

Written Testimony of
Scott Charney
Corporate Vice President, Trustworthy Computing, Microsoft Corporation
Implementing New Models for Information Age Security

Before the
House Committee on Science and Technology
Subcommittee on Technology and Innovation
Hearing on “Assessing Cybersecurity Activities at NIST and DHS”

June 25, 2009

Chairman Wu, Ranking Member Smith, and Members of the Subcommittee, thank you for the opportunity to appear today at this important hearing on cybersecurity and for entering my written testimony into the Record of this Committee. My name is Scott Charney, and I am the Corporate Vice President for Trustworthy Computing at Microsoft. I also served as one of four Co-Chairs of the Center for Strategic and International Studies (CSIS) Commission on Cybersecurity for the 44th Presidency. Prior to joining Microsoft, I was Chief of the Computer Crime and Intellectual Property Section in the Criminal Division of the United States (U.S.) Department of Justice. I was involved in nearly every major hacker prosecution in the U.S. from 1991 to 1999; worked on legislative initiatives, such as the National Information Infrastructure Protection Act that was enacted in 1996; and chaired the G8 Subgroup on High Tech Crime from its inception in 1996 until I left government service in 1999.

Today I will share a brief assessment of cyberspace security and discuss:

- 1) Establishing Information Age security strategies for government;
- 2) Advancing Federal civilian enterprise security; and
- 3) Clarifying roles and enhancing capabilities for the Department of Homeland Security (DHS) and the National Institute of Standards and Technology (NIST).

Cyberspace Security: Understanding the Evolving Threats

We are locked in an escalating and sometimes hidden conflict in cyberspace. The battle of bits and bytes has very real consequences for America, other nations, the private sector, and all other Internet users. Cyber attack joins terrorism and weapons of mass destruction as one of the new, asymmetric threats that puts the U.S. and other governments at risk. Cybersecurity has improved, but these improvements have not kept pace with the increasing availability and value of data, nor the number or sophistication of cyber attacks. 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. Such data, particularly when not well secured, presents an attractive target for those seeking competitive or strategic advantage, or financial gain.

The resulting cybercrime economy is complex, sophisticated, and growing. It has numerous participants, some willing (malware developers) and some unwilling (victims of cyber attacks); some clearly good (security researchers that disclose vulnerabilities responsibly) and some clearly bad (vulnerability traffickers). Over the past decade, attacks that bad actors carry out have also grown in sophistication, expanding from opportunistic viruses and worms that were disruptive and sometimes damaging to very targeted, stealthy, and persistent attacks. In today's evolving cybercrime economy, any individual can engage in activities formerly limited to nation-states, and any nation, regardless of traditional measures of sophistication, can gain economic and military advantage through cyber programs.

When self-replicating computer worms entered the public consciousness several years ago, it was in the form of malware, such as Win32/MSBlast, Win32/Sasser, and Win32/Slammer, that exploited vulnerabilities to spread rapidly and caused system disruption or failure. These threats were highly visible and garnered significant attention. Exploit-based worms, while still a concern, have receded from prominence as Microsoft and other software vendors have reduced the vulnerabilities these worms relied on to spread, and users deployed security technologies meant to thwart these attacks. With the traditional vectors of mass propagation reduced significantly, today's prominent worms rely much more on social engineering techniques to gain

access to information technology (IT) environments, like enterprise networks and consumer machines. A gap in the application and oversight of enterprise-wide and consumer security controls, as well as insufficient monitoring and analysis of the real-time health of networks, can create significant risk both nationally and globally.

Today Microsoft tracks more than 30,000 types of malware families and some of these families have millions of variants. There are infections by these variants in machines around the world, but linking an infected machine with the cyber attacker who infected it is very difficult. The lack of identity for hardware, software, data, and people on the Internet makes it difficult to determine the source of attacks, yet knowing the source is essential to ensuring the appropriateness of response. Attribution of cyber attacks is one of the most fundamental challenges facing the international community. Absent strong attribution abilities, international and national strategies to deter cyber attacks will not succeed.

Microsoft has long recognized the growing need to improve software security to counter cyber threats. In 2002, Microsoft changed the way it built software by implementing the Security Development Lifecycle (SDL). The SDL provides customers with high quality, well-engineered and rigorously tested software that helps withstand malicious attacks by requiring threat models to be built at design time and requiring that specific security milestones be met at each stage of the development process. Every Internet-facing or enterprise-class product from Microsoft is required to go through the SDL, resulting in measurable improvements in the security and privacy of Microsoft's software. We also continue to work with partners in the computing ecosystem to help better protect our mutual customers and all Internet users. For example, we are members of the Software Assurance Forum for Excellence in Code (SAFECode)¹ which promotes the advancement of demonstrably effective software assurance methods. These efforts are essential in reducing the attack surface of products. Technology alone, however, will not create the trust necessary to realize the full potential of the Internet. Technological innovation must be aligned with social, political, economic and IT forces to enable change. Working with partners in the ecosystem, Microsoft is advancing End-to-End Trust,² driving and shaping these forces to create a safer, more trusted Internet.

¹ www.safecode.org; members include EMC, Juniper, Microsoft Nokia, SAP, and Symantec.

² www.microsoft.com/endtoendtrust

What can government do to counter this underground cybercrime economy? First, understanding the nature of cyber threats is critical. Breaking down the complexity of the cyber threat is necessary to inform the useful allocation of resources for defense and to guide more effective risk management. Our defenses must consider the diversity of players, motivations, and methods in the cybercrime economy, and must either raise the costs for adversaries to carry out attacks or decrease the value of successful attacks. Lowering the return on investment for cyber attacks can deter some bad actors or lessen the consequences of attacks that do occur.

Establishing Information Age Security Strategies for Government

Government must balance dual, and often interrelated, roles to effectively manage emerging cyber threats. First, as a public policy entity, the government is responsible for protecting public safety, as well as economic and national security. In this capacity, the United States must develop a national cyberspace strategy to address the full spectrum of significant risks presented by the Information Age. But the Federal government is also a large and widely distributed enterprise, with countless globally distributed “customers” (e.g., citizens who want to connect with their government), partners, operations, networks, and resources. Although distinct, the policy and enterprise roles are not entirely separate, as each affects and informs the other.

Architecting a Comprehensive and Coordinated National Strategy

The recently released White House *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* outlined key policy challenges the Nation faces as a result of the dynamic cyber threat landscape.³ The White House review recognized that:

The Federal government is not organized to address this growing problem effectively now or in the future. Responsibilities for cybersecurity are distributed across a wide array of federal departments and agencies, many with overlapping authorities, and none with sufficient decision authority to direct actions that deal with often conflicting issues in a consistent way. The government needs to integrate competing interests to derive a

³ http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

holistic vision and plan to address the cybersecurity related issues confronting the United States. The Nation needs to develop the policies, processes, people, and technology required to mitigate cybersecurity-related risks.

I support the near-term action plan in the review, which includes activities to appoint a lead policy official in the White House, staff a National Security Council Directorate, and prepare an updated national strategy to secure information and communications infrastructure.

This is a significant undertaking that will require continued White House and Congressional leadership. National security strategies create a framework to employ all elements of national power — economic, diplomatic, law enforcement, military, and intelligence. A comprehensive cyberspace security strategy must include these elements and articulate how they will be employed to ensure national security, economic security, and public safety, and to assure delivery of critical services to the American public. In the Industrial Age, power was generally based on physical might; in the Information Age, power is derived from information, knowledge, and communications.

Constructing An Information Age Security Model

Just as we need a new national strategy to ensure the nation's cybersecurity, the government must also carefully determine an effective model for managing government-wide cybersecurity. In this regard, one can view the Federal government as a large collection of businesses with different missions, partners, customers, data, assets, and risks. There are some responsibilities and practices (e.g., developing information security plans, implementing the Federal Desktop Core Configuration (FDCC)) that should be done by each and every Federal agency. The number and diversity of component organizations, functions, and systems, however, means that a fully centralized model for managing security will not work. Each agency has a unique security paradigm with differing threats, so each agency needs to manage its own risk.

If some security controls should be applied uniformly across the government, but other security controls need to be carefully tailored to address an agency's mission and risks, it becomes clear that the government needs to establish a hybrid model for information security that improves

security across the Federal enterprise and fosters agility to counter ever-changing threats. A hybrid model could create a holistic security framework for managing and reducing the attack surface of the Federal enterprise. Such a model would include:

- A centrally managed *horizontal security function* to provide a foundation of government-wide policy, standards, and oversight; as well as
- *Vertical security functions* resident in individual agencies to manage their risks.

This combination of horizontal and vertical functions ensures that minimum security goals and standards are set, yet provides agencies the flexibility to manage risks appropriately for their unique operating environments.

Advancing Federal Civilian Enterprise Security

For more than 25 years, the Federal government has been struggling to evolve its policy, organizational, and operational information security management frameworks. Over two decades, legislation has been passed that has incrementally established and enhanced authority, organization, and accountability. The three most important elements of the foundation include: the *Paperwork Reduction Act of 1980*,⁴ which centralized government-wide responsibilities into the Office of Management and Budget (OMB); the *Clinger-Cohen Act*,⁵ which established dedicated Chief Information Officers for the major departments and agencies across the government; and the *Federal Information Security Management Act (FISMA)*,⁶ which created the first comprehensive information security framework for the Federal government. Additionally, OMB mandated implementation of the FDCC by February 2008. The FDCC mandate requires Federal agencies to standardize desktop configurations to meet FDCC requirements and is intended to improve security, reduce costs, and decrease application-compatibility issues. This was an attempt to create government-wide policy and standards, but it lacked the oversight and supporting capabilities to be implemented effectively.

⁴ P.L. 96-511, December 11, 1980.

⁵ P.L. 104-106, February 10, 1996. The law, initially entitled the Information Technology Management Reform Act (ITMRA), as subsequently renamed the Clinger-Cohen Act in P.L.104-208, September 30, 1996.

⁶ P.L. 107-347, December 17, 2002.

Understanding what exists and conducting periodic tests of controls does not create the strategic and operational information security commensurate with the sophisticated Information Age threats that now confront agencies. Congress should consider how to implement an effective model for managing the security of the Federal enterprise, build enhanced cybersecurity capabilities within the government, and fund agencies appropriately to fulfill their vertical and, in some cases, horizontal responsibilities. There are two basic options I see: coordinated incremental change or comprehensive reform. Incremental change may be more appealing to agencies and the under-resourced individuals responsible for cybersecurity, but slow change may be inadequate and ineffective to counter evolving threats. Comprehensive reform, however, will substantially challenge the status quo. Such reform would require a sustained commitment of the Executive and Legislative branches to construct an innovative and agile Federal enterprise for the Information Age.

Defining Clear Roles for DHS and NIST

The hybrid model I outlined above could be applied more effectively to the Federal enterprise to improve security and increase agility. In this implementation, DHS and NIST would provide the horizontal function, and individual agencies would have vertical functions:

- *Horizontal Functions:*
 - *Department of Homeland Security:* DHS should set security control policy, articulating cybersecurity goals and outcomes. Put another way, DHS should develop “minimum baselines for security” and work with the standards community where appropriate. DHS should also develop processes to exchange and foster implementation of best practices that exceed minimum standards so that agencies can more quickly achieve higher levels of security when necessary to address their own unique agency risks.
 - *National Institute of Standards and Technology:* NIST should create government-wide standards to help agencies meet the security control policy set by DHS. NIST’s Special Publication (SP) 800-53, *Recommended Security Controls for*

*Federal Information Systems*⁷ is an example of standards created by NIST that apply government-wide. NIST should, like DHS, also help agencies exceed any government-wide minimum standards.

- *Vertical Function in Individual Agencies:* Agencies should continue to have responsibility for – and accountability for – assessing their risks and implementing effective management controls. This includes activities to configure and patch systems, build effective incident response capabilities, identify and detect unauthorized access, test security controls regularly, audit for compliance, and implement security changes based upon testing, auditing, and environment changes. Agencies’ risk management should be a continuous cycle of related activities performed as part of a documented information security program.

Clarifying Roles and Enhancing Capabilities for DHS and NIST

To fulfill the horizontal function described above, DHS and NIST need to have clear roles and enhanced capabilities. I will briefly describe some of the successes of and challenges to each of these organizations, and then focus my remarks on how to enhance their capabilities and funding so they may successfully provide the horizontal security function for the Federal enterprise.

DHS

DHS is in a state of transition, with changes in vision and leadership underway, so an assessment of its efforts must separate the past from the future.

DHS has partnered well with industry in the IT and Communications Sectors for infrastructure protection and that partnership is producing results. The partnership has advanced both strategic risk management and operational information sharing. For example, industry and government will be releasing shortly the IT Sector Risk Assessment called for in the National Infrastructure Protection Plan. The Risk Assessment outlines several mitigations (e.g., robust coordinated

⁷ Federal Information Processing Standards (FIPS), including “*Standards for Security Categorization of Federal Information and Information Systems*” and “*Minimum Security Requirements for Federal Information and Information Systems*” also provide guidance.

response and out-of-band data delivery) that public and private sector owners and operators can implement to better manage sector-wide risk. DHS is also improving how it facilitates distribution of actionable information (via Critical Infrastructure Information Notices and Federal Information Notices), which enables more timely implementation of security updates and helps to reduce malware infections such as the Conficker worm. This partnership is essential because cybersecurity is a shared challenge that involves government as well as the owners, operators, and vendors that make cyberspace possible. To date, this partnership does not yet fully extend into the cybersecurity research and development (R&D) portfolio managed by the DHS Science and Technology Directorate. This gap must be addressed to provide greater awareness of and, where possible, coordination across public and private sector R&D activities.

But DHS has struggled without an actual strategic plan for cybersecurity. As a result, its efforts have not always focused on the right areas and were not optimized for effectiveness. The lack of a cohesive vision was exacerbated by constant changes in leadership, lack of personnel, and inadequate funding for its mission. The Comprehensive National Cybersecurity Initiative (CNCI) was an important catalyst to drive improvements in DHS. It outlined specific initiatives in key areas, provided greater funding, and enabled more rapid increases in staff. The CNCI, however, still did not provide the coordinated vision that is needed. Moving forward, DHS should develop a strategic vision and look to build on its strengths in partnership, information sharing, and growing security capabilities to function in the horizontal role I outlined above.

NIST

NIST has also contributed significantly to advancements in cybersecurity, and must continue to do so in the future. The Information Technology Laboratory is an important voice in the cybersecurity conversation, and its Computer Security Division is doing valuable work, such as creating NIST's cyber guidance and hosting the Information Security Automation Program to automate technical security operations. The Computer Security Division, unfortunately, is not sufficiently resourced to address the growth in its responsibilities and workload.

This growth is proportionate with the continuing pace of technological innovation. For example, NIST is advancing two important initiatives for newer technologies and services that will each

have considerable cybersecurity implications: Securing the SmartGrid and Cloud Computing. In particular, NIST's cloud computing work is focused on the effective and secure use of cloud computing in the government and private sector. As NIST continues to explore cloud computing and cloud security, I would suggest it focus on three areas:

- Utilize a risk-based information security program that assesses and prioritizes security and operational threats;
- Promote regular maintenance and update of security controls that mitigate risk; and
- Support international standards frameworks and certifications that ensure controls are designed appropriately and are operating effectively.

The Computer Security Division should continue to focus on standards, and its resources should be increased to meet those expanding responsibilities. NIST's cybersecurity efforts will also continue to grow and benefit from increasing the partnership with the private sector, and more specifically, the IT and Communications Sectors. With greater resources, NIST will make a more dramatic impact on the cybersecurity of the computing ecosystem.

Enhanced Capabilities

DHS and NIST both must build on their successes, overcome challenges, and expand their capabilities to support government-wide policy, standards, and oversight of cybersecurity. I will outline five core capabilities that I believe should exist as part of a government-wide horizontal function for the Federal enterprise. These capabilities must be operationalized in the agencies to meet basic security requirements; however, my discussion below focuses on the government-wide horizontal function provided by NIST and DHS and the enhanced value created by analyzing data across the government infrastructure. NIST should provide the standards to enable these capabilities, and DHS should provide the operational aspect of each.

The growing connectivity of systems, number of devices, and value of information that exists in the Federal enterprise means that it is critically important to improve the trustworthiness of connections and transactions to reduce risk. The five capabilities outlined below will provide

value in the near-term, but that value will only increase as the Federal enterprise develops 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 in the Federal enterprise will empower better trust decisions and increase accountability.

Security Monitoring: Watching the real-time health of the networks involves more than traditional network monitoring. In addition to security data from intrusion detection systems, the government could also use information provided by IT assets, such as routers, hosts, and proxy servers, to evaluate its operational and security status. By taking advantage of the general purpose sensors that are built into every well-managed infrastructure, government can gain greater insight on the real-time health of the networks and take action to mitigate risks and respond to incidents.

Audit: Meaningful audit data can improve agencies' cybersecurity posture because audit drives behavior, and it provides accountability. The audit capabilities I am referring to are more than comprehensive yearly reporting; they include continuous audit, with spot checks and periodic evaluations, as well as quarterly and annual reporting. Quarterly or annual reporting provides a snapshot of overall security posture and trends, while the spot and periodic evaluations can be used to assess the adequacy of controls and compliance to defined requirements.

Advanced Analytics: The large amounts of monitoring and audit data must ultimately be turned into insights that can be used to inform more effective cybersecurity responses. That response may be operational as discussed below, or it may be more strategic and involve changes in policies, controls, and oversight. It may also be a combination of both, with operational incidents informing longer-term decisions. Either way, for this to happen, government must have the right data, must analyze that data in the context of the Federal enterprise, and that data must drive action. Fusing together disparate data from a variety of organizations and systems to create a common operational picture is challenging; building the analytic capabilities (e.g., correlation) to derive valuable insights is even harder. The monitoring and audit capabilities I mentioned earlier would create a baseline of data about the real-time health and overall trends in security across

the Federal government. DHS can combine this with threat information from the Intelligence Community and advanced technical analyses to create an operational awareness of the attack surface of the Federal government in ways simply not possible in the private sector. This is the power of innovative government analytics – insights gained from this fusion not only inform horizontal response, but also transition back to the vertical functions resident in the departments and agencies to manage steady state risks. It can even aid the private sector if the government is willing to share the analysis.

Agile Response: Building Information Age security in the Federal enterprise will make it a better partner with the private sector for improving operational security. Over the past 10 years, there have been several attempts to improve operational coordination between and among key government and private sector stakeholders, but these have met with limited success. I strongly support creating a more effective model for operational collaboration to move us from the less effective government-led partnerships of the past to a more dynamic and collaborative approach involving cybersecurity leaders from government, industry, and academia. A collaboration framework for public private partnerships should include focused efforts to:

- Exchange threat and technical data (at the unclassified level as much as possible) to enable meaningful action, with rules and mechanisms that permit both sides to protect sensitive data. This approach is a shift from past practices that viewed information sharing as an objective as opposed to a tool;
- Create global situational awareness to understand the state of the computing ecosystem and events that may affect it;
- Analyze risks (threats, vulnerabilities, and consequences) and develop mitigation strategies; and
- When necessary and consistent with their respective roles, respond to threats.

Innovative Security Controls: The technologies used in enterprises today often grow faster than security organizations can make sense of them. Since computing technologies will continue to advance at a rapid pace, organizations creating security policy, standards,

and technologies must consider how transformative changes in technology (e.g., wireless, RFID, peer-to-peer networks) create different risks and require different controls to maintain or improve security.

Moving Forward

One of the greatest challenges facing government is measuring its progress in improving cybersecurity. Are things better, worse, or the same? What is “success”? I strongly advocate for tracking progress, but must also caution against thinking of cybersecurity in terms of success and failure. Recognizing that cyberspace threats are not going to disappear and that attackers will be persistent and adaptive, it is not about risk elimination but risk management. As long as threats evolve, so must our efforts to protect against them. The U.S. must build holistic Information Age strategies to combat these threats in a coordinated manner. Reducing the attack surface of the Federal enterprise and mitigating broad classes of threat will require fundamental changes. According to OMB, Federal agencies spent approximately \$6.2 billion (approximately 9.2 percent of the total IT portfolio) securing the government’s total IT investment of approximately \$68 billion for the fiscal year 2008.⁸ But these resources and the current capabilities they fund do not provide sufficient defense. Absent agile government-wide security policies, standards, and oversight capabilities, the Federal enterprise will present an unacceptably easy target. There is mounting proof that we must build an Information Age security model that creates a horizontal (cross-government) set of security requirements and builds, on top of that horizontal layer, agency specific protections to ensure that the government (generally) and each agency can fulfill its mission and protect the security of its information network.

⁸ Fiscal year 2008 FISMA Report to Congress.