NII, cannot be done at a sector or entity level (one-size does not fit all); rather because of the diversity of infrastructure and dynamic risks, these efforts must be done at the function, process, system, or asset level. While we appreciate the simplicity of focusing on entities, such an approach would not guide limited resources to achieving the appropriate security goals for infrastructure with differing risks. For example, many IT Sector entities operate infrastructure that could be considered critical (e.g., Internet routing and access), but may also operate infrastructure that is not (e.g., mobile gaming applications), and resources should be focused more on protecting critical functions than misallocated to protect non-critical functions at the same level.

- *Risk-Based*: The designation of infrastructure, whether as CCI or NII, must be based on risks associated with disruption, failure, or compromise. We believe that policymakers should start that risk-based process by defining CCI as those functions, processes, systems, or assets (not entities) that if destroyed, incapacitated, or exploited could have *significant* negative consequences to national security and public safety. Using these criteria, the scope of CCI in the IT Sector would be very small— only a few functions, processes, systems, or assets in the IT Sector would have the necessary scale and impact to have a first order impact on national security and public health and safety. On the other hand, when considering the NII, we believe that it should focus on infrastructure that is essential for economic security and innovation; using these criteria, the scope of NII would be much broader than that of CCI. While much of NII may be relied upon by CCI, it would not have the potential to create direct impacts like CCI. Finally, using this approach, there would also be a very broad set of infrastructure that, while important, falls outside of the Critical Infrastructure Key Resource designation.

- *Interoperable and Flexible*: Any process to designate infrastructure and manage risks must be interoperable and flexible. Because the IT Sector is continually innovating new products and services, any strict segmentation today will be outdated in a few years, if not a few months. Also, risks change—potential consequences fluctuate, both in scale and time, known vulnerabilities are addressed and new vulnerabilities identified, and threats evolve. Finally, when using a function, process, system, or asset approach, the two regimes must ultimately be compatible and interoperable because there are entities that may operate both CCI and NII.

  Whatever framework is created to determine whether a system, asset, or network is CCI or NII, it must be done in a way that is consistent, repeatable, and applied equally. Having a framework that depends upon circumstance is unsustainable in a business environment. It must also address technological evolution. In other words, infrastructure that may still be developing today, or has not yet even been imagined, could eventually reach a magnitude of scale whereby it becomes critical in the future; similarly, infrastructure that is critical to national security now, could eventually be supplanted by new products and services and no longer meet the threshold for being CCI. Accordingly, we recommend that if Commerce undertakes this work, it aligns closely with DHS and the private sector to ensure that the processes for managing cyber risk for both CCI and NII be constructed to ensure that they are clear, risk-based, technology-neutral, and work together as seamlessly as possible.

- *Market-Driven Compliance*: While in most cases, CCI will be (in some manner) dependent on NII, Microsoft believes that no additional incentives or requirements would be necessary for NII relied upon by CCI. We are concerned that imposing specific security requirements on entities that operate NII relied upon by CCI would create barriers to entry for companies, whereby owners and operators would have to choose whether they create products and services for use in the national security domain or the commercial environment. Creating disparate approaches would break the current model whereby commercial-off-the-shelf (COTS) products and services can be procured at competitive prices and then deployed and managed in a manner customized for the unique risk environment in which they operate. Furthermore, the owners and operators of infrastructure, not the entities that rely on that infrastructure, are best positioned to understand and manage the risks in their environment. Accordingly, we recommend that owners and operators of CCI impose obligations upon the NII entities from which they purchase products and services in order to satisfy their own regulatory obligations.

Using the process outlined above, we believe that CCI and NII could be defined in a manner so as to drive interoperable security enhancements in both infrastructures without modifying existing authorities or those proposed in some of the policy proposals regarding CCI (Figure 2 below). Rather, the approach acknowledges the need for narrowly scoped regulation, involving both DHS and primary regulators, to meet national security requirements for some critical infrastructures; accounts for DHS' existing coordination authority for critical infrastructure protection as defined in the Homeland Security Act of 2002; and highlights Commerce's responsibility for raising awareness of security considerations and fostering cyber security education and training to drive economic and technological development, as well its role as an expert and convener in the standards community via NIST.

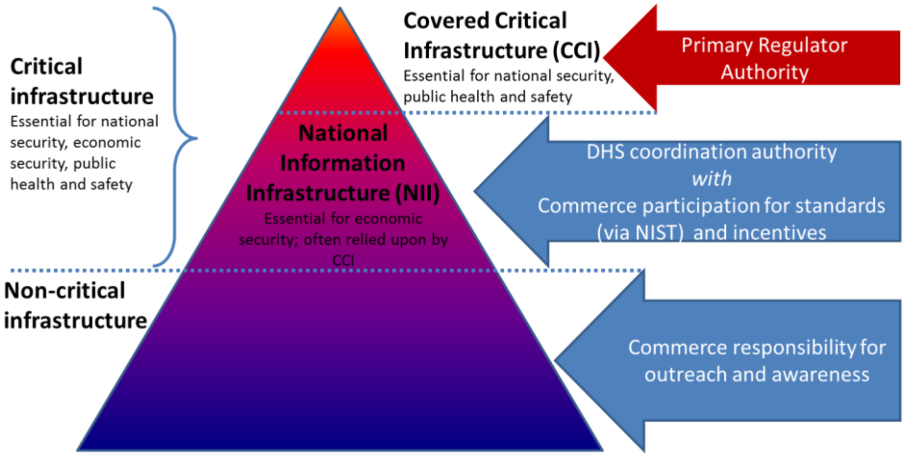
Critical infrastructure
Essential for national security, economic security, public health and safety
Covered Critical Infrastructure (CCI)
Essential for national security, public health and safety
Primary Regulator Authority
National Information Infrastructure (NII)
Essential for economic security; often relied upon by CCI
DHS coordination authority *with* Commerce participation for standards (via NIST) and incentives
Non-critical infrastructure
Commerce responsibility for outreach and awareness

Figure 2: Graphical representation of authorities and responsibilities for IT infrastructure

The difference between this model and the existing paradigm is based on Commerce's comment in the Green Paper that "[e]ven the most effective means for cybersecurity are useless if entities do not adopt them." While DHS, working with private sector, should define reasonable security goals and objectives for the NII, and NIST should facilitate the development of international standards, *Commerce also has a role to play in helping to create a marketplace environment that incentivizes private-sector improvements to cyber security.*

Microsoft believes that DHS and Commerce, through its policy office and NIST, should work together as follows:

- *Department of Homeland Security*: DHS should work with the private sector and other government partners, including Commerce and primary regulators, to articulate cyber security goals and objectives. Put another way, DHS should work under the NIPP framework to identify cyber security risks and priorities to help create a baseline of security for CCI and NII. DHS should also work with NIST, where appropriate, to foster development of standards for outcomes where none currently exist. CCI would be the subject of primary regulatory oversight and either third party or, in rare cases, government audits. For example, the owners and operators of information technology systems that control nuclear power plants would be subject to the primary regulatory authority of the U.S. Nuclear Regulatory Commission (NRC). The NRC would understand what security goals and objectives are necessary, based on the guidance from DHS, and work in cooperation with nuclear infrastructure owners and operators to ensure that the proper mix of people, policies, and technology are in place to mitigate those risks that cannot be tolerated.

DHS should also develop processes to exchange best practices that would exceed the security baseline so that organizations can achieve higher levels of security when they deem it necessary to address their own unique risks. We offer additional information on this role in our response to questions concerning the development of codes of conduct below.

- *National Institute of Standards and Technology*: NIST also has an important role to play in the area of promoting improved cyber security for NII. We agree that NIST is the appropriate agency to facilitate the development of cyber security technology and standards through the Cyber Security Division of its Information Technology Laboratory. NIST must also continue to engage in an open and transparent process with industry in the process of developing any guidance for private industry. It is also sensible to coordinate the government's engagement in standards setting bodies—and NIST is best suited to this role. It is imperative that NIST be adequately funded so that it has the necessary in-house expertise to take on the task of working with the private sector for these efforts.

- *Department of Commerce*: Commerce, working in close coordination with DHS, should continue to lead cyber security outreach and awareness for all infrastructures, critical and non-critical, and should become a more active participant in the current NIPP process, catalyzing existing market incentives to improve cyber security. See more in Commerce's role for outreach and awareness in our responses to questions concerning incentives.

As noted, when discussing the role of DHS, Microsoft strongly believes any effort to enhance cyber security must be risk-based, and focus on appropriate and feasible goals and objectives. For NII, this means recognizing that all companies, and in particular the small- and mid-sized innovators that help advance the state-of-the-art in technology, have limited resources. Therefore, driving investments in one area will most often create opportunity costs in another. With that consideration, we do not believe that the question of "most serious cyber security *threats*" as included in the Green Paper is the right approach. Instead, we believe that efforts to improve cyber security of NII should be focused on addressing the highest *risks*, and that these risks are quite often concerns that are not related to conventional "actor and intent" threats.

For infrastructure supporting innovation and economic growth, the risks of greatest concern are often associated with the challenging decisions of how to utilize limited resources. As NII providers advance the state-of-the-art in technology, investments in either innovation or security will necessarily drive improvements in one while creating opportunity costs in the other. This natural tension is one that infrastructure owners and operators face today. It is of particular concern when considering what security gains can truly be realized across the NII, and the impact of such efforts, even if voluntary, on companies, especially on small and mid-sized businesses.

More broadly beyond the IT Sector, policy makers in the Administration should pursue a careful reconciliation of which sectors and infrastructures are, in fact, critical using the infrastructure-focused construct outlined above, with a greater consideration of risks to national security and public health and safety. While some sectors (e.g., Nuclear) are well-suited to traditional 'sector-based' risk management approaches, others (e.g., Communications and Healthcare and Public Health) may be like the IT Sector and require a more nuanced and innovative approach. We believe that existing policy defining critical infrastructures is overly expansive and, in fact, presents one of the greatest risks to efforts to increase the security of the infrastructure that is truly critical. The tendency to use broad sweeping and loosely defined criteria to define critical infrastructure creates regimes in which too many things are critical, leading to a bloated governance and management structure for both government and industry, driving unwieldy inventorying and reporting requirements, and consuming and misappropriating limited resources, thereby distracting and reducing the effectiveness of both government and industry efforts.

Developing codes of conduct[2]

As outlined above, identifying existing and developing new codes of conduct cannot be successfully accomplished without first better understanding the security goals and objectives the government and private stakeholders are trying to reach and behaviors and outcomes that are desired. First, as outlined when describing DHS' role, DHS, its government partners, including the Department, and industry need to set strategic context and define reasonable cyber security goals and objectives for NII, while carefully considering the diversity of players, infrastructure, operations, and risks in the ecosystem. These security goals and objectives must recognize and appropriately balance the natural tension between improving cyber security and innovation.

We believe this set of cyber risk management principles could then form the basis of voluntary codes of conduct—a collection of recommended security goals and objectives that, if appropriately incentivized, would drive adoption of standards and widely accepted industry practices, and therefore, raise the level of cyber security across NII. As noted in the discussion of roles above, codes of conduct could be used to advance the principles and establish a baseline of security. Entities could, as they deem necessary, also implement additional controls to improve the robustness of their operations, products, and services. If appropriately based on globally recognized, voluntary, consensus-based standards and widely accepted industry practices, voluntary codes of conduct would be an effective means to promote adoption of sound security principles by NII providers. Codes of conduct can be effectively developed and promulgated through a respected third party industry group. Leveraging the work of existing industry groups, such as the Sector Coordinating Councils (SCC) and Information Sharing and Analysis Centers (ISAC), would reflect a consensus-based process that demonstrates the collective best practice of the overall industry. It would also facilitates the development of principles that are not specific to any particular product or any one company, which instills more confidence in the process and minimizes concerns from customers, vendors and/or regulators.

Driving broader implementation of widely accepted industry standards will need to be a key goal, but we recognize that standards have not kept pace with the cyber security landscape and must evolve

[2] *The relevant questions from the Green Paper addressed in this response include: Are there existing codes of conduct that the NII can utilize that adequately address these issues? Are there existing overarching security principles on which to base codes of conduct? What is the best way to solicit and incorporate the views of small and medium businesses into the process to develop codes?*

more quickly. We strongly support the development of industry-led practices to augment existing standards. While standards benefit from the wide variety of participants and expertise in the development process and often represent "best of breed," they are developed through a deliberative process, which means that they will necessarily lag behind cutting edge developments in security practices and technologies. This gap should be addressed, in part, by promoting widely accepted industry practices to ensure that best of breed processes, practices, and technologies can be implemented as available.

As an example, the ICT community identified secure software development as an objective, developed and recommended a set of key principles for secure development, and promulgated those principles through SAFECode.[3] The implementation of these principles has yielded marked improvements in the security of software products. There are six core principles- all of which are non-proprietary and consistent with accepted security and software development practices.

- Technical personnel involved in software development should complete a practical and comprehensive course of secure development training and commit to ongoing training, on an annual basis
- There should be a documented minimum development standard for security and privacy mandated for the organization
- A threat model should be produced for applications under development; product specifications should include mitigations for identified threats
- Secure coding practices should be a requirement using either established, generally accepted techniques or new practices that produce the same effect
- Applications should be tested using dynamic security analysis methods and reassessed against the threat model
- Applications should include a final security review, archival of tools and artifacts necessary for post-release servicing and a documented, actionable incident response plan

These principles are broad, longstanding, scalable, and inherently flexible, which allow entities to implement organization-specific practices, policies, and procedures appropriately tailored to address their respective mission, goals, and priorities.

The Australian iCode,[4] a voluntary code of practice for Australian Internet Service Providers (ISPs) to improve cybersecurity for all consumers, is another example of industry practices, implemented at scale, driving security improvements in the ecosystem. The code provides a consistent approach for Australian ISPs to help inform, educate, and protect their customers in relation to cyber security to reduce the number of compromised computers in Australia. At Microsoft, we believe that government and industry must continue to explore ways to work together and to leverage the collective impact of our defenses to help improve the security.

[3] The Software Assurance Forum for Excellence in Code (SAFECode) is a global, industry-led effort to identify and promote best practices for developing and delivering more secure and reliable software, hardware and services. Its members include Adobe Systems, EMC, Juniper Networks, Microsoft, Nokia, SAP and Symantec.

[4] http://www.icode.net.au/

Some subsectors or entities, however, may lack the resources or expertise to establish an internal cyber security function to define or meet the principles outlined in the code of conduct, yet these subsectors and entities should have a strong business interest in and responsibility to their customers for security. In these cases, NIST can consider how to foster and promulgate a managed security service model, whereby small and medium businesses (SMBs) could outsource security management to a service provider to serve as a normalized business model. Lack of security and technical expertise, budget constraints, and unfamiliarity with the litany of regulatory requirements and how to implement them can create an undue burden on SMBs and divest their already constrained resources from growing their businesses and innovating entrepreneurial opportunities to supporting business functions. These factors create a need for an alternative business model that can effectively respond to their security needs in a cost-effective manner. By catalyzing this approach, SMBs can take full advantage of the security expertise of an existing market, which can be broadly adopted and scaled to the varying business and information security needs. Whether NIST decides to adopt a managed security service model or develop an entirely different set of codes of conduct, in order to achieve a unified approach towards information security for the NII sector, it is essential that the codes developed for SMBs align and are interoperable with those of the sector at large.

We recommend optimizing the capabilities of established channels familiar to SMBs before launching a new initiative or process. Additionally, it is important to designate a single entity to facilitate and oversee this process to ensure adequate representation of, accountability to, the SMBs.

Interoperability to Ease Implementation

Developing, identifying and asserting conformance with standards and practices[5]

The standards proposed in the Green Paper are appropriate to consider as many of them are globally recognized, industry-led, voluntary, and consensus-based and have widespread adoption. Any effort to

[5] *The relevant questions from the Green Paper addressed in this response include: Are the standards, practices, and guidelines indicated in section III.A.2 and detailed in Appendix B of the Green Paper appropriate to consider as keystone efforts? Are there others not listed here that should be included?; What process should the Department of Commerce use to work with industry and other stakeholders to identify best practices, guidelines, and standards in the future?;How can the Department of Commerce or other government agencies encourage NII subsectors to build appropriate best practices? Is there a level of consensus today around all or any of these guidelines, practices, and standards as having the ability to improve security? If not, is it possible to achieve consensus? If so, how? In a fast changing/evolving security threat environment, how can security efforts be determined to be relevant and effective? What are the best means to review procedural improvements to security assurance and compliance for capability to pace with technological changes that impact the NII and other sectors?;What incentives are there to ensure that standards are robust? What incentives are there to ensure that best practices and standards, once adopted, are updated in the light of changing threats and new business models; What conformance-based assurance programs, in government or the private sector need to be harmonized; How important is the role of disclosure of security practices in protecting the I3S? Will it have a significant financial or operational impact?;Should an entity's customers, patients, clients, etc. receive information regarding the entity's compliance with certain standards and codes of conduct?;Would it be more appropriate for some types of companies within the NII be required to create security plans and disclose them to a government agency or to the public? If so, should such disclosure be limited to where NII services or functions impact certain areas of the covered critical infrastructure?*

identify new best practices, guidelines, and standards requires the active participation of industry and other relevant stakeholders.

Microsoft has concerns, however, with the Green Paper's proposal to develop a “nationally recognized approach to minimize vulnerabilities in the I3S” under the auspices of NIST. (See Cybersecurity Green Paper pp. 3-4, 11). We believe that development of industry codes of conduct should not be led by the government, and that standards development should, whenever possible, occur through international standards bodies given the global nature of the IT Sector.

The extent to which standards are effectively implemented also has a direct impact on the resulting security improvements. Leveraging well-recognized standards, such as the International Organization for Standardization Information Security Management Systems standards (ISO27000 series) facilitates implementation, but it is also equally important to have performance metrics that measure the effectiveness of specific practices in achieving their intended outcome and the impact of the overall practices in mitigating security risks. Metrics can be a concrete, quantitative, and objective means to determine the efficacy of guidelines, practices, and standards and further support the adoption of specific ones. In order for market forces to properly incentivize security improvements, it must be possible to effectively measure and understand which security efforts yield measurable results and at what cost. Again, this work could be accomplished through collaboration with industry-led consortia, with NIST playing a strong role as a participant, and if necessary, as a convener.

When working to identify the appropriate mechanism for conformance with voluntary codes of conduct, we encourage the Administration to, again, found its approach in the same graduated risk management framework outlined above, i.e., for higher risks, such as those facing CCI, the mechanisms to demonstrate compliance may be more rigorous, possibly including third party audits and, in extremely rare cases, perhaps government audit, but for conformance for voluntary codes of conduct, a self-attestation model should suffice. We similarly believe that the incentives for CCI must also be strongest as the requirements and costs would be higher, and used this concept in framing our recommendations when proposing incentives in the next section.

The Green Paper also asks about the concept of widely disclosing cyber security plans by NII companies on a voluntary basis. We understand the purpose of this proposal to be to allow interested parties, such as shareholders, to understand the preparedness of a given entity. To the extent that such disclosures are made on a truly voluntary basis, we believe the proposal to be worthwhile, recognizing that the public nature of the disclosure may take specific and detailed information out of the plans. As the Administration understands, publishing security plans detailing how CCI will be protected would jeopardize our national and economic security. Instead, the Administration proposes that covered entities must publish high-level summaries of their plans. While companies may wish to voluntarily publish an assessment against their frameworks as a market differentiator, we fear a mandate to do so would become a time consuming exercise that does not improve—and could substantially threaten—cyber security. Rather, we support companies and customers working together through normal business channels, including those designed to protect confidential information between companies, so that risks can be understood and assessed.

Similarly, we would be concerned about proposals that mirror the Administration's plan to require publicly traded companies to make a series of certifications regarding the development of a plan, evaluation by a third party, and the results of that evaluation. We are concerned that this approach confuses the policy goal of ensuring the protection of CCI or NII systems with the policy goal of protecting investors. Public companies work diligently on disclosures that present a balanced picture of the strategic and operational risks and opportunities companies face. Prescriptive disclosure can erode a company's ability to present this balanced picture based on its specific facts and circumstances

The importance of automation[6]

Improving the state-of-the-art of automated security depends first on defining what specific aspects of automated security need to be improved. For example, there are many types of security functions that can be, and indeed are, automated. These include anti-virus detection, malware detection and removal, configuration management, access control management, and anomaly detection. One automated detection area where the ecosystem could benefit from is increased research into robust zero-day detection. Like the security models mentioned below, signature-based attack detection is another technology that has endured the test of time. For many known and "one-off" attacks, signatures are a necessary part of protecting a machine or network. However, for new, previously unknown attacks, signature-based detection fails. Without a pre-existing signature, an attack cannot be stopped.

Signature-based detection is naturally reactive, and more proactive approaches to all types of attacks (from viruses and worms to spyware and botnets) are worthy of continued research and automation. Such work should cover a defense-in-depth strategy for detecting attacks as well as design principles to harden software binaries to be attack resistant. This work must be done to counter the disturbing trend of underground trade in zero-day exploits. Signature-based detection must be augmented with robust solutions for detecting and mitigating zero-day attacks to protect critical infrastructure and business assets alike.

Microsoft continues to make significant investments in security technologies which automatically protect software and users from attack. Three of these technologies include:

- Address Space Layout Randomization (ASLR) shuffles memory, leveraging the concept of moving target defense, to make it harder for exploit code to operate predictably
- Data Execution Prevention (DEP) leverages the concept of minimum required functionality, ensuring that data that should not be executed as code cannot be
- Enhanced Mitigation Experience Toolkit (EMET) is based on automating, allowing users to apply multiple advanced mitigations simultaneously and verify which are running

[6] *The relevant questions from the Green Paper addressed in this response include: How can automated security be improved? What areas of research and automation should be prioritized and why? What areas of research and automation should be prioritized and why? How can the Department of Commerce, working with its partners, better promote automated sharing of threat and related signature information with the NII? Are there other examples of automated security that should be promoted?*

The growing connectivity of systems, number of devices, and value of information that exists in and across government and private sector systems means that it is also critically important to improve the trustworthiness of connections and transactions to reduce risk. Greater automation of security and compliance will provide value, yet that value will only increase as we develop and adopt better ways to ensure that hardware, software and data can be trusted, and that those connecting to its networks are who they claim to be and can only do what they are authorized to do. Improving identity and authentication of these elements will empower better trust decisions and increase accountability. Microsoft supports the vision for a citizen-centric, privacy-enhanced identity ecosystem as articulated in the National Strategy for Trusted Identities in Cyberspace (NSTIC). We also strongly support the NSTIC program and the National Program Office at the Department in their work to realize this vision, which will provide a variety of choices for authenticating identity online while helping to enhance security and privacy.

Commerce could also help by encouraging the creation of a marketplace for managed security as described earlier in our response when discussing codes of conduct for SMBs. Once there is demand on a sufficient scale, companies can make a business out of securing infrastructure for SMBs that do not have the resources or expertise to do it themselves. The Department should consider focusing on those automated computing functions or processes present in almost every SMB in the United States (e.g., automated payment processing) as well as the places where Personally Identifiable Information and money come together, which are very attractive to attackers and where SMBs will be most compelled to act. If we are able to minimize the relatively easy attacks that do not require technically adept “bad guys,” through automated security services, it would decrease fraud, vastly improve the overall health of the ecosystem today, and the limited resources we do have can be targeted against the most skilled and determined hackers.

Given the limited resources of the federal government and the Department, we believe that the best use of resources, beyond the two described above, lies in driving fundamental basic research necessary to ensure global leadership in ICT security. Two important areas that Microsoft has consistently pointed out to be addressed include:

(1) Security Models: The security models still in use today include the Bell-LaPadula confidentiality model and the Biba data integrity model. Each of these models has its origins in the 1970s and was intended for systems in use at that time. The Clark-Wilson information integrity model is somewhat newer (mid 1980s) but has seen little real adoption. Modern distributed and cloud-based computing systems defy many of the assumptions underlying existing models of security. As the industry moves more toward a services-based software delivery paradigm, new thinking about robust, formal descriptions of confidentiality and integrity is needed to frame the design and analysis of modern secure systems. It is time for these models to be reconsidered and redeveloped so that they address the concerns of realistic systems.

(2) Security Usability: Usability and security are often at odds. Highly-secure systems are notorious for being hard to use and manage. Poorly designed interfaces lead to dangerous misconfiguration of important systems so that an otherwise secure system is put into an

insecure state. They can also lead to user actions that compromise the protection of highly sensitive information, and thus undermine the protections provided by systems that otherwise realize the vision for Tailored Trusted Spaces.

The analysis of properties of usable and secure systems is an interdisciplinary research problem that has the potential to decrease human error in configuring a secure system and providing guidance to users who must respond to error messages, maintain secure software settings, and manage the disposition of their sensitive information.

Commitment and Leadership as Incentives[7]

Companies that have functions, processes, systems, or assets that fall within a definition for the NII will naturally deliver the level of security demanded by the market. Socially responsible companies, such as Microsoft, will, in the interest of national security and public safety, offer somewhat greater levels of security than are specifically demanded by the market. Beyond those levels, shareholders would reasonably be expected to object.

It has become evident over time that the government believes that more should be done than the markets are demanding. There may be segments of the market---e.g., highly critical infrastructure in regulated sectors---where such gaps should be expected (i.e., the market doesn't provide for national security needs) and may need to be addressed through government oversight. Such an approach, however, would undoubtedly stifle the innovation that is the engine of growth for companies offering Internet-based and ecommerce products and services. The Green Paper, therefore, appropriately focuses on identifying existing market forces that can be leveraged to close any gaps identified between what the market is delivering and what the government deems necessary to protect public safety and national security. In order to ensure the effectiveness of this approach, we believe there are some specific actions Government shouldn't take, and others they should.

For example, Microsoft has concerns about the Green Paper's approach to developing incentives for adoption of and compliance with voluntary codes, standards, or practices through the use of increased liability or enforcement actions.   Specifically, we are concerned by the Department's reference to the enforcement action against BJ's Wholesale Club, Inc. because, unlike the other cases cited in this section of the Green Paper, the BJ's Wholesale Club matter did not involve a company that was alleged to have made a promise and then to have broken it. Rather, the case involved a involved an allegation by the

[7] *The relevant questions from the Green Paper addressed in this response include: Should the government play an active role in promoting these standards, practices, and guidelines? If so, in which areas should the government play more of a leading role? What should this role be? Should efforts be taken to better promote and/or support the adoption of these standards, practices, and guidelines? In what way should these standards, practices, and guidelines be promoted and through what mechanisms? What are the right incentives to gain adoption of best practices? What are the right incentives to ensure that the voluntary codes of conduct that develop from best practices are sufficiently robust? What are the right incentives to ensure that codes of conduct, once introduced, are updated promptly to address evolving threats and other changes in the security environment?; How can liability structures and insurance be used as incentives to protect the NII?; What other market tools are available to encourage cyber security best practices?; Should federal procurement play any role in creating incentives for the NII? If so, how? If not, why not?*

government that a company was so far out of the norm for widely accepted industry practices for security customer data that its actions could be treated as being unfair to consumers—and thereby subject the company to a civil law enforcement action—even absent any deceptive statement or a specific legal duty to employ certain security precautions. Without commenting upon the specific allegations leveled against BJ's Wholesale Club, Microsoft would be concerned with the notion that this approach could be used to enforce “voluntary” codes of conduct, standards, and industry practices against even companies that were not party to them.

On the other hand, there are a series of actions government can take to better leverage and catalyze existing market forces to enhance cyber security for NII, including leading by example through adopting codes of conduct and supporting standards internally and for procurement, facilitating information sharing, promoting codes of conduct and incentives internationally, helping to develop the business case for security, increasing education and awareness, and promoting research and development.

Lead by Example

The government can serve an important role by serving as an example for industry and by leveraging its own buying power and as an example for the industry. As the Green Paper notes, "[i]f the government wants private actors to develop and maintain codes of conduct that evolve more rapidly, it should lead by example."[8] There are two ways that the U.S. government can effectively demonstrate such leadership in addition to its efforts to support and facilitate the development of codes, standards, and practices through NIST's cooperation with industry-led consortia. If the government puts its significant weight behind the adoption of security standards that require widespread adoption, both through its own use of those standards (part 1) or through contractual demands imposed upon those seeking to sell to the government (part 2)—the markets will follow.

First, the government should lead in the adoption of international or globally accepted standards or generally accepted industry practices both in the systems that it owns and operates and those that are owned and operated on its behalf. The U.S. government may be able to best demonstrate the importance of a security standard or practice by using it. Such actions may do more to ensure greater adoption than would be possible through efforts to highlight individual companies—or even groups of companies—who have implemented them. Indeed, U.S. government leadership may be necessary to overcome economic disincentives to the adoption of standards that yield benefits to the network as a whole rather than primarily to the entity adopting the standard.[9]

[8] As the Green Paper notes, Microsoft and others raised this point in responses to the Department of Commerce's NOI. "Microsoft, for example, raised the need to develop metrics that help answer questions such as “What does it mean for a product to be secure? How can one judge a product’s security guarantees?” Microsoft Comment at 19-20. See also Microsoft Comment at 3 (discussing the need for “quality metrics” to improve design process and detect defects through sampling, rather than a “‘100% inspection’”).

[9] See Allan Friedman, Brookings Economic and Policy Frameworks for Cybersecurity Risks, July 21, 2011 at p. 10. “Even adding new security components can be difficult if it requires individual decisions. Many security innovations, such as DNSSEC, yield their benefits to the entire network. There is little incentive to be the early adopter, since network security products often do not improve overall security until other users adopt them. Indeed, products that are not subject to network externalities and offer benefits to the early adopters, such as SSH and IPsec, are more likely to succeed and diffuse quickly” (Ozment, Andy and Stuart Schechter, “Bootstrapping the Adoption of Internet Security Protocols,” in The Fifth Annual Workshop on the Economics of Information Security, Cambridge, UK, June 2006.).

The U.S. government can leverage its procurement power for products and services that have incorporated specific security standards. This would encourage providers to adopt cyber security codes, standards, and practices that have been identified as effective. As always, such efforts must be technology neutral so that they do not favor a particular solution or vendor to the exclusion of others that might satisfy the government's needs. In addition, such efforts must be undertaken in a manner that is transparent and that holistically manages risks while giving adequate consideration to other core governmental and societal values—cost, data portability, accessibility, and privacy.

Facilitate information sharing within CCI and NII[10]

One of the best ways to promote public private partnerships is through active participation, working to create trust, define clear goals, work on clearly defined challenges, and remain committed to the constructive and two-way nature of such engagements. We encourage the Department to participate more actively in the public private partnership defined under the NIPP, taking on a greater role in helping to create a marketplace environment those incentives private-sector improvements to cyber security.

As part of that engagement, the Department should work with DHS and the private sector to address the myriad of classic information sharing challenges hindering our collective progress, and, in particular, the lack of a compelling reason for sharing, (i.e., value proposition). In our experience, the majority of public private partnership efforts to date have focused on information sharing. While information sharing is important, it cannot be — as it has been to date — the end goal; rather, we must focus instead on sharing specific information in a timely manner with parties who are capable of acting on it.

Microsoft strongly supports creating a more effective model for operational collaboration to move us from the less effective partnerships of the past to a more dynamic, collaborative, and self-governing approach involving cyber security leaders from government, industry, and academia. Collaboration is more than information sharing and is more than coordination; collaboration involves stakeholders working together, jointly assessing operational risks, and developing and implementing mitigation strategies. We suggest that an effective collaboration framework for public private partnerships should include focused efforts to:

- Exchange technical data (at the unclassified level as much as possible), with rules and mechanisms that permit both sides to protect sensitive data;

[10] *The relevant questions from the Green Paper addressed in this response include: What role can the Department of Commerce play in promoting public private partnerships?; How can public private partnership be used to foster better incentives within the NII?; How can existing public private partnerships be improved?; What are the barriers to information sharing between the NII and government agencies with cyber security authorities and among NII entities? How can they be overcome?; Do current liability structures create a disincentive to participate in information sharing or other best practice efforts?*

- Create global situational awareness to understand the state of the computing ecosystem and events that may affect it;
- Analyze the risks (threats, vulnerabilities, and consequences) and develop mitigation strategies;
- When necessary and consistent with their respective roles, respond to threats; and
- Develop cyber threat and risk analytics as a shared discipline. For example, one could combine government and private-sector information and then use the private sector's expertise in analyzing large data sets in pseudonymous ways to get new insights into computer security without raising privacy concerns.

Microsoft's Security Intelligence Report surveys data from 117 countries and over 600 million computers worldwide and we recently completed a review of the countries that have had the lowest malware rates to find out what they are doing well, so that we can share that information with others. The countries with the lowest malware rates are: Austria, Finland, Germany and Japan and each country had a variety of reasons for its success in combating malware.[11] Overall, we found six reasons why those countries are more successful in the fight against malware:

1. *Working together* - a strong public private partnerships that enable proactive and response capabilities
2. *Active monitoring* - CERTs, ISPs and others that actively monitor for threats in the region can address emerging threats more effectively
3. *Speed matters* - an IT culture where system administrators respond rapidly to reports of system infections or abuse is helpful
4. *Strong techniques to mitigate infections* – enforcing policies and actively remediating threats via quarantining infected systems on networks in the region is effective
5. *Education is key* - Regional education campaigns and media attention that help improve the public's awareness of security issues can pay dividends
6. *Prevent piracy* - Low software piracy rates and widespread usage of Windows Update/Microsoft Update has helped keep infection rates relatively low

The goals we are working to achieve in the long term and the operational mission must be clear and articulated, the roles of government and industry must be well-defined, and all participants must demonstrate commitment and continuity to achieve success. The aim is to create a trusted and focused collaborative alliance among the government, academia, and the private sector that enables us to work together to improve the cyber security of CCI and NII.

Promote codes of conduct and incentives internationally[12]

[11] Strong broadband penetration helped deploy patches quickly (Austria); a view that acting quickly against threats is in the interest of both IT administrators and users (Finland); a large Computer Emergency Response Community (CERT) with strong partnerships (Germany); The "Cyber Clean Center" partnership between over 76 ISPs, 7 security vendors (including Microsoft), and government agencies help educate consumers and remove infections from their computers (Japan)

[12] *The relevant questions from the Green Paper addressed in this response include: How can the Department of Commerce work with other federal agencies to better cooperate, coordinate, and promote adoption and development of cyber security standards and policy*

The creation and ubiquitous adoption of internationally accepted cyber security standards and codes of conduct require collaboration. This collaboration should extend across the full range of international bodies including, but not limited to, organizations such as the International Telecommunications Union (ITU), Internet Engineering Task Force (IETF), Common Criteria Recognition Arrangement (CCRA), Internet Governance Forum (IGF), the International Standardization Organization (ISO), and the Internet Corporation for Assigned Names and Numbers (ICANN). The U.S. government has, in the past, demonstrated strong leadership – such as the NIST AES and SHA3 algorithm competitions and ongoing work within the IETF – and its continued full participation in and encouragement of open standardization processes will assist international acceptance of cyber security standards and practices. Successful collaboration extends beyond solely representing positions of the U.S. government or broad positions of U.S. companies. Instead, both industry and government need to work together to help raise awareness about the potential risks to the global market place for ICT and the long-term impact for all markets that enact opaque regimes to address security issues, such as hindering the free flow of information.

The initial steps towards achieving effective collaboration involves focusing advocacy and cooperation efforts on working with like-minded nations to define clearly articulated norms of nation-state behavior in cyberspace. Such efforts, for instance, could help to deter state support for cyber attacks or hold nation-states that support such efforts accountable for their actions. Successful collaboration on ICT standards also means that the U.S. government and its like-minded international partners should strive to pursue regular and open engagements (i.e., bilaterally, multilaterally, through technical dialogues, at an overarching political level, all of these or through other mechanisms) with countries that pursue different approaches with a view towards harmonizing positions to the extent possible. The U.S. government should seek to create mechanisms for exchange and harmonization of business norms to the extent practicable. The traditional bilateral engagements that are government to government are effective, but it would also be valuable to enhance or find new mechanisms that enable broader technical exchanges between and among governments and industry technology leaders.

To keep up with the advancing pace of cyber security, the U.S. government is exploring cyber security legislation, which includes discussions of different types of cooperative arrangements with the international community/countries of interest to promote a synchronized approach for managing cybercrime-related issues. Legislators should continue to meet with global organizations that retain expertise in the cyber landscape of the countries within which they conduct business, such as private-sector IT companies, international industry consortiums, governments, and academic and research institutions to inform the international components of U.S. cyber security policy and to provide meaningful contributions to the discussion taking place in the global arena. Additionally, the U.S. International Strategy for Cyberspace introduces country and culture neutral principles for international engagement of cyberspace norms and responsibilities. To advance these principles, the U.S. government can consider developing or revising recommendations issued from an existing advisory group or prior

internationally?; How should the U.S. government work internationally to advance codes of conduct in ways that are consistent with and/or influence and improve global norms and practices?

publications, such as the Comprehensive National Cybersecurity Initiative, U.S. International Strategy for Cyberspace, and other cyber security-related initiatives or proposals. These efforts can promote a constructive and collaborative process from the onset that serves global interests.

Help develop the business case for security[13]

Assessing returns on cyber security investment is a difficult undertaking. Data are not readily available, organizations are often reticent to release it, and where data is available it is often not comparable due to a multitude of company-specific factors. A better understanding of cyber security incidents and economic costs associated with these events can be gained by the Department through work with DHS and other agencies to improve the consistency of data collected about their cyber security incidents and their impact. Although gathering incident cost information is difficult, many information sharing mechanisms exist for exchanging operational data. New mechanisms are not needed, where necessary, existing roles and responsibilities need to be harmonized.

Building the nation's cyber economic model is not about determining money spent on security and adding up costs related to losses or disruptions are far from trivial. At a medium or large enterprise level, cost assessments are very complicated. Attempts to compare or normalize costs between different enterprises are difficult. For example, an enterprise considers a number of factors when determining where and how to allocate security investment costs. Accurately comparing security investments between different companies requires an understanding of several important (and sometimes intangible) factors that determine where investments are made. These include but are not limited to: (1) what processes and procedures does the enterprise have for information and cyber security; (2) to what degree are their operations and mission critical services built upon software and services that have security integrated into them; (3) what is the security governance process and response capabilities of the enterprise; (4) what is the level of executive awareness or involvement in security; and (5) what is the overall awareness of personnel regarding their respective roles in cyber security.

While it can be difficult to discern explicitly how each of the five factors above influence where an enterprise makes its security investments they are in many respects critical factors for quantifying cyber security. Public and private enterprises can sometimes estimate the money spent on technologies, tools, or services for related to security but this provides an inaccurate picture of the actual investment in security. For example, if enterprises absorb cyber security costs related to the processes, procedures, or specialized personnel into their business operational costs then the additive costs related to acquiring technology, tools, or services may appear disproportionately low. In order to better understand the impact of cyber incidents and the economic costs associated with those events, Microsoft recommends that the Department initiate two parallel activities:

[13] *The relevant questions from the Green Paper addressed in this response include: What is the best means to promote research on cost/benefit analyses for NII security? What information is needed to build better cost/benefit analysis? Are there any examples of new research on cost/benefit analyses of NII security? In particular, has any of this research significantly changed the understanding of Cybersecurity and Cybersecurity-related decision making?*

1. Encourage DHS to work with relevant agencies to improve the consistency of data collected about cyber security incidents and their impact.

2. Require the Department's Bureau of Economic Analysis to modernize its economic accounts to capture and report information about cyber security investment. New measures are needed to identify the trade in cyber security related goods and services. And similarly, to measure corporate capital, and operation costs of cyber security.

Increase awareness and education[14]

Microsoft supports a strong role for the Department, working in coordination with DHS, to lead cyber security awareness and education for all infrastructures – critical and non-critical – and all users – consumers, SMBs, enterprises and government. We believe that the National Initiative for Cybersecurity Education (NICE), being coordinated by Commerce via NIST, is a key effort underway that will help improve cyber security awareness for citizens and help build a more cyber savvy workforce. The release of the Draft NICE Strategic Plan for public comment demonstrates a willingness by the Department to engage the broad community of stakeholders involved to advance such an expansive challenge, and we look forward to collaborating to advance this initiative.

The Department should also continue working with DHS and the private sector to improve awareness by developing and executing on a number of "breakthrough implementations" of "Stop. Think. Connect." This unifying message was developed for the general public, but is not yet widespread or well-known. Pooling resources could result in innovative and broad-reach ways of calling attention to the message and drive traffic to available resources (e.g., in-flight and movie-theater showings of PSAs, etc.). The "Stop. Think. Connect." initiative is unique in its success for several reasons. It brought together decision-capable subject matter experts from dozens of public and private entities who are passionate about and dedicated to advancing the issue. "Coop-e-tition" was the order of the day, and companies put individual agendas aside for the benefit of the greater good. This model can be replicated for other efforts.

As part of that awareness campaign, we should not only promote about efforts to protect computing devices (i.e., PC, laptop, tablet, smart device, etc.), but also focus on personal online safety– instilling in individuals those habits and practices designed to combat social engineering and protect the person and his/her assets. Particularly when engaging with the K-12 demographic, we cannot ignore cyber bullying, risks associated with social networking and online reputation, exposure to inappropriate content, child identity theft, respect for intellectual property, etc.

We have also observed that while current cyber security funding programs focused on higher education are performing worthwhile actions, the fact remains that the output of these programs pale in relation

[14] *The relevant questions from the Green Paper addressed in this response include: What new or increased efforts should the Department of Commerce undertake to facilitate cyber security education? What are the specific areas on which education and research should focus? What is the best way to engage stakeholders in public/private partnerships that facilitate cyber security education and research?*

to the threat environment and are failing to address the root cause of the security problems in the IT space. Their efforts are largely palliative, not curative. Note that the U.S. is facing a problem of “scale” as well as “skill” – while graduating more Master’s- and PhD-level security professionals helps address the skill deficit, it does not address the scale of the present or future security threat.

The goal of U.S. government cyber security education programs should be to create “security-literate” graduates from both community college and vocational institutions, as well as traditional undergraduate programs in compute intensive disciplines (e.g. CS, EE, CE, IS, SE) to *address the scale problem*. At the same time, the U.S. government should increase opportunities for “security-focused” post-baccalaureate programs (i.e. doctorates) to *address the skills gap*.

To that end, the Department should fund a study to evaluate the core classes and content of the ACM/IEEE Computing Curricula for undergraduate education with the expressed purpose of:

- Identifying security and privacy conceptual gaps in the core computing curricula
- Creating platform agnostic content (exercises, instructor guides, tools, etc.) focused on the security and privacy elements of each *core* concept in the Computing Curricula.

Research performed in a variety of fields has shown that students learn better by constant exposure to a concept rather than a short duration of intensive study. Degree programs that only address security and privacy issues in the context of elective courses are missing a unique opportunity. In this scenario, *security literacy* at the baccalaureate level would be achieved by students receiving *consistent exposure* to IT security concepts throughout their educational career. Students graduating from these programs would not be experts; however, they would be reasonably well-versed in computer security and privacy topics and thus would carry that foundational knowledge onward in their careers as IT professionals. This would also increase the number of potential students seeking to pursue graduate studies in information security and privacy. Existing graduate study programs in information security (e.g. DHS/NSA Centers of Excellence) would address the skills need for expert, *security-focused* technologists and theoreticians.

University courses are created to address the learning outcomes specified in the Computing Curricula. Weaving a small number of specific security- and privacy-focused exercises into each course in the Computing Curricula core should not cause faculty to neglect core learning themes in favor of security, nor would it require them to become security experts. On the other hand, having students constantly exposed to security concepts throughout the educational core may have a better chance of influencing positive behaviors over the long haul–and if done correctly–could positively influence the number of students that choose to pursue security studies at the graduate level.

Promote cyber security R&D[15]

Cyber security research will in generally benefit CCI, NII, and even non-critical infrastructure as well, and it is important not to develop separate streams of funding and research communities. For example, the six key R&D topics in Trustworthy Systems and Cybersecurity outlined by the President's Council of Advisors on Science and Technology (PCAST) in their Dec. 2010 report[16] are: (1) advancing trustworthy system characterization; (2) understanding and improving the social dimensions of trustworthy systems and cyber security; (3) creating foundations for cyber security; (4) formulating the definition and application of security and privacy policies; (5) improving methods to detect and mitigate security attacks; and (6) developing methods for the implementation of a "survivable core" of essential cyber-infrastructure. All of these areas are quite relevant to CCI, NII, and other infrastructures. For example, trustworthy system characterization (#1) includes work on applying different standards of reliability and trustworthiness to different systems; an ability to tailor security and other processes to systems' specific levels of risk and threat is critical. Another important area within trustworthy system characterization (#1) is methods for assessing the trustworthiness of supply chains (valuable for small and medium sized businesses). Research on the social dimensions of trustworthy systems and cyber security (#2) will also extremely important for NII. Social science research and awareness of legal, social, and ethical implications should be a part of the NII research agenda, including on the economics of cyber security, such as costs and incentives; on the human factors associated with behavior in interacting with NII systems; and on attitudes around the relationships between security and other areas, such as usability, privacy, openness, and transparency.

The cloud is a new model for implementing information technology systems, and as such, will raise new questions about how best to develop, disseminate, and implement security approaches. For example, one of the differences between cloud and traditional IT implementations is who manages and controls security processes. Customers and cloud providers have to coordinate risks to ensure that a consistent security posture is maintained independent of who is responsible for the various layers of the system. In terms of research, many of the areas already being studied, such as encryption, usability, resilient architectures, network security, and co-tenancy, will continue to be relevant although the methods and challenges in a cloud environment may be different. Additionally, the relative priority of research areas may shift in light of the growing adoption of cloud services.

As can be seen from the list above and the recommendations outlined in other lists of research priorities,[17] there are many challenges in securing information systems, including NII, and there are deep

[15] *The relevant questions from the Green Paper addressed in this response include: What areas of research are most crucial for the I3S? In particular, what R&D efforts could be used to help the supply chain for I3S and for small and medium-sized businesses? What is needed to help inform I3S in the face of a particular cyber threat? Does the I3S need its own "fire department services" to help address particular problems, respond to threats and promote prevention or do enough such bodies already exist?; What role does the move to cloud-based services have on education and research efforts in the I3S?*

[16] PCAST's "Designing a Digital Future: Federally Funded Research and Development in Networking and Information Technology" - http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-nitrd-report-2010.pdf.

[17] "NITRD CSIA IWG: Cybersecurity Game-Change Research & Development Recommendations" - http://www.nitrd.gov/PUBS/CSIA_IWG_%20Cybersecurity_%20GameChange_RD_%20Recommendations_20100513.pdf ; National Research Council's "Toward a Safer and More Secure Cyberspace" - http://www.nap.edu/catalog.php?record_id=11925

and hard research problems that need to be tackled to ensure our defenders are not outstripped by our attackers. The NII will benefit most if the federal government focuses on supporting this long-term basic research, enabling a vibrant research community to form and share results broadly. The government and universities should also focus on supporting education programs that produce not only security practitioners, but also train future researchers. (This includes improving access to computer science education in K-12.)

Research conducted in industry will be vital in realizing the implementation of insights from basic research programs. The R&D tax credit is an important incentive, and it should be permanently extended and the alternative simplified credit rate should be increased from 14 percent to 20 percent.

The current federal support for cyber security research, development, and standards, including work at the Department, is very important and should continue. In building on these efforts (i.e. the work underway in the interagency Networking and Information Technology Research and Development program), the Department could play a role in facilitating the public-private collaboration and information sharing that can provide critical context for research, especially basic research at universities, in cyber security. This might include convening conferences and workshops designed to bring academic and industry researchers together. One area of potential value would be facilitating the development of model systems, datasets, and problems that accurately reflect key characteristics or vulnerabilities of real systems but could be disseminated broadly in unclassified settings for basic cyber security research.

Conclusion

Improving the overall cyber security posture of infrastructures – those critical for national security, public safety, and economic security, and those that fall outside of the Critical Infrastructure Key Resource – can yield a tremendous impact on the economic vitality of the Nation, and, in turn, for Nations around the world. The three themes – Innovation, Interoperability, and Incentives – espoused in our response form an important construct that considers the various roles, responsibilities, and interplay of private-sector infrastructure owners and operators, software and service providers, and government stakeholders; the dynamic nature of infrastructure risks and the interdependencies between CCI and NII; and the need for demonstrated government commitment and leadership. We believe that this construct provides framework for creating the appropriate balance between security and innovation.

The Department has an essential role in this framework to help create a marketplace environment that incentivizes private-sector improvements to cyber security. For example, the Department should continue to lead cyber security outreach and awareness for all infrastructures, should participate more actively in the public private partnership defined under the NIPP, and could encourage the creation of a marketplace for managed security services for SMBs. We also recognize NIST's key role as a convener and participant in existing global standards setting efforts. In developing our response to the Cybersecurity Green Paper, we identified a series of questions that require further exploration by both government and industry as efforts to formulate policy in this space continue. Microsoft looks forward to our continued engagement with the government as we thoughtfully craft and implement both the policy and risk management approaches to enhance the cyber security of infrastructures.

Submitted by:

J. Paul Nicholas

Senior Director, Global Security Strategy and Diplomacy

Trustworthy Computing

Microsoft Corporation

Redmond, WA

September 21, 2011