Written Testimony of
Scott Charney
Corporate Vice President, Microsoft Corporation's Trustworthy Computing
Securing America's Cyber Future: Simplify, Organize and Act

Before the
House Committee on Homeland Security
Sub-Committee on Emerging Threats, Cybersecurity, and Science and Technology
Hearing on "Reviewing the Federal Cybersecurity Mission"

March 10, 2009

Chairwoman Clark, Ranking Member Lungren, and Members of the Subcommittee, thank you for the opportunity to appear today at this important hearing on cybersecurity. My name is Scott Charney, and I am the Corporate Vice President for Trustworthy Computing at Microsoft. I served as one of four Co-Chairs of the Center for Strategic and International Studies' (CSIS) Commission on Cybersecurity for the 44th Presidency. I served on the Commission as an industry expert with more than 18 years of security technology experience in both the public and private sectors, and have a long history of leading domestic and international cybersecurity efforts.

Prior to joining Microsoft, I was Chief of the Computer Crime and Intellectual Property Section in the Criminal Division of the U.S. Department of Justice. I was involved in nearly every major hacker prosecution in the United States 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.

Representative Jim Langevin (D-RI), Representative Michael McCaul (R-TX), Lt. Gen. Harry Raduege, USAF (Ret.), and I led the CSIS Commission effort, along with project director Jim Lewis of the Center for Strategic and International Studies, to identify key cybersecurity challenges facing the new administration and provide a set of recommendations to address those challenges. Guided by our Congressional co-chairs, we assembled a group of individuals with cybersecurity experience in both government and industry. The aim of the group was to identify both short-term recommendations that the next administration could implement quickly to make a noticeable improvement in the nation's cybersecurity, and longer-term recommendations that are critical to the nation's future cyber-objectives.

Thank you for the opportunity to appear today to provide a perspective on "Reviewing the Federal Cybersecurity Mission." I would like to address four specific themes that cross the Commission recommendations including: (1) the need for a comprehensive and coordinated national strategy for cyberspace security; (2) the imperative to radically evolve and elevate the public private partnership model; (3) the need for an identity metasystem that makes the Internet dramatically more secure while protecting important social values such as privacy and free speech; and (4) the necessity for a new regulatory model that protects innovation while providing appropriate government oversight.

Comprehensive and Coordinated National Strategy

As the CSIS Commission report makes clear, 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 even what we have come to call "the Internet citizen." Cyberattack joins terrorism and weapons of mass destruction as one of the new, asymmetric threats that puts the U.S. and its allies at risk. To be clear, there are risks to cyberspace other than those related to security; for example, the increasing number of machines and applications creates a very complex environment with challenging reliability issues, and our increased dependence on information technology makes the availability of systems a national and international imperative. But for the purposes of this testimony, I will confine my remarks to security.

The information age has arrived, but the Unites States has not yet built a comprehensive national cyberspace security strategy. The need for such a strategy has never been more urgent. America's leadership in a connected world cannot be assumed from its leadership in the industrial world. In cyberspace, the country does not remain unchallenged, as recent events have clearly proved. Some of the challenges we face include:

- America's reliance on interdependent global networks;
- The misuse of information technologies to support violent extremism;
- The ability of any individual to engage in activities formerly limited to nation-states (e.g., cyber-military espionage and cyber-warfare); and
- The ability of any nation, regardless of traditional measures of sophistication, to gain economic and military advantage through cyber programs.

In addition to these challenges, the Internet citizen – those individuals who use cyberspace for social and commercial interactions – is critically relevant to any solution. Unsecured computers can turn everyday users into a launch platform for attacks. Fear about online security and availability can have sweeping economic consequences. Trust in cyberspace, on the other hand, can create new opportunities, markets and possibilities.

The United States must plan, organize and act accordingly to develop a national cyberspace security strategy that can address these challenges. Historically, national security strategies have been characterized by their employment of all elements of U.S. 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 and public safety, ensure economic prosperity, and assure delivery of critical services to the American public. Such a strategy must also recognize the ever-mounting importance of economic security. In the industrial age, power was generally based on physical might; in the information age, power is derived from information, knowledge, and communications.

In my opinion, there are three fundamental attributes that span all of the elements of national power. Articulating and advancing a clear understanding of norms, attribution, and deterrence in

the context of cybersecurity can dramatically improve the national and international cyberspace ecosystem.

Norms: U.S. foreign policy and diplomatic engagements on issues related to cyberspace security are not as focused as our efforts to combat terrorism or stem proliferation of nuclear weapons. I believe that the U.S. should marshal its significant diplomatic skills and expertise to advocate for cyberspace security and increase multilateral cooperation. I would caution that advocacy and cooperation are not goals in themselves. We need to focus advocacy and cooperation efforts toward specific outcomes. For example, working with like-minded nations to define clearly articulated norms of nation-state behavior in cyberspace could help to deter state support for cyberattacks or hold nation-states that support such efforts accountable for their actions.

Attribution: Attribution of cyberattacks is one of the most fundamental challenges facing the international community and the United States. The inability to attribute attacks can greatly impede the effectiveness of the nation's response. Too often, valuable time is lost trying to determine if an attack or penetration of a system was an isolated criminal incident or one perpetrated by a foreign intelligence organization. Attributing the source is essential to ensuring the appropriateness of response — criminal prosecution or military/diplomatic measures. Absent strong attribution abilities, international and national strategies to deter acts will not be taken seriously by the community of attackers who thrive on this diagnostic weakness, nor by criminals that prey on citizens' inboxes and online accounts. Thus, we must focus on identity and authentication in cyberspace and enhancing swift international cooperation on cyberattacks.

Deterrence: Deterrence did not happen overnight in the Cold War; the concept and strategy took several years to develop. Deterrence in the information age is perhaps even more complicated due to the lack of attribution and the inability to identify strong mechanisms to prevent hostile actions. But the United States can learn important lessons from the nuclear experience. In the Cold War, the United States kept sensitive information secret, but disclosed enough about our strategy and capabilities that allies and adversaries alike understood our commitment to national security and our ability to protect it. We must do the same for cyberspace.

Deterrence is very difficult when adversaries and bad actors are motivated and persistent. In order to improve cyberspace security in a meaningful way, deterrence requires a clear and unambiguous commitment by our nation and understanding by the spectrum of bad actors — from cybercriminals, to organized crime, to nation-states — that violations of our cybersecurity have consequences. What makes deterrence successful is commitment, broadly known and broadly felt.

The sheer number of extremely important issues that transcend agency boundaries suggests that the coordination of any national cybersecurity strategy must reside within the one organization responsible for ensuring that the government acts as one government. If the government wants to use all the instruments of its power — economic, diplomatic, law enforcement, military and intelligence — then the center of gravity must be in the White House. I support the

Commission's recommendations that, if implemented, would elevate the priority of cybersecurity and improve its strategic coordination. Creating a National Office for Cyberspace in the Executive Office of the President will provide the interagency coordination required to identify, assess, and manage cyberspace risks.

This office does not need to assume or manage all cybersecurity functions; rather, it should have a tightly defined mandate to develop strategy and coordinate the implementation of that strategy by the agencies that have jurisdiction over the elements of national power. It must also be recognized that the White House office will be best able to provide strategic leadership only when the agencies of government responsible for executing their respective cybersecurity responsibilities are staffed with experienced and competent professionals who are resourced appropriately.

As you know, President Obama has directed the National Security Council and Homeland Security Council to initiate a 60-day review of the plans, programs, and activities under way throughout the government that address cyberspace security. According to the White House, *the review will build upon existing policies and structures to formulate a new vision for a national public-private partnership and an action plan to: enhance economic prosperity and facilitate market leadership for the U.S. information and communications industry; deter, prevent, detect, defend against, respond to, and remediate disruptions and damage to U.S. communications and information infrastructure; ensure U.S. capabilities to operate in cyberspace in support of national goals; and safeguard the privacy rights and civil liberties of our citizens.*[1]

A successful cyberspace security strategy requires more than a plan and an organization; it requires partnership. The private sector drives the design, development and implementation of the products and services that power cyberspace. Our technical expertise and experience in the global marketplace make us key partners in developing national and international cyberspace security strategies. For more than a decade, the government and the private sector have partnered to address various aspects of cybersecurity, but this partnership has not achieved the robust results that are needed to protect cyberspace effectively. Therefore, my next key recommendation is to redesign that partnership.

Radically Evolve Public Private Partnerships to Advance Cyberspace Security

Cyberspace security is a shared challenge and requires government and the private sector to work together. The private sector designs, deploys, and maintains much of the nation's critical infrastructure. However, the private sector faces unique challenges because its customer base and supply chains are global. It also builds commercial products that can be targeted by sophisticated advisories, including nation-states. Private sector firms are increasingly being forced to think about security challenges that cannot reasonably be mitigated by commercially realistic development practices, especially as users remain price-sensitive.

The government also faces challenges. Unlike certain other traditional aspects of national security, cyberspace cannot be secured by the government alone; it requires a coordinated effort

[1] http://www.whitehouse.gov/blog/09/03/02/Cyber-review-underway/.

involving the owners, operators, and vendors that make cyberspace possible. The bifurcation of responsibility (the government must protect national security) and control (it does not manage the assets or provide the functions that must be protected) dictates the need for a close partnership with clearly defined roles and responsibilities that optimizes the capabilities of participating stakeholders.

Since the 1990s, well-intended public private partnerships have been created to address this need, yielding a perplexing array of advisory groups with overlapping missions, different stakeholders with varying capabilities, insufficiently articulated roles and responsibilities, and plans with literally hundreds upon hundreds of recommendations. In the few instances where groups overcame institutional adversities and developed meaningful recommendations, the repeated unwillingness or inability to implement those recommendations at the Federal level has damaged the partnership significantly. Absent a comprehensive national strategy and clear purpose, both government and private sector stakeholders will continue to struggle to be effective.

Advancing cyberspace security requires a radical evolution of public private partnerships as we currently know them. What does radical evolution mean? The federal government and private sector stakeholders must articulate a new philosophy for collaboration, one that starts with a very simple premise: government and private sector efforts should be synergistic and efficient. This requires that the government and private sector: (1) identify those security requirements that will be fulfilled by the market; (2) identify national security requirements; and (3) identify how the gap between market security and national security can be filled. This effort must be focused on protecting functions (e.g., communications) as opposed to simply physical assets. Moreover, we must build operational partnerships that let us effectively mitigate and respond to threats. Finally, to the extent important work is ongoing, the parties must identify what works and have the courage to retire what does not, even though retiring organizations may be viewed as draconian by those who have invested in these efforts in the past.

As part of the evolution, it is important that the public private partnership concentrate on what is truly critical to cyberspace security and build trusted and effective collaboration between government and private sector stakeholders.

What functions are critical?

The Commission identified four critical cyber-infrastructures:

- Energy;
- Finance;
- Converging information technology and communications;[2] and
- Government services (including state and municipal governments).

[2] Outside the United States, this is referred to as the ICT sector. See "Telecommunications Task Group Final Report," CSIS Cybersecurity Commission http://www.csis.org/media/csis/pubs/081028_telecomm_task_group.pdf, for more information on why "the boundary between information, information technology, and telecommunications services has become almost indistinguishable."

This is not to suggest that all these infrastructures are identical. If power fails, the cascading effect is immediate and significant; by contrast, the result of an attack on government will depend upon what government service is affected. In essence, energy and information technology and communications form the backbone of cyberspace, and the availability of government services and finance are particularly important for national security. While other infrastructures depend on cyberspace, an interruption of their operations would not broadly affect cyberspace itself. If energy, finance, the converging information technology and communications networks, along with government services, can continue to function as intended while under attack, cyberspace will continue to support the nation. Thus, these infrastructures should be the focus of a more attentive cyberspace security effort.

Trusted and Effective Collaboration

The majority of public private partnership efforts to date have focused on information sharing. While information sharing is important, it cannot be — as it had been to date — the end goal; rather, we must focus instead on sharing information that is actionable and then taking action. The CSIS Commission recommended three new partnership groups to advance beyond information sharing to enable trust and action. I will focus my comments on the two that would most significantly and immediately enhance our cybersecurity and resiliency by permitting better strategy development and operational collaboration.

Evolve Strategic Presidential Advisory Bodies

Trust is the foundation of a successful partnership between government and the private sector. In the past few years, despite good intentions on both sides, trust between government and the private sector has declined. Trust is built on personal relationships and in small groups, with parity of stakeholders and demonstrated commitment. Large, diffuse groups with floating engagements among a range of participants are not conducive to building the level of dialogue that promotes trust. When the President brings C-Level officers to the table and addresses challenges in a trusted forum, he can drive a powerful set of changes in the cyber-ecosystem. Advisory committees that engage senior level government and private sector personnel, such as the National Security and Telecommunications Advisory Committee (NSTAC) and the National Infrastructure Advisory Council (NIAC), have served past presidents well. However, the split between national security and emergency preparedness communications and cybersecurity is artificial and dangerous. In the information age, with its converged information technology and communications infrastructure, the distinction between these two groups creates overlap and limits progress on developing and improving cyberspace security capabilities. Accordingly, the Commission recommended establishing the President's Committee for Secure Cyberspace to replace the NSTAC and NIAC.

In addition to establishing the proposed Committee for Secure Cyberspace as a C-level membership organization operated under Federal Advisory Committee Act, the Administration should act to reform current decision-making bodies in government that do not have private sector involvement. For example, the Joint Telecommunications Resources Board (JTRB), which is chaired by the Office of Science and Technology Policy, consists of agencies, such as

the Department of Defense (DOD), the Department of Homeland Security, the General Services Administration, and the Department of Commerce.[3] The JTRB is chartered to make decisions on how to prioritize telecommunications resources in non-wartime crisis, yet absent an effective channel into the private sector, the JTRB would be challenged to fulfill its charter. Another parallel entity is the National Cyber Response Coordination Group, an organization intended to help identify and coordinate response to a cyber-based crisis. Unfortunately, this interagency government group does not have a meaningful way to engage the private sector, thus limiting its strategic and tactical effectiveness.

Create Operational Collaboration

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. For example, the private sector has invested and maintained information sharing and analysis centers, but they are all too often ignored by government agencies. The Commission recommended creating a new organization, the Center for Cybersecurity Operations (CCSO), to address operational issues that affect cyber infrastructure.

I strongly support creating a more effective model for operational collaboration to move us from the less effective partnerships of the past to a more dynamic and collaborative self-governing approach involving cybersecurity leaders from government, industry, and academia.

Collaboration is not about plans; it is about outcomes. To create actual operational collaboration, we must learn from the experiences of the past. 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. I would like to add to the Commission recommendation and 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;
- Create global situational awareness to understand the state of the computing ecosystem and events that may affect it;
- Analyze the risks (threat, 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.

What needs to be accomplished over 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 goal is a trusted and

[3] Executive Order 12472, "Assignment of National Security and Emergency Preparedness Telecommunications Functions," section 2(b)(3), April 3, 1984, available at http://www.ncs.gov/library/policy_docs/eo_12472.html.

focused collaborative alliance for both strategy and operations among the government, academia, and the private sector.

Take action today to create a more secure tomorrow

Online collaboration, commerce and, in some instances, public safety depend on trust. Today the mechanisms to provide authentication and attribution in cyberspace do not meet the needs of the Internet citizen, enterprises or governments. The lack of trust stems in part from our inability to manage online identities effectively and the excessive reliance on voluntary efforts to close key gaps in security.

Identity Imperatives

In the context of national security, weak identification and authentication limits an organization's ability to enforce security policies to protect sensitive information and systems, and hinders effective government and industry response to cyberattacks. From an economic security perspective, these weaknesses prevent Internet users from taking reasonable steps to protect themselves from dangerous parties. Creating the ability to know reliably the person and/or device that is sending a particular data stream in cyberspace must be part of an effective cybersecurity strategy. Even sophisticated attackers face difficult challenges — and find their access restricted — because of better authentication.

This need for improved identity and authentication in cyberspace has been documented in numerous forums, and government and industry are progressing on multiple initiatives to address it. For example, in the United States, the Federal Financial Institutions Examination Council's (FFIEC) Guidance for Authentication in an Internet Banking Environment has spurred the use of stronger authentication in online banking. The experience of the DOD was that intrusion into its networks fell by more than 50 percent when it implemented Common Access Cards (CAC). Homeland Security Presidential Directive 12 (HSPD-12) ("Policy for a Common Identification Standard for Federal Employees and Contractors") is another U.S. authentication initiative which requires federal agencies to improve their identity and credentialing processes, using smart cards to secure both physical and logical access to federal facilities and networks. These and other federal initiatives have had success, but it is often limited to the sector or domain for which they are attempting to affect change.

Past efforts to radically improve identity management for cybersecurity have not failed due to lack of awareness regarding the problem, nor a lack of efforts to address it. Much more simply, there are too many disparate efforts resulting in stove-piped policies and technologies that conflict and compete with each other, instead of driving toward a coordinated, interoperable, scalable security- and privacy-sensitive solution. There is also, particularly in the consumer sector, a serious "chicken-and-egg" problem: consumers are not interested in robust online identity tokens because government and commercial sites do not consume them, and government and commercial sites do not build technology to consume such tokens because, after all, no consumer has them. I want to re-emphasize a point made earlier: any successful public private partnership should start with the premise that the government should fill market gaps in security. Thus, as part of an overall cybersecurity strategy, the government should accelerate the adoption of authentication technologies by supporting the creation and use of digital credentials. This

would include issuing and accepting such credentials in appropriate circumstances, catalyzing the private sector market for digital identities, and establishing the appropriate governance structure for the issuance, use, revocation, and destruction of digital credentials.

The use of digital IDs also reduces the need to authenticate people by having them provide private details about themselves, known as Personally Identifiable Information or PII. This usage would reduce the need to transmit, store and use private information to identify individuals, thus increasing privacy and helping prevent crimes such as identity theft. Stronger authentication, combined with appropriate rules regarding the use of such authentication mechanisms, could enhance both security and privacy.

I recognize that efforts to improve authentication raise sensitive privacy and civil liberties issues, but it is possible to improve authentication for critical functions without unduly compromising our values.[4] This can be done if we integrate privacy issues into the design, development and operation of the identity metasystem.

The Role of Regulation

Opinions vary widely on how industry and government can best work together to more effectively increase cybersecurity across critical infrastructures and government. But even if public and private cooperation is optimized and operationalized, that will not provide the level of security necessary to meet national security demands. This is true because markets respond to customer demand and most customers, even though more aware of security issues today than in the past, will not pay for the level of security likely necessary to protect national security.

This recognition, however, does not mean the first step to address the gaps between the current and desired states of security should be broad-based regulation. Rather, the government should encourage a balanced approach, one that combines industry self-regulation with government influence (through, for example, procurement regulations) and then includes carefully tailored regulation when necessary. I believe such a combined approach can be highly effective without unduly raising the costs for users and stifling the very innovation that is needed to make infrastructures more secure.

When security gaps are identified — and neither market forces nor non-regulatory government intervention suffices to address that gap — government should focus on adopting the regulatory model suggested by the CSIS Commission. In this model, industry identifies the best practices, and the government ensures their adoption and works to harmonize requirements across sectors. I would also add that any government regulation should follow certain key principles: it should solve a clearly identified problem; it should neither be under-inclusive (fail to solve the problem fully) nor over-inclusive (address more than the problem); it should not be crafted in a way that creates unintended consequences; and it should be technology-neutral and not create hard-to-modify statutorily imposed technology requirements that stifle innovation and prevent further enhancements in security.

[4] For more on this topic, including how the government can ensure privacy is protected in a better authenticated environment, see the White Paper on Establishing End to End Trust, www.microsoft.com/endtoendtrust (pp. 6-7).

Progress in cyberspace security is not without cost. Voluntary efforts have closed many security gaps but have not done enough. Establishing a cohesive national strategy with a robust public private partnership will create a framework for tailored regulations that can advance identity and trust in a manner that markets alone cannot.

Moving Forward

The first major Presidential document on emerging threats in cyberspace was published more than a decade ago when the President's Commission on Critical Infrastructure Protection released its seminal report.[5] At that time, only 1.7% of the world's population (70 million people) had Internet access. In the years that have followed, the world has changed dramatically. Attacks have evolved from exploits designed to garner attention to targeted stealth attacks that are designed for more nefarious purposes, such as conducting identity theft, economic espionage, and military espionage. In 2008, almost a quarter of the world's population (more than 1.5 billion people) had Internet access, and it continues to grow.[6] The rise of the Internet has permitted new forms of social connection, and created new educational and economic opportunities. But the richness of cyberspace also permits criminals, foreign intelligence organizations and nation-states to exploit cyberspace for profit, espionage or conflict. Securing America's future in the information age depends upon creating a comprehensive national strategy for cyberspace security, one that simplifies, organizes and enables operational partnerships between and among government and private sector stakeholders, including Internet citizens.

[5] http://cip.gmu.edu/archive/5_PCCIPCriticalFoundations_1097_full_report.pdf.
[6] http://www.internetworldstats.com/emarketing.htm.

Supplemental information for
Scott Charney
Corporate Vice President, Microsoft Corporation's Trustworthy Computing

House Committee on Homeland Security
Sub-Committee on Emerging Threats, Cybersecurity, and Science and Technology
Hearing on "Reviewing the Federal Cybersecurity Mission"

March 10, 2009

Address and Contact information:

Mr. Scott Charney
One Microsoft Way
Building 27
Redmond, WA 98052
(office) 425-707-3440

Topical Outline:

I would like to address four specific themes that cross the Commission recommendations including: (1) the need for a comprehensive and coordinated national strategy for cyberspace security; (2) the imperative to radically evolve and elevate the public private partnership model; (3) the need for an identity metasystem that makes the Internet dramatically more secure while protecting important social values such as privacy and free speech; and (4) the necessity for a new regulatory model that protects innovation while providing appropriate government oversight.

1. Comprehensive and Coordinated National Strategy
    a. Norms
    b. Attribution
    c. Deterrence
2. Radically Evolve Public Private Partnerships to Advance Cyberspace Security
    a. What functions are critical?
    b. Trusted and Effective Collaboration
3. Take action today to create a more secure tomorrow
    a. Identity Imperatives
    b. The Role of Regulation
4. Moving Forward