MICROSOFT RESPONSE TO THE DEPARTMENT OF COMMERCE NOTICE OF INQUIRY ON CYBERSECURITY, INNOVATION AND THE INFORMATION ECONOMY

Docket No.: 100721305-0305-01

Dated: September 20, 2010

Microsoft Corporation (Microsoft) files these comments in response to the Notice of Inquiry (NOI) issued 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 July 28, 2010.

Microsoft appreciates this opportunity to provide its comments on the eight topics set forth in the NOI, including, (1) Quantifying the Economic Impact; (2) Raising Awareness; (3) Web Site and Component Security; (4) Authentication/Identity (ID) Management; (5) Global Engagement; (6) Product Assurance; (7) Research and Development; and (8) An Incentives Framework for Evolving Cyber-Risk Options and Cybersecurity Best Practices. Each topic will be addressed more fully below.

INTRODUCTION

Microsoft's products, platforms and services are used by millions of customers around the world, in all walks of life, and to fulfill a wide range of commercial and personal activities and needs. As the Department and the Task Force look to better understand the challenges facing the future of the Internet and priorities around cyber-security, it is important that the focus remain on continuing to enhance and support an innovation economy.

Microsoft recognizes that technology skills are increasingly important to all kinds of jobs in all corners of the globe. For example, the U.S. Bureau of Labor Statistics estimates that 77 percent of American jobs will require technology skills within the next decade. A tech-savvy workforce is a critical component for economic growth. While Microsoft has a worldwide program to reach over reach over 20 million people globally per year through the Community Technology Skills Program, Commerce can and should continue to support policies that grows the skill set of the workforce and encourages innovation [1]

(1) Quantifying the Economic Impact

[1] "Workforce Development", http://www.microsoft.com/about/corporatecitizenship/en-us/our-commitments/goals/workforce-development.aspx, last visited September 9, 2010.

Recognizing the challenge of quantifying the scope of the losses that the economy and businesses face due to cyber incidents, the Internet Task Force (Task Force) sought input on the "availability of authoritative, aggregated data on cybersecurity investments and losses from cyber incidents might yield a quantitative picture of the economic impact of cyber intrusions and attacks."[2]

The innovation of information and communications technologies (ICT) has profoundly changed industrial age economic models and enabled new business models. Within a few short decades the majority of the world's enterprises have adopted and integrated ICT into core business operations and service delivery capabilities. The integration of ICT into virtually every aspect of modern economy and the shift the knowledge-based economy is sometimes referred to as the Information Age. This rapid integration and the resulting dependency on ICT presents a challenge to policy and decision makers who must make key investment decisions about their enterprises and how best to assure their missions while innovating to meet market realities. All too often these decisions are made with very little attention to the risks and benefits related to security of the ICT that is now critical to the modern enterprise.

The NOI asserts that:

> "The availability of authoritative, aggregated data on cybersecurity investments and losses from cyber incidents might yield a quantitative picture of the economic impact of cyber intrusions and attacks. Such data would enable industry and the government to evaluate the severity of cybersecurity threats and emerging trends and to make informed decisions about the trade-offs of different cybersecurity strategies and investment options."

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 cybersecurity; (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 cybersecurity.

[2] "Notice of Inquiry", Office of the Secretary, Department of Commerce, Federal Register, July 28, 2010 at 44219 (NOI).

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 cybersecurity. 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 cybersecurity 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. To date, it appears that it is only these additive costs that at the enterprise level or even within government agencies seem to yield meaningful data.

Understanding the financial impacts of cyber incidents is somewhat more straightforward. Incidents that disrupt services, expose confidential data, or destroy intellectual property, or damage the reputation of the enterprise are somewhat easier to calculate in terms understanding the damage. Organizations can measure the economic impact of failures in cybersecurity – whether applying patches to remediate security vulnerabilities or removing and recovering from malware infections. Similarly, while economic impact of losses of confidentiality (stolen intellectual property and the like) is somewhat harder, it is still feasible to calculate.

In the past the US Government has attempted a number of different types of voluntary gathering methods that have taken the form of surveys or discussions with the private sector to gather data. These have largely been ineffective for several reasons. First, there is a cost associated with reporting data related to investments or losses from incidents. The cost includes personnel time that has to be devoted to locating the data analyzing and it formatting it into a meaningful response. In some instances as noted above, there is no accurate way to compile investment data. Second, there can be considerable risk in sharing both investment and loss data related to cyber events.

In order to better understand the impact of cyber incidents and the economic costs associated with those events, Microsoft recommends that Commerce initiate parallel activities:

1. Work with the Department of Justice to better understand the economic impact of losses due to cyber crime and Internet-related fraud and identity theft.

2. Partner with DHS, in its role as Chair of the Government Coordinating Council, to work with relevant agencies to develop metrics to assess and report economic impact of cyber security incidents more consistently.

3. Require the Bureau of Economic Analysis (BEA) to better to capture and report information about cybersecurity investment. New measures are needed to identify the trade in cybersecurity related goods and services.

4. Work with DHS to assess economic losses and statistical analysis that can be gleaned from cyber incidents reported to DHS by the Federal agencies.

(2) Education, Awareness, and Information Sharing

Education, awareness and information sharing are central to improving cybersecurity in ICT products and services, and to the resiliency of the critical infrastructures that rely on them, and of business and individual consumers broadly. Information sharing has become a term of art and while it is infused throughout education and awareness, it also stands alone. In its broadest sense information sharing relates to the exchange of data between individuals or organizations with an agreed upon protocol for the way the shared data will be treated. Information sharing can happen at policy, operational, or technical levels, including between machines. Formal information sharing -- which defines the semantics and structure of the data items being passed around -- is inextricably linked to situational awareness.

Each domain, education and awareness, has a number of important, and, at times, challenging elements related to cybersecurity.

- **Education:** Cybersecurity education can be thought of in two main areas: (1) Academic Education -- including specific disciplines such as software engineering, computer science or management of information systems; specific skills training such as coding, systems administration, or configuration management; and (2) Industry Training -- industry training initiatives to increase security engineering skills. Each area is very different but both contribute to overall security of the cyber ecosystem.

- **Awareness:** that is, who needs to be appraised of what -- generally falls into two categories (1) general consumer cybersecurity awareness about the need for online safety and security, (2) awareness of decision/policy makers related to how cybersecurity impacts business and operational investments or incidents, often for the purpose of decision-making.

- **Information Sharing:** the mutual exchange of information regarding tactical or strategic incidents in an enterprise, sector, or at the national level.

<u>Academic Education -- Improving Security Curricula</u>

Fundamentally, the computer industry employs people skilled in two complementary but different disciplines, software and infrastructure. Information technology (IT) education has traditionally bifurcated into computer science and management information systems.

Cybersecurity skills required by each discipline and are not well addressed by their respective curricula.

Microsoft has repeatedly asserted the need to integrate security considerations into introductory computer science and programming classes. The goal is not to turn these classes into training,

but to ensure that everyone who learns to program is aware of the need to program securely. In addition to programming classes, Management Information System classes should also include security training applicable to IT system architecture and configuration, IT system security policy, defensive methods and their limitations, and methods for identity authentication, authorization and audit.

Changing college curricula is a slow process and the Department should work with the National Science Foundation and through NIST to engage universities to help foster the necessary changes. The Cyber Corps Scholarship for Service Program has been an effective model for enhancing cybersecurity education centers across the United States[3]. While it has not formally changed curricula, it has increased academic focus on cybersecurity and helped to bring a capable cadre of IT professionals into the government work force. More needs to be done to bring students into advanced computer science and computer engineering disciplines. The Department of Commerce should work with the relevant Federal Agencies, the private sector and Universities to increase scholarships and promote greater participation in computer science and engineering.

In addition, there is a fundamental shift happening in the field of management information systems brought on in part by the dramatic increases in reliance on ICT but also in part by integration of cloud services, speed of transactions, speed of attacks, and scale of operations. In addition to the speed at which cyber risks can change, the very targets at risk can shift. These changes have resulted in a quantum leap in demand for security risk management skills among IT information systems management professionals. Traditional IT risk management would have enterprises prioritize the protection of their most critical assets. However, the rise of sophisticated targeted attack on major enterprises (public and private) reveals that attackers do not always go after the most critical assets but they may target less important assets knowing that the assets will be less well protected and that attacks thus may evade detection. Changes in threat dynamics and tactics should be driving commensurate changes in risk management disciplines.

Furthermore, the emergent "identity ecosystem" (see the "Authentication / Identity Management" Section) creates demand for skills in credential management, authentication, and authorization.

The Task Force should recommend that the Department work with the National Science Foundation, relevant Federal Agencies, the private sector and Universities to:

- Increase software assurance content, and specifically security engineering content, in computer science curricula;

[3] "Federal Cyber Service: Scholarship For Service", https://www.sfs.opm.gov/ContactsPI.asp?p=st, last visited September 9, 2010.

- Increase information technology risk management content in management information systems curricula;
- Increase content about authentication and authorization models in both computer science and management information systems curricula; and Increase scholarships and promote greater participation in computer science and engineering.

Commerce can also continue to encourage the Department of Homeland Security to continue its focus on risk assessment and help broaden the scope of its analyses beyond critical infrastructures, to provide risk assessment criteria for non-critical infrastructures.

Industry Training -- Initiatives in Cybersecurity Training

As a result of the lack of security education in college level computer science and engineering curricula, individual companies and industry groups have been required to step in and ensure that their employees have basic awareness of the importance of security and the need for developers and other ICT professionals to ensure the security of systems and data.

Beyond providing awareness and a grounding in the fundamentals of security, employers are responsible for ensuring that their employees have the specific skills required to integrate security into their work. In our experience training applied in a work context is especially effective. Microsoft has designed in-house training to help developers better understand and apply core cybersecurity concepts including:

- The current threat environment and the corresponding importance of secure development practices
- Secure design principles
- Secure coding principles
- The most common errors that lead to security vulnerabilities
- Threat modeling
- How to find/test security related issues in code
- How to fix security issues

Other companies have also recognized the need for greater cybersecurity knowledge in the workforce. Microsoft is a founding member of the software Assurance Forum for Excellence in Code (SAFECode). 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.

SAFECode members found that the lack of formal education on secure software design, development and testing principles at the university level and the infancy of many corporate

software assurance programs have resulted in a shortage of software engineers who already possess the secure development skills desired by software vendors.[4] As a result, SAFECode members developed a framework that can be used by small, medium, and large enterprises to develop in-house corporate security training for software assurance. The SAFECode framework details the "what" and the "how" of well-known and deployed techniques to improve cybersecurity.[5] But an enterprise must also decide on how to prioritize their cybersecurity investments.

Another industry initiative, known as the "Building Security In Maturity Model" ("BSIMM")provides a starting point for considering what activities should be integrated into the development process.[6] The Department of Commerce should continue to encourage important private sector work, such as that of SAFECode and BSIMM, and work with the relevant Federal Agencies, private sector and Universities to increase awareness of these industry initiatives among small and medium businesses and the segments of the information technology sector which support them.

Awareness

The need to raise awareness about cyber security among different audiences requires the adoption of appropriate communication processes. General consumer cybersecurity awareness, about the need for online safety and security, and the awareness of decision/policy makers, related to how cybersecurity impacts business and operational investments, require "broad reach" communication methods.

Microsoft's online safety and privacy education site provides cybersecurity information for the general consumer.[7] This information is arranged using these that address consumer concerns:

- Protect Your Family: Minimize the risk of cyber-bullying, help kids use social networking sites more safely, and use parental controls in Microsoft products to help keep your family safer online.
- Protect Yourself: Create strong passwords, handle suspicious e-mail messages, download files more safely, and use anti-phishing technologies to keep yourself safer online.
- Protect Your Computer: Get information about security updates, products, and technologies to help protect your computer. Learn the 4 steps to computer security and more.

Microsoft has also served for a number of years on the National Cyber Security Alliance's Board of Directors, and has long-supported the "Stay Safe Online" initiative. Microsoft also supports

[4] "Software Assurance: An Overview of Current Industry Best Practices", http://www.safecode.org/publications.php , last visited September 9, 2010.
[5] http://www.safecode.org/publications/SAFECode_Training0409.pdf, last visited September 9, 2010.
[6] http://bsimm2.com/index.php, last visited September 9, 2010.
[7] Microsoft Online Safety http://www.microsoft.com/protect/, last visited September 9, 2010.

the Department of Homeland Security's National Cyber Security Awareness Month (NCSAM), which comes each October, and supports DHS's efforts to raise awareness regarding cyber security. The Task Force should recommend that the Department join in support of the NCSAM, and help amplify the efforts of DHS to reach the computing public around cyber security.

Information Sharing

Today there are sufficient information sharing mechanisms spanning the policy, operational and even some technical environments. But the myriad of groups and organizations involved in this space are not often used effectively for several reasons, all of which have been priorities of the Department of Homeland Security for some time. First, the government often does not provide data which the private sector can consume and use such as technical data to secure software and services, or unique analysis and telemetry. Second, the concept of "information sharing," especially at the national level, is nebulous in a commercial context and better suited to a specific incident, or to specific national security needs for which legal process already exists. Third, public private partnerships can be become too focused on plans rather than outcomes. Finally, there is often too much emphasis on "information sharing" rather than collaboration. If there is an effective collaboration framework for public private partnerships then operational information sharing about relevant events will be a natural and sustainable outcome. Improving collaboration and operational information sharing requires focused efforts to enhance:

- Exchange of technical data (at the unclassified level as much as possible), with rules and mechanisms that permit both sides to protect sensitive data. Microsoft encourages the Department to provide information in a format similar to that used by the Department of Veterans Affairs[8] and more aggregate information similar to that provided by the Government Accountability Office[9];

- Joint analysis of risks (threat, vulnerabilities, and consequences) and development of mitigation strategies; and

- Further innovation in threat reduction efforts to ensure the security of the broader ecosystem.[10]

The business community understands the mechanisms available for sharing operational cybersecurity information. The proliferation of these mechanisms presents its own challenges. It has been 10 years since 9/11 and 7 years since the National Strategy to Secure Cyberspace. Industry has seen the advent of the National Infrastructure Protection Plan, and the NIPP Risk

[8] VA-NSOC, http://www4.va.gov/ABOUT_VA/docs/MONTHLY_REPORT_APR2010.pdf, last visited September 9, 2010.
[9] GAO, http://www.gao.gov/new.items/d10536t.pdf, last visited September 9, 2010.
[10] Scott Charney, testimony before the U.S. House of Representatives, Committee on Homeland Security, "Securing America's Cyber Future: Simplify, Organize and Act," March 10, 2009, available at http://www.microsoft.com/presspass/exec/charney/031009testimony.mspx.

Assessment for each of the 17 critical infrastructures in the US. We have seen the growth of operational Information Sharing and Analysis Centers (ISACs) and the more policy-focused Sector Coordinating Councils working in conjunction with the Government Coordinating Councils. We have international CERT collaboration through FIRST, and an industry collaboration response group in ICASI. This is in addition to all of the capabilities that each company has on its own.

The Task Force can partner with the Department of Homeland Security to better understand information sharing and response models. The Task Force can also recommend that the Department become a model of information sharing and cyber security response, by providing greater access to its own network data, engaging in greater analysis of its own intrusions and mitigations, and leading by example amongst federal agencies about how to share information with other departments, and with the private sector.

(3) Web Site and Component Security

In the NOI, the Task Force asks specifically whether third party verification of websites or components could be effective in reducing the proliferation of malware, and how best to do so.[11] Malware and other malicious content do infect computers and other user access devices (e.g., smart phones) through Web sites the user visits. Also users can inadvertently be encouraged to access a malicious web site through "bad guy" techniques such as the poisoning of search engine results for popular queries.

The NOI proposes that web site and component security be improved through third party verification. Microsoft does not believe that third-party verification of web site and component security is, unto itself, effective in reducing malware and eliminating web-based threats. It should not come as a surprise to the Task Force that reducing threats to web sites is a challenge for everyone who uses the Internet, just as security is a challenge for all in the physical world. For consumers, it remains key that citizens use the most currently available technologies, deploy patches quickly, and keep anti-virus software current on all devices. Industry has made, and continues to make, investments in web site security. For example, Microsoft has a program applied to partners using our web space that requires certain controls and scans of a partner's web sites to check for vulnerabilities. Only when a partner has satisfied our requirements , is the partner allowed to go live. Other companies and the government can and should require quality controls and security checks of content available from their publicly-accessible domains. When considering the feasibility of a central program for scanning web-sites, some challenges are: (a) that the number and churn of sites will cause any scans or checks to become out-of-date very quickly; (b) whether a program for US web sites could be effective given the global reach of the Internet and its content.

[11] NOI at 44220.

Additionally, consideration needs to be given to the methods used to secure websites. There is an increasing number of malicious sites that mimic safe/secure sites. Methods used to secure web sites rely on public key encryption-based security certificates. These certificates are offered on a commercial basis by Certificate Authorities and are procured by website owners. A more rigorous method of associating certificates with the organizations that own the certificates and the websites that utilize them would provide a more reliable method for distinguishing good sites from malicious.

Microsoft recommends that Commerce initiate these parallel activities:

1. Partner with DHS to encourage the adoption by website owners and developers of proven software security engineering best practices, and to help DHS target small business and e-commerce sites to improve website security.

2. Work with the Department of Homeland Security and relevant agencies to understand whether a need for a more rigorous approach to certificate issuance exists within the US government.

(4) Authentication / Identity (ID) Management

The Task Force is continuing to examine the issue of whether more state of the art authentication or identity management technologies can make an appreciable difference in cyber events that impact consumers, and whether any current identity management systems help mitigate those risks to consumers.

Microsoft is a strong believer in the importance of balancing the privacy and security needs of customers to create a more effective authentication and identity management capability for Internet users, both consumers and enterprises alike. Steadily increasing numbers of users, devices, and online activity require improved mechanisms to ensure trust. Integral to ensuring trust, users will require trusted identities and the ability to maintain control of their personable identifiable information (PII).

To deliver the new level of trust demanded in the information society identity, privacy, and reputation must become assessable factors. To conduct some transactions, the parties involved will accept anonymity and for other sorts of transactions accountability will be mandatory.

Anonymity and accountability are widely believed to be diametrically opposed goals with privacy proponents on one end and accountability and security proponents on the other.

However, it is impossible to address some privacy questions using the identity and authorization technology in common use today. Today the commonly-used strong authentication credentials -- X.509 certificates -- are all-or-nothing affairs: if one wants to use a certificate to prove one's identity one is forced to reveal all of the certificate's content/information, even if only a small portion of the certificate's content is relevant to the access request being made.

But the anonymity versus accountability debate is in fact a fallacy. Breakthrough advances in cryptography, like U-Prove™ [12] technology, made in the past three decades enable computers to perform protocols that provide both strong security and privacy. These protocols have yet to be implemented into identity products and frameworks, however, and a much better job needs to be done to educate target markets on their existence and benefits.

Microsoft encourages the Department of Commerce to move quickly to accelerate the broad use of these technologies in government and commercial information systems.

Microsoft does not agree with those who advocate a "rip and replace" strategy in order to implement the new identity and authorization technologies. Microsoft advocates technology co-existence. In the short and medium term, the new technologies are best suited to address the anonymity and accountability challenges posed by citizens and the multitude of internet connected devices. In the long term these new technologies will slowly replace technologies used today by enterprises and web services.

Below we discuss how the existing infrastructure designed for enterprises and services must continue to evolve to meet the needs of enterprises and online services today. We follow this by considering what is necessary to establish privacy protecting, identity and authentication for the billions of citizens and devices now connecting to the Internet. And in conclusion, we consider improvements to better support these new and existing technologies, and provide a summary of our recommendations to the Department.

Establishment – Enterprises and Services

Microsoft continues to believe that existing identity and authentication technologies based on public-key cryptography are the best available for general enterprise and web-service use. These technologies are well-understood – for example the DoD Common Access Card (CAC) uses a version of these technologies – and provide adequate assurance when the proper cryptographic algorithms and key management techniques are used.

The NOI asks if new tools or technologies are emerging for identity or authentication. There are existing technologies are not static, advances continue to emerge from research and be incorporated in commercial products. There are recent advances in:

a. **Algorithms:** there is the shift to new algorithms for authentication and identity management. For these the Commerce should defer to NSA / DoD's on algorithm choices and mandate compliance with NSA's Suite B and any related NIST guidelines. This shift is already happening because of DoD requirements, their broad civilian use would be beneficial.

b. **Credentials:** the development of anonymous and pseudo-anonymous credentials ("limited revelation" credentials to use the Commerce terminology) have emerged. These offer

[12] http://www.microsoft.com/mscorp/twc/endtoendtrust/vision/uprove.aspx, last visited September 9, 2010.

tremendous opportunities in the proper contexts and scenarios, to have strong authentication while protecting the identities of citizens from unnecessary (and potentially dangerous) disclosures.

However, broad commercial adoption of these technologies needs to be accelerated. To encourage improvement in authentication / identity management controls, mechanisms, and supporting infrastructures the US Government should:

a. Require the use of authentication and identity management controls when interacting on-line with appropriate USG websites and services that require a suitable level of assurance – possibly starting with contractors to USG and for access to government websites. For example:

   Consider the broad use of strong (two-factor) identity / authentication credentials. This can be achieved by requiring the use of strong credentials for some government websites. Consider as an example EFTPS.gov, the Treasury Department's Electronic Federal Tax Payment System. EFTPS is essentially a banking website. It is used by millions of people and businesses to make income tax payments, including estimated tax and form 1040 payments, but the supported logon mechanisms are username + password + 4-digit PIN, and the PIN is sent in the mail. If the government is serious about raising the standard of cybersecurity protection and increasing awareness then it should start supporting the use of strong identity/authentication credentials on widely-used government websites that require individual authentication.

b. Encourage deployment of identity and authentication technologies in the private sector through the use of incentives and pilot programs. For example:

   Consider, what can be done to encourage US banks to issue credit cards using strong authentication mechanisms – similar to the existing European chip-and-pin system.

<u>Establishment – Citizens and Devices</u>

As introduced above, not all transactions require the same type or amount of identity data. For example a high value transaction will require more identity evidence than browsing a news site. Mechanisms are needed to allow the technical limitation of the information revealed to be only that information which is essential to a transaction. The ability to create these mechanisms has been enabled through innovations in digital technology over the last three decades.

Many identity systems will raise privacy concerns. However, the capability now exists to address many of the major privacy concerns with new technologies including anonymous credentials, revocable anonymous credentials, and pseudo-anonymous credentials. These technologies offer great possibilities for doing strong authentication on-line while revealing only the minimum set of attributes needed to complete the transaction.

Authentication and identity technologies have recently been addressed in the draft "National Strategy for Trusted Identities in Cyberspace Creating Options for Enhanced Online Security and Privacy" dated June 25, 2010.[13] Microsoft supports the approach described in this strategy. The strategy addresses the key challenges posed by online security; the need for privacy protection, voluntary participation, and the inter-operability (portability) of identity credentials and authentication systems. Of particular note in this context, the document also calls out the importance of supporting minimal disclosure.

In March of 2010, Microsoft released a community technology preview (CTP) of its U-Prove™ cryptographic technology.[14] We also made our patented crypto algorithms available under the Microsoft's Open Specification Promise (OSP).[15] Microsoft donated two reference Source Development Kits (SDKs) in source code (a C# and a Java version)[16] under a liberal free software license (BSD); our intention being to enable the broadest audience of commercial and open source software developers to implement the technology in any way they see fit.

The benefits of wide-scale adoption of limited revelation identity systems or anonymous credentialing include the ability for a user to limit disclosure of identity/authentication-related information to just that necessary to satisfy authorization policies. Limited disclosure reveals only what is necessary to prove compliance with an authorization policy. Widespread deployment of privacy-preserving technologies will help protect individual citizen identities on-line and deter the collection and profiling of information about consumer browsing habits by third-parties.

There is an urgent need to accelerate the adoption of these privacy-preserving technologies. The government can best promote market development of more effective authentication tools through appropriate standard-setting activities and by requiring the use of standards-compliant strong authentication mechanisms when engaging in procurement and access activities with the USG.

The US Government should also encourage implementation of privacy-preserving technologies in pilot applications.

Improvements required - Authorization

Similarly to identity and authentication technologies, authorization technology also faces challenges. Existing authorization technology is being overwhelmed by the rapid growth in the number of interconnected users, devices and applications. Authorization technology enables a

[13] http://www.dhs.gov/xlibrary/assets/ns_tic.pdf, last visited September 9, 2010.
[14] https://connect.microsoft.com/content/content.aspx?ContentID=12505&SiteID=642, last visited September 9, 2010.
[15] http://www.microsoft.com/mscorp/twc/endtoendtrust/vision/uprove.aspx, last visited September 9, 2010.
[16] http://code.msdn.microsoft.com/uprovesdkcsharp, http://code.msdn.microsoft.com/uprovesdkjava, last visited September 9, 2010.

computer to apply an "access policy" in order to limit the number of functions an authenticated user can perform. A user's access to a particular computer function can to be subject to multiple access policies. Each policy may be authored and maintained by a different policy authority and these policy authorities may be independent and in many situations subject to different legal jurisdictions.

Designers and implementers of access policy technology are now challenged by questions about how to express policies in an electronic form, how to compose policies from multiple policy authorities, and how to "test" composed policies for overlap and gaps.

First some context. Authentication and Authorization are separate concepts. Simply because an identity was authenticated does not mean that party (that identity) is authorized to perform a particular action. An authorization policy (also known as an access control policy) determines which actions an identity (a user or a device) is allowed (authorized) to perform. A best practice in security architecture is to separate decisions about identity and authentication from decisions about the actions an identity can perform (is authorized for).

A user's access to particular content can be subject to multiple access policies. Each policy may be required by a different policy authority, and these policy authorities may be independent and in many situations subject to different legal jurisdictions (e.g. UK and US). Existing authorization technology needs to advance to enable: (a) policy to be expressed in a machine readable form, (b) policy from multiple authorities to be composed, and (c) composed policies to be tested for overlap and gaps.

Policy description languages – for example logic based languages possess interesting and desirable properties for policy description applications -- are understood and research is now converging with standards. For example through future versions of XACML (eXtensible Access Control Markup Language).

The US Government must encourage research into authorization policy languages through appropriate basic research funding channels (e.g. NSF, DARPA). An example of a possible program is:

> Research into how ITAR (International Traffic in Arms Regulations) access policies can be expressed using an access policy description language. A user's access to particular content can be subject to multiple ITAR access policies. Each policy may be required by a different policy authority and these policy authorities may be independent and in many situations subject to different legal jurisdictions (e.g. UK and US).
>
> ITAR is an important body of polices used by multiple companies internationally, for example as represented by TSCP.[17] TSCP is an active industry effort to develop technology

[17] "Transglobal Secure Collaboration Program," http://www.tscp.org, last visited September 9, 2010.

for secure collaboration between multiple policy authorities located in different jurisdictions. These efforts will benefit from inter-agency encouragement to drive machine readable ITAR access policies.

Improvements Required – Minimum Disclosure "Stack" Protocols

The co-existence of existing and new identity and authentication technologies, as advocated above, is needed to accelerate the adoption and reap the benefits of these newer technologies. However, this co-existence also obscures a fundamental mismatch between the old and new protocols. Older protocols like TCP/IP run low in the protocol stack and do not support the capabilities provided by newer technologies like U-Prove™ that run at higher levels in the stack. Over time the mismatch between protocols at different levels in the stack must be resolved such that all necessary protocols provide both strong security and privacy.

The Department should support the review, research leading to possible redesign of all necessary protocols in the protocol stack so they support both strong security and privacy.

Improvements Required – Digital Credential Issuance

Different categories of transactions require the parties to the transaction to have to different levels of confidence. For financial transactions there needs to be, within the appropriate legal framework, "force of law" -- including criminal penalties, to back up the necessary credentials since identity credentials issued by third parties are elements of a commercial transaction and subject to contract law.

The question of which entities are authorized to issue digital authentication credentials will vary by country. Many countries will authorize multiple entities to issue authentication credentials. Organizations providing access to digital assets will accept the authentication credentials that meet their validation requirements. There are scenarios where government issued credentials for use with government provided services are also accepted by commercial organizations and the reverse – for example government may recognize authentication credentials issued by organizations it holds large contracts with. This model is used in other countries, often combined with Public Key Infrastructures. Sweden and Costa Rica are two such examples, where the banking industry is leveraged to attest to identity of individuals who then get government-issued Smart Cards.

In summary, Microsoft encourages the Department of Commerce to move rapidly but thoughtfully. The government should not set up programs that are independent or which compete with industry or the standards organizations that exist today. Any programs must be supportive of the progress being made by NIST, and by other USG Departments and agencies. More

specifically, Microsoft recommends that the Task Force encourage the Department to look for ways, directly or in partnership with other agencies, to:

- Require the use of authentication and identity management controls when interacting on-line with appropriate USG websites and services that require a suitable level of assurance.
- Establish standards for the issuance of digital authentication credentials that could be used with US government sites.
- Encourage deployment of identity and authentication technologies in the private sector through the use of incentives and pilot programs.
- Encourage the implementation of privacy-preserving technologies.
- Encourage research into authorization policy languages.
- Research the relationship between different protocol layers in the protocol stack and the goal of minimal disclosure and make recommendations to modify standards so that all necessary protocols support both strong security and privacy.
- Work with industry to identify the issues associated with issuing and managing Root Certificates on a national scale.

On balance, new programs would be helpful. Other countries are progressing, in some cases rapidly, to address access authentication and authorization questions. In one sense US industry and USG are "in the same boat" -- both are competing internationally.

(5) Global Engagement

In the NOI, the Task Force seeks comment on whether businesses are experiencing cybersecurity challenges in conducting business globally, and whether balkanization of the ICT market due to differing cybersecurity standards poses a real threat. Microsoft agrees that international security concerns, if not coordinated and managed, could impede competition and global markets.

ICT is essential to the economy and security of the modern nation state and to the regional and global markets in which they participate. Countries around the world are increasingly concerned about the security (confidentiality, integrity, and availability) of the software, services and hardware on which they rely for critical infrastructure, government services, defense and more. This concern is being manifest in the form of increased security standards, local intellectual property requirements, and new evaluation and certification methods.

<u>International security concerns can impede competition and hurt global markets</u>

The creation of many different requirements, different national standards, and evaluation methods hurts the global ICT vendor community. At first blush this may appear to advantage the

countries who are using these methods to slow the movement of foreign-developed technologies into their systems and services. However, this approach is very short-sighted and hurts the global innovation of ICT. As markets mature, the very requirements that are indeed to protect a given country may disadvantage it as it begins to export indigenous technologies to other markets and finds it must then comply.

At some level each country is likely to have an evaluation process or scheme much like any major enterprise does. These unique compliance requirements increase the cost of product delivery in those markets for vendors and also deny the country access to the latest technologies, including security innovations. Recognizing that there is likely to be some country specific evaluation requirements, each country's evaluation scheme and its results must be clearly understood by the global ICT community. Of greater concern than a country's unique evaluation regime is the transparency of that regime. The operation of an "opaque" evaluation scheme, rightly or wrongly, leaves open the possibility that the evaluation process does not treat all companies, domestic or international, equally.

Microsoft encourages Commerce and other relevant Agencies to work internationally to ensure that countries with specific evaluation requirements implement requirements that are technology agnostic, and employ evaluation processes that are transparent and which treat domestic and international vendors equally.

Collaboration is key to promoting internationally accepted cybersecurity standards and practices

The ubiquitous adoption of internationally accepted cybersecurity standards and practices requires collaboration. This collaboration should extend across the full range of international bodies including, but limited to, organizations such as the International Telecommunications Union, Internet Engineering Task Force (IETF), Common Criteria Recognition Arrangement (CCRA), Internet Governance Forum, and the International Standardization Organization (ISO).

Successful collaboration goes beyond just representing positions of the USG or broad positions of US companies. Instead, both industry and government need to work together to help raise awareness about the potential risks to global market place for ICT and the long-term impact for all markets that enact opaque regimes to address security issues. Another are where increased collaboration can ensure more transparent and congruent approaches to security is in Common Criteria. A more collaborative approach by the US Government in the international Common Criteria planning process would demonstrate leadership and minimize the possibility of the US merely becoming another participant. The US Government has, in the past, demonstrated strong leadership -- such as the NIST AES and SHA3 algorithm competitions and ongoing work within the IETF – its continued full participation in and encouragement of open standardization processes will assist international acceptance of cybersecurity standards and practices.

Successful collaboration on ICT standards also means that the USG and its international partners need to keep regular and open engagements with countries that deviate from international norms

(i.e., bilaterally, multilaterally, through technical dialogues, at an overarching political level, all of these or through other mechanisms). The USG should seek to create mechanisms for exchange and collaboration. The traditional bilateral engagements that are government to government often lead to slow moving policy exchanges. It would be valuable to find new mechanisms that enable technical exchanges between and among government and industry technology leaders. Microsoft encourages the US to exercise leadership by encouraging transparent measures to mitigate security risks such as outlining lawful intercept best practices that recognize privacy equities.

(6) Product Assurance

Product assurance is a global issue. Users and suppliers benefit if product assurance criteria and evaluation regimes are harmonized globally. Microsoft supports an internationally agreed product assurance evaluation process with mutual recognition that has explicit publically available assessment criteria. However, product assurance regimes need to evolve at a pace commensurate with the evolving cybersecurity landscape.

Several questions need to be considered as the product assurance regimes evolve:

- What are the assurance criteria and how are they established?
- How compatible are different assurance and evaluation regimes?
- What is the impact on products and on product lifecycles of the work required for assurance and evaluation?

Assurance criteria and how are they established

The Common Criteria (CC), the most broadly adopted product assurance criteria available today, has not kept pace with the evolution of threats to cybersecurity. It should be recognized that Common Criteria evaluation does not provide users with any assurance that a product will be resistant to attack. Evaluation at best assures users that a product incorporates the features specified in a government-prepared "protection profile" document. The US and other Common Criteria countries are seeking a more effective and realistic evaluation process. This is a move in the right direction.

To coordinate the evolution of their CC requirements and to assure that requirements are realistic and feasible, some other countries have initiated formal industry advisory boards for their Common Criteria schemes. US should emulate this practice in order to develop an effective industry-government dialogue that can clarify product assurance goals and challenges.

In our view it is quite possible for US Government and international product assurance guidelines to be crafted for software used in the "real-world". There have been several attempts at devising such guidelines, and much progress. The challenge today is completing the process and gaining international agreement on the guidelines developed. The Task Force can and

should recommend that NIST engage in the CC process to help promote greater awareness of the importance of expanding and updating Common Criteria, in order to help it expand into the next generation of software assurance needs.

(7) Research and Development

There are currently several government agencies and offices looking at the question posed by the Task Force: "How can the federal government best promote additional commercial and academic research and development in cybersecurity technology?"[18] It is Microsoft's view that the Department should leverage industry and academia by using its limited funds to finance research rather than development. The Department's funding should not be redundant to industry investments but instead should support basic, fundamental research on the hardest problems in security, some of which are highlighted more fully, below. If the resulting research is broadly disseminated, then competitive forces will ensure that the best solutions get commercialized and made available.

For the IT industry to advance toward the goal of a more secure internet, investments must be made in these areas:

- 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 were intended for systems in use at that time. Newer security models such as the Clark-Wilson information integrity model (mid 1980s) and role based access control (RBAC) work by NIST have emerged. However, commercial adoption of RBAC has lagged because the model remains poorly understood. [19] Moreover, modern distributed and cloud-based computing systems defy many of the assumptions underlying existing these older 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.

- Security Usability

  Usability and security are often at odds. Highly-secure systems are famous 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.

[18] NOI at 44222.
[19] "Building A Role-Based Access Control Model," http://www.forrester.com/rb/Research/building_role-based_access_control_model/q/id/34386/t/2, last visited September 9, 2010.

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 and maintain secure software settings.

- Robust Zero-Day Attack Detection

  Like the security models mentioned earlier, 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) is a worthy area for continued research. Such research 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.

To assure America's leadership in this space Government research investments are needed to drive fundamental advances for the entire IT industry. These advances will require innovations to deliver the next generation of a security lifecycle model, architecture and design, security metrics, and binary and code analysis.

To assure America's leadership innovations are required in order to deliver the next generation of a security lifecycle model, architecture and design, security metrics, and binary and code analysis.

Government research investments are needed to drive the necessary fundamental advances in:

- Architecture and Design

  Software architectures and designs that improve assurance would lead to more widespread secure development and reduce the risk of insecure deployment. Are there exemplar secure architectures for common software components? Are there design patterns for secure communication, authentication and data integrity?

  Recommended architectures and designs would lead to the development of secure reusable components and put secure development within the reach of a larger number of software developers.

It is important that this research focus on real world problems and scenarios, and cannot be focused on hypotheticals or questions on the margins of computing – this area is too important to ignore.

- Security Metrics

  Running commercial security analysis tools against production code is not research. Instead, research in security assurance should focus on the collection of data that will lead to meaningful measurements of system or software security. In short, we need a base set of measures that allow quantification of important aspects of security. What does it mean for a product to be secure? How can one judge a product's security guarantees?

  Once we understand the set of important metrics, we need to understand what data is required to evaluate those metrics. Data throughout all phases of the development lifecycle needs to be cataloged, assessed and used to provide metrics to guide the decision making process, including day-to-day development guidance and release readiness measures.

- Source-Level and Binary-Level Analysis

  The current state of binary, source code and source-code-equivalent (e.g., scripts) analysis allows reasoning about a small subset of security issues. Well understood problems like buffer overflows enjoy excellent support but other problems are outside the scope of current tools and theory.

  An order of magnitude improvement in our capability to analyze source and binary code for potential design defects should be the goal. A better understanding of patterns of insecurity and how those patterns can be found in code and binaries is important.

  Further research should focus on detection of malicious code embedded in a binary or of unauthorized modification of a binary, which would be useful to address questions of code integrity and pedigree.

The NOI questions the effectiveness of using a federal government-sponsored "grand challenge program" to draw attention to and promote work on specific technical problems. Microsoft prefers an alternative approach to "grand challenges". Government should sponsor academic engagements in security research that address specific hard problems which are proposed by industry and academics, and selected by peer review. The projects resulting from these problems would then be scheduled and managed by expert program managers.

(8) An Incentives Framework for Evolving Cyber-Risk Options and Cybersecurity Best Practices

The incentives question is a long-standing issue in cyber security policy debates. For years, companies and trade associations across all sectors have had differing views on whether

incentives are needed, and what form those incentives should take. In fact, the question is a bit of a distraction, because if a company, or even an individual, feels impacted by security, he or she will take action to increase security. Incentives are not needed to induce consumers and businesses to purchase alarms for their homes or businesses – it is done out of need, and an assessment of risk.

The more important question raised by the NOI is whether the best practices and risk assessment criteria and methodologies can be adopted and scaled to businesses and users outside the critical infrastructure arena. In Microsoft's view, the answer is a resounding yes. The National Infrastructure Protection Plan sets forth a framework for assessing risk that had been applied across all critical infrastructures, and is well known today. The Task Force should recommend that Commerce partner with the Department of Homeland Security and the Sector Coordinating Counsels to create risk assessments for the private sector, and with input from each Sector Coordinating Counsel, make more specific recommendations for small and medium size businesses in each sector generally. Commerce can make that same request of DHS and the Sector Coordinating Counsels for assistance in simplifying some of the myriad best practices for critical infrastructures for use by commercial enterprises broadly. In addition, Commerce can work with DHS on the Voluntary Private Sector Preparedness Accreditation and Certification Program to help raise general business capabilities around preparedness, disaster management, emergency management, and business continuity, in all of which cyber security plays a role.[20]

CONCLUSION

Microsoft appreciates this opportunity to provide its comments in response to this Notice of Inquiry issued 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.

In conclusion Microsoft commends the Department of Commerce in convening the Internet Policy Task Force to study these very important issues regarding cybersecurity, innovation and the information economy.

Microsoft encourages the Department to:

- Partner with relevant agencies to better quantify the economic impact of cybercrime and cyber security threats by utilizing the Department's own experiences;
- Support the Department of Homeland Security by promoting greater awareness with industry regarding cyber security threats and mitigations;

[20] "Voluntary Private Sector Preparedness Accreditation and Certification Program," http://www.fema.gov/media/fact_sheets/vpsp.shtm, last visited September 16, 2010.

- Help drive the rapid adoption of emerging, innovative identity, authentication and authorization technologies;
- Encourage collaboration domestically, and internationally on global engagement and product assurance challenges;
- Drive research and development into hard cyber security problems that will enable subsequent waves of innovative products and services.

Submitted by:

Microsoft Corporation
Redmond, WA
September 20, 2010