Statement of Edward Amoroso, Ph.D.

Senior Vice President & Chief Security Officer
AT&T

Hearing: "DHS's Cybersecurity Mission:
Promoting Innovation and Securing Critical Infrastructure"

United States House of Representatives

Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies

April 15, 2011

Chairman Lungren and Ranking Member Clarke, I would like to thank you and all the members of the Subcommittee for this invitation to address the significant challenges facing the private sector and the Department of Homeland Security in securing critical infrastructure from cyber threats. In my testimony, I will try to identify current challenges as well as the actions that can be taken to address those challenges; and in particular how to coordinate the government's cybersecurity capabilities with the private sector's investment in infrastructure and operational capabilities.

My Background

I currently serve as Senior Vice President and Chief Security Officer of AT&T, where I have worked in the area of cybersecurity for the past twenty-six years. My educational background includes a Bachelor's degree in physics from Dickinson College, as well as Masters and PhD degrees in computer science from the Stevens Institute of Technology, where I have also served as an adjunct professor of computer science for the past twenty-two years. I am a graduate of the Columbia Business School, and have written many articles and five books on the topic of cybersecurity. My most recent book is entitled "Cyber Attacks: Protecting National Infrastructure" (Butterworth-Heinemann, 2011).

My current responsibilities include design and operation of the security systems and processes that protect AT&T's vast domestic and international wired and wireless infrastructure. This infrastructure is the core asset that permits AT&T to provide the wide variety of advanced network services that AT&T offers to its many millions of customers around the world, ranging from the largest global business enterprises to individual consumers. AT&T has also had the opportunity to work with the Department of Homeland Security (DHS) in a variety of ways in the decade since the Department was created.

For instance, we actively participate with DHS in the National Cybersecurity Communications Integration Center (NCCIC) in both its national security/emergency preparedness and cyber security missions. We are also active participants in the President's National Security Telecommunications Advisory Council (NSTAC) and the Communications Sector Information Sharing and Analysis Center, both of which are administered by DHS. We have also supported DHS in the testing and evaluation of prototype network-based cyber security capabilities over the last several years. Finally, we were the first company to obtain a formal Authority-To-Operate to provide Trusted Internet Connection service to Government Agencies through the General Services Administration (GSA)/DHS joint Managed Internet Protection Service initiative under the GSA Networx contracts.

What is cybersecurity?

Simply put, from the perspective of protecting the nation's critical infrastructure, cybersecurity is the ability to protect critical systems from disruption, or critical information from alteration or theft. Potential threats range from disgruntled individuals to criminal elements to transnational actors to sophisticated and well-resourced nation states. Motives can range from mischief to deliberate acts of hostility through sabotage and terrorism. The methods and forms of infrastructure intrusion are continually advancing so as to bypass standard preventive measures such as the application of firewalls and intrusion detection systems between the critical system and the Internet at large. One such form of evolving cyber attack uses “botnets” – which are run by malicious parties who are increasingly adept at harnessing the power of dispersed personal computers and other smart devices attached to the nation’s networks and using them to attack unsuspecting victims.

As the largest provider of communications and network services in the world, AT&T takes very seriously its responsibility to protect our infrastructure and our customers from the vast and ever changing cyber threats. Cyber security is a business imperative at AT&T, and we work very hard at it, investing significant resources to innovate and keep pace with technology that may be either the source or target of the threats. The size and scope of AT&T’s global network, coupled with our industry-leading cybersecurity capabilities, gives AT&T a unique perspective into malicious cyber-activity. AT&T offers one of the world's most advanced and powerful global backbone networks, carrying 23.7 Petabytes of data traffic on an average business day to nearly every continent and country (a Petabyte is a million billion bytes of data, or a “one” followed by 15 zeros), and we expect that to double every 18 months for the foreseeable future. Our intelligent network technologies give us the capability to analyze traffic flows to detect malicious cyber-activities, and in many cases, identify very early indicators of attacks before they have the opportunity to become major events. For example, we have implemented the capability within our network to automatically detect and mitigate most Distributed Denial of Service Attacks within our network infrastructure before they affect service to our customers, and we continue to improve our ability to provide global coverage to mitigate denial-of-service attacks from multiple locations across the United States, as well as nodes in

Europe and Asia. We are constantly improving our cyber capabilities, including the ability to detect and mitigate Advanced Persistent Threats, the most sophisticated and pernicious forms of cyber attack.

What needs to be done?

I would like to outline four broad themes for your consideration during today's hearing. Improving the overall cyber security posture of the United States is a daunting task. We cannot undertake this challenge unilaterally – it is clearly a global issue in all its dimensions. The Administration and the Congress have put forth a variety of ideas and initiatives on how we can begin to tackle this challenge; some are helpful, and some would stifle the innovation and flexibility we need to identify and respond to the ever changing threats. Improving our national cyber security posture is a long journey that will not be solved by simple pronouncements or regulatory dictates. We can, however, start to put some foundational elements in place to build on for the future.

1. Build a Collaborative Active Cyber-Defense Capability.

First and foremost, the United States needs to build a collaborative active cyber-defense capability. The global communications infrastructure is the primary vehicle for delivery of cyber attacks against U.S. interests, yet there is no comprehensive coordination mechanism for rapidly detecting and analyzing attacks and responses. Each Tier One communications network operator and service provider monitors its own network to varying degrees, with varying capabilities to mitigate or block attacks. In addition, the multiple government programs which already exist are focused on monitoring traffic to and from multiple government networks – none of which are operationally integrated. Given the increasing sophistication and scope of cyber attacks, we can no longer expect that individual companies or consumers, or disparate government network monitoring programs, provide adequate protection against evolving threats.

Attack related protective information might be known to the Federal Government, for example, but otherwise unknown to private industry. In the event that a government agency becomes aware of a malicious attack signature that could be deployed into intrusion detection systems to protect industrial, non-government assets, the government should have the confidence that it can be so deployed without further delay or review. A collaborative active cyber-defense capability to detect, analyze, and mitigate malicious cyber activities in the core networks that make up the Internet itself will enable cyber attacks to be detected and attempts be made to stop them before they reach their target.

Such a capability should leverage and build upon the existing cyber security capabilities of the Tier One network operators and service providers whose networks are the core of the Internet in the United States, as well as the complimentary capabilities of the security technology and software industries. Critical national systems, large and small business, industrial concerns, and individual Internet users can all be better protected by this umbrella approach. Combining these elements to work in a collaborative and coordinated fashion can provide the basic foundation for the active cyber-defense capability. National intelligence capabilities to identify cyber threats and provide advanced warning can also be leveraged. In this way, a new collaborative cyber defense capability will both feed into and strengthen existing public-private coordination and response efforts.

2. Government Leadership in Acquisitions and Cyber Management.

The United States government should lead by example in cyber security. The federal government is the largest single purchaser of information technology and network services in the

United States, and its leadership and buying power can have great influence on the cyber security marketplace. Several worthwhile federal initiatives are in place to improve cyber security for the ".gov" domain, such as the Trusted Internet Connection effort by the Office of Management and Budget (OMB) and its instantiation via the General Service Administration/Department of Homeland Security joint initiative on Managed Trusted Internet Protection Service, but they are being applied inconsistently. The Department of Defense also has its own effort to protect ".mil", separate from the ".gov" efforts. These initiatives do not yet take full advantage of the portfolio of managed security services offered by many private sector network service providers, such as network-based protection against Distributed Denial of Service (DDOS) attacks. The federal government needs a clear and comprehensive strategy for cyber security of all Federal systems which make up ".gov" and ".mil" - one which effectively leverages existing cyber security capabilities offered by the network service providers.

Further, the current roles and authorities of the various federal agencies overlap and are unclear with respect to cyber security for federal government infrastructure, as well as the protection of other critical infrastructure, national assets and individual consumers. Congress can lead by establishing the respective and definitive roles and authorities of the various Executive Branch elements involved in all aspects of cyber security – including the National Security Council and the Cyber Policy Coordinator, the Office of Management and Budget, the Office of Science and Technology Policy, the Department of Homeland Security, the Department of Commerce including the National Institute of Standards and Technology and the National Telecommunications and Information Administration, the Department of Defense including U.S. Cyber Command and the National Security Agency, the Department of State, the Federal Communications Commission, and the Federal Trade Commission. The United States needs a unified Federal effort on cyber security with a clear understanding of the roles involved – not the confusion, inconsistency, and overlap that currently exists.

3. Global Strategy.

The United States must move forward aggressively to create a comprehensive strategy for addressing global cooperation in cyber security. We must reinforce the leadership of the United States in shaping the future of the Internet, and assuring it's stable, reliable, and secure operation, concurrent with the expansion of U.S. enterprise in the global Internet marketplace. In particular, all members and participants of the global Internet community must achieve consensus on the fundamental point that malicious cyber activities of any sort will simply not be tolerated. Concurrent with these efforts, Congress should also expand incentives for investment by the private sector to help invigorate U.S. technology leadership in cyber security and the Internet.

4. Cyber literacy.

We all must redouble our efforts in cyber security education and awareness across the full spectrum of the Internet user base – from the boardrooms of our largest companies to the millions of individuals who surf the 'net. Current efforts in cyber security education and awareness are fragmented and the messaging is often confusing. The ultimate key to improving our national cyber security is technology innovation driven by market demand from informed users and purchasers of all kinds. By creating market demand for cyber security through heightened consumer awareness, we can spur fundamental security innovation at all levels of the Internet eco-system, and allow the United States to continue as a leader in Internet development. To that end, Congress should designate a lead Agency on cyber security education, and support that designation with an appropriate level of funding to make it effective. The roles of other

Federal Agencies in supporting this effort should also be clarified.   AT&T is itself actively engaged in the provision of cyber security information and protective tools to our customers, and actively participates in pan-industry cyber awareness education efforts such as "Stop.Think.Connect," the coordinated messaging effort spearheaded by the Anti-Phishing Working Group and the National Cyber Security Alliance and comprised of government agencies, private sector entities, and not-for-profit corporations.

In the past, cybersecurity legislative proposals have included a variety of regulatory schemes, such as certification regimes, that, while well-intentioned, are too often the antithesis of innovation – such requirements could have an unintended stifling effect on making real cyber security improvements. Our cyber adversaries are very dynamic and ever more sophisticated, and do not operate under a laboriously defined set of rules or processes. The challenges we face in cyber security simply cannot be solved by imposing slow moving, consensus-based bureaucracy on those who build, operate, and use cyber space. Overbroad regulation and certification requirements can have unintended consequences, such as emphasizing the status quo by focusing on yesterday's challenges. An overly prescriptive approach can only serve to stifle Internet innovation and the technology leadership of the United States in the global information infrastructure.

The Internet itself was created through innovation. Some key early investments by the government helped spur that innovation. Congress and the Administration have leadership rolls to play in assuring that the United States continues to focus on technology innovation. Burdening the private sector with the cost of unnecessary and ineffective regulations and processes is contrary to that objective, and will only slow advances in cyber security. Congress must insist on and support initiatives that provide the flexibility needed to deal with the dynamics of the threat and the technology, while creating innovation and investment through market demand.

I thank the Subcommittee for its timely and focused attention on cybersecurity, and I look forward to providing on-going guidance, assistance, and recommendations as we collectively work to reduce the cybersecurity threat to our nation and our critical infrastructure.