Before the

DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration

In the Matter of	)	
	)	
Cybersecurity, Innovation and the	)	Docket No. 100721305-0305-01
Internet Economy	)	
	)	
	)	

COMMENTS OF AT&T INC.

Keith M. Krom
Theodore R. Kingsley
AT&T Inc.
1133 21st Street, N.W.
Washington, D.C. 20036
(202) 463-4148
(202) 463-4627

TABLE OF CONTENTS

Before the

DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration

In the Matter of	)	
	)	
Cybersecurity, Innovation and the Internet Economy	)	Docket No. 100721305-0305-01
	)	
	)	

COMMENTS OF AT&T INC.

AT&T Inc., on behalf of itself and its affiliates, hereby submits these comments in response to the Department of Commerce Internet Policy Task Force ("the Department" or "Task Force") Notice of Inquiry, "Cybersecurity, Innovation and the Internet Economy" ("NOI" or "Notice").[1]

INTRODUCTION

AT&T commends the Task Force's ongoing focus on Internet policy challenges and, in particular, those relating to cybersecurity. In its NOI, the Task Force sets out the global and constantly evolving nature of cyber threats and vulnerabilities and identifies key stakeholders in the cybersecurity dialogue: consumers, small, medium and large enterprise users outside the critical infrastructure and key resources (CIKR) realm and their customer base, private sector infrastructure providers, and software and service providers. The Task Force is in a unique position to take a broad view of cybersecurity issues which encompass the entire Internet ecosystem and to consider the impact of any government action on end-user customers,

[1] 75 Fed. Reg. 44216, Notice of Inquiry (July 28, 2010) ("NOI").

economic and market conditions, and continued innovation and technical advancement of the Internet.

AT&T, in its roles as a global IP network and provider of Internet connectivity services and solutions, is a key communications CIKR sector stakeholder. While the primary focus of the NOI is on enhancing the cybersecurity practices of commercial entities and consumers outside the CIKR sectors, AT&T's experience is relevant to the work of the Task Force. AT&T provides Internet connectivity and managed security services to business and consumers within and outside of the 18 CIKR sectors identified by the Department of Homeland Security ("DHS"). As a result, AT&T has observed a wide range of cyber threats and related stakeholder behaviors within the global Internet ecosystem.

I. BACKGROUND: THE ROLE OF PRIVATE AND PUBLIC SECTORS

A significant proportion of current consumer vulnerabilities arise from the application and device layers, where even small security flaws are exploited by hackers to create vast networks of hijacked consumer-managed systems that cause substantial economic and social damage. Technological vulnerabilities are compounded by the fact that many users do not take appropriate steps to protect themselves online, or fall victim to creative, socially engineered scams and attacks. And, as the Department notes, computing devices are increasingly interconnected with the consequence that security deficiencies in even a limited number of systems can be exploited to launch cyber intrusions or attacks on other systems.[2]

[2] NOI at 44217.

A. The Role of the Private Sector

The Department announces its intention to recommend public policies and private-sector norms that can markedly improve the overall cybersecurity posture of key stakeholders. The Department concurrently states its belief that public policies affecting cybersecurity as well as private sector norms require a fresh look, and acknowledges the valuable roles, responsibilities, and capabilities of the private sector in creating tools and strategies to mitigate cyber risks. In light of the varied, nefarious and adaptive nature of the cyber threats, the most effective weapons in the cybersecurity challenge remain private sector innovation and flexibility. Preserving and encouraging these protections should be an essential policy goal. The private sector understands the importance of cybersecurity to its customers and to its own economic viability, and already addresses cybersecurity in a substantial way. Through substantial investment and innovation, the private sector has developed extremely sophisticated and real-time cybersecurity practices without overly prescriptive norms that could have unintentional consequences.

As it undertakes a fresh look at the public polices and private sector norms relevant to cybersecurity, the Department should therefore take care to identify the wide-ranging communications sector cybersecurity efforts already underway – which are effectively promoted through market forces. AT&T itself has taken market-leading steps to educate and empower its customers through information and security tools tailored to the needs of those customers. The desire to avoid the significant economic and reputational damage that can be caused by a major cyber attack, coupled with intense competition among communications service providers, drives innovation in cybersecurity as service providers strive to constantly stay ahead of evolving cyber threats as well as their competition, resulting in improved network security for all users.

In sum, all stakeholders need to be engaged in cybersecurity efforts throughout the entire Internet ecosystem: Internet service providers (ISP.), operating system vendors, application developers, equipment manufacturers, search engines, and the full spectrum of enterprise and individual users. These stakeholders must work together to develop, provide, and, in the case of consumers and enterprise customers, implement cybersecurity solutions that ensure that consumers and businesses will continue to reap the benefits associated with the expansion of online services and technology innovation.

B. The Role of Government

In many ways the government's interest in cybersecurity should begin at home. All government agencies concerned about cybersecurity, which is to say, as a practical matter, each and every government agency, must work together to develop a coordinated approach to cybersecurity. The Federal government is already undertaking a wide range of activity designed to enhance security – both through individual agency initiatives as well as part of public-private sector partnerships.

AT&T believes that the government can enhance cybersecurity primarily through policies designed to identify industry best practices and incentives and promote the development of voluntary standards in areas such as identity management. Moreover, these policies should be informed and animated by several basic principles:

- Cybersecurity solutions are not a one-size-fits all endeavor. Different elements of our nation's cyber infrastructure have wide-ranging levels of cybersecurity sophistication and capabilities and, as such, face different threats, offer different solutions and have different market motivations.
- Cybersecurity requires an end-to-end approach that spans from the physical layer and the core IP network, through the application layer and device interface and to all users.

- Intelligent networks, as well as enhanced and improved software applications and features, are needed to address the evolving cyber threat. Accordingly, private-sector norms that would restrict or otherwise prohibit private sector service providers from deploying innovative threat reduction capabilities within their networks to ensure information security would compromise the trustworthiness of that infrastructure.

- The temptation to establish new, but essentially duplicative, advisory bodies and reporting requirements and mechanisms should be avoided. Additional reports and audits cannot secure cyberspace. Rather, it should be the public policy of the United States to leverage and consolidate existing public and private sector efforts, encourage the use of best practices, and to develop a way for the public and private sectors to share relevant cyber threat information in real-time.

- U.S. cybersecurity policy should encourage continued private sector innovation and investment. Most investment in the ongoing fight against cyber threats is occurring in the private sector. Private sector norms fashioned after a rigid regulatory paradigm will not encourage investment in technologies that can keep pace with the rapid evolution of global cyber threats.

- The government should be a leader in the area of education and raising awareness. Cybersecurity efforts will succeed only if they are made known to Internet users and users are incented to adopt them. In this regard, AT&T especially commends the National Initiative for Cybersecurity Education ("NICE").[3]

- U.S. cybersecurity policy should include global Internet governance strategies to address both domain name system (DNS) security and resiliency issues as well as an effective process in the event of global cyber attacks/incidents.

- U.S. cybersecurity policy must strike an appropriate balance between protecting subscriber privacy, ensuring the protection of proprietary data and securing the nation's critical infrastructure.

Policies informed by these principles should work effectively to encourage the tools and practices necessary to protect the nation's infrastructure and communications network from cyber attack and thus preserve consumer confidence in the security and trustworthiness of the Internet.

[3] http://csrc.nist.gov/nice/aboutUs.htm (last accessed Sep. 16, 2010)

II. RELIANCE ON THE INTERNET IS INCREASING, WITHOUT A CORRESPONDING INCREASE IN USER SECURITY LITERACY

As the Department observes, small, medium and large businesses, as well as consumers, will rely increasingly on the Internet and as that reliance grows, the level of cybersecurity must keep apace.[4] Indeed, consumers increasingly rely on broadband service for everyday transactions – banking, shopping, accessing electronic health records, and engaging in job training and education – and in these contexts consumer choose to share, globally, an unprecedented amount of information with trusted parties. As a result, cyber-based attacks pose serious economic and national security challenges.

The White House, in its Cyberspace Policy Review, stated that a "growing array of state and non-state actors such as terrorists and international criminal groups are targeting U.S. citizens, commerce, critical infrastructure and government. These actors have the ability to compromise, steal, change or completely destroy information."[5] Consumer Reports recently estimated that cyber-based attacks have cost $8 billion over the past two years and affected over 1.2 million users.[6]

Today, a significant proportion of Internet vulnerabilities arise from the application and device layers. In fact, IBM reports that World Wide Web ("Web") application vulnerabilities

[4] NOI at 44219.

[5] "Cyberspace Policy Review, Assuring a Trusted and Resilient Information and Communications Infrastructure," National Security Council, at 1 (2009 (NSC Policy Review).

[6] "Boom Time for Cybercrime: The economy and online social networks are the latest fodder for scams," Consumer Reports (June 2009).

make up more than half of the disclosed vulnerabilities since 2006.[7] In particular, IBM points to the vulnerability of Web application plug-ins and document formats, indicating that "[t]hree of the five most prevalent malicious Web site exploits of 2009 were PDFs, one was a Flash exploit, and the other was an ActiveX control that allows a user to view an office document through Microsoft Internet Explorer."[8] The identification and resolution of such vulnerabilities is a continuing and ongoing process.

A fundamental challenge is that many Internet users do not take the basic steps necessary to protect themselves online due to cost, lack of information (or, conversely, information overload), lack of understanding, lack of interest or use of pirated software. For example, millions of users do not diligently install security patches issued by application and operating system developers. As a recent paper by the Internet Security Alliance ("ISA"), a multi-sector trade association focused on addressing issues of information security, framed the problem, "[e]xpert testimony, including that from sophisticated government representatives, confirmed that we know how to address the vast majority of these issues, but that we are just not doing it. The key is implementation."[9] The fact that such a large number of users fail to take this step greatly exacerbates a problem, discussed further below, caused by the regular and public release of security patches, which can expose critical vulnerabilities to hackers.[10]

---

[7] IBM Security Solution, *X-Force 2009 Trend and Risk Report: Annual Review of 2009* at 5 (Feb. 2010).

[8] *Id.* at 6.

[9] Internet Security Alliance, *Implementing the Obama Cyber Security Strategy via the ISA Social Contract Model* (2009) at 4.

[10] *See* Mark Bowden, "The Enemy Within" *Atlantic Magazine* (June 2010) *available at* http://www.theatlantic.com/magazine/archive/2010/06/the-enemy-within/8098 (last visited Sep. 16, 2010).

Cyber criminals and hackers increasingly rely upon exploiting user carelessness, lack of sophistication or naïveté in ways that would be difficult or impossible to address at the network level. For instance, one of the top ten security threat trends for 2010 identified by software security expert Symantec was the use of "social engineering as the primary attack vector."[11] As Symantec explains, "more and more, attackers are going directly after the end user and attempting to trick them into downloading malware or divulging sensitive information under the auspice that they are doing something perfectly innocent."[12] From the perspective of the attacker, targeting end users directly through social engineering is attractive because it can effectively bypass network and software security protections without the need to exploit any systemic technical vulnerability.

Even where all parties are acting responsibly, the challenges of cybersecurity are compounded by the dynamic and constantly evolving nature of cyber threats. New versions of software and devices and subsequently released software patches are hacked as soon as, or even sometimes before, they become publicly available.[13] Further, the sophistication and versatility of cyber attacks is increasing exponentially and requires rapid innovation and user vigilance to address.

---

[11] *See* Kevin Haley, Symantec "Don't Read This Blog" http://www.symantec.com/connect/blogs/don-t-read-blog (Nov. 17, 2009) (last visited Sep. 16, 2010).

[12] *Id.*

[13] As the Executive Director, Strategic Initiatives, AT&T Government Solutions, explained the number and speed of "zero day attacks" or incidents occurring on the day that new security vulnerability is announced in the form of a software patch, have dramatically increased. *See* John Nagengast, Executive Director, Strategic Initiatives, AT&T Government Solutions, Remarks at the Cyber Security Workshop at 17 (Sept. 30, 2009) *transcript available at* http://www.broadband.gov/Departments/ws_26_cyber_security.pdf (last visited Sep. 16, 2010) ("Nagengast Remarks").

This is illustrated in the evolution of Conficker, a worm that emerged in 2008 and has created the largest network of infected computers (or "botnet") in the world, estimated to be in 7 million computers throughout 200 countries. Conficker has adapted quickly and has gone through several versions and upgrades. At various times, when the cybersecurity community identified a flaw in the worm, the worm was quickly updated before the flaw could be used to eradicate it.[14]

Although Conficker is among the most notorious of botnets because of its scope and sophistication, it has not, as of yet, manifested a clearly harmful agenda. Other malicious software has had much more invasive and damaging objectives. For example, a variety of criminal organizations are believed to be operating small botnets based on Zeus or Zbot, which is actually a rentable toolkit available for a fee from the developer.[15] Once installed, the malware lays dormant on the victim's PC until the user logs-in to a financial institution to engage in online banking. Zeus then inserts itself into the middle of the transaction to capture the user's login credentials, forwarding them to the criminal element operating the botnet.

Another harmful code, Koobface, was the first botnet to propagate through online social networking sites. Initially spreading over Facebook, Koobface has since adapted to infect users of numerous other sites including MySpace, Twitter, Friendster, Bebo, hi5, Tagged, Netlog,

[14] *See* Bowden, *supra* note 10.

[15] *See* Loucif Kharouni, "New ZBOT Variants Targeting European Banks" *TrendLabs Malware Blog*, http://blog.trendmicro.com/new-zbot-variants-targeting-european-banks/ (Mar. 23, 2010) (last visited Sep. 16, 2010).

fubar and myYearbook.[16] Once a PC is infected with Koobface, it is instructed to download additional components that hijack browser searches, steal encryption keys, and act as a malicious webhost to capture new victims. These threats underscore the need for cybersecurity policies that will both educate consumers and enterprise users as well as encourage the private sector to invest in innovative technologies to keep pace with the dynamic and evolving nature of cyber threats.

III. THE COMMUNICATIONS SECTOR PROACTIVELY SECURES CYBER SPACE

The communications sector understands the importance of cybersecurity to its customers and to its own economic viability, and already addresses cybersecurity in a substantial way. At AT&T cybersecurity is a constant mission, and although it cannot stop every threat targeted toward its customers,[17] AT&T considers security to be a cornerstone of the network management functions that it performs in the United States and worldwide.[18] AT&T continually monitors traffic patterns on its network to identify malicious behavior and respond to vulnerabilities and attacks. This includes monitoring traffic patterns from known origins of malicious activity as well as tracking trends on the network ports themselves.

This monitoring is complemented by an understanding of the realities of network usage. For example, network management techniques must be able to distinguish between normal

---

[16] *See* Methusela Cebrian Ferrer, "The Allure of Social Networking" *CA Security Advisor Research Blog*, http://community.ca.com/blogs/securityadvisor/archive/2009/05/31/the-allure-of-socialnetworking.aspx (May 31, 2009) (access requires password).

[17] Indeed, as the Department Notes, "it seems highly unlikely that all risks will ever be completely eliminated." NOI at 44216.

[18] AT&T defines cybersecurity as the collective set of capabilities, procedures, and practices that undertaken to protect its network and customers from the full spectrum of cyber threats assuring that the information, applications, and services AT&T provisions are secure, accurate, reliable, and available wherever and whenever they are desired. Nagengast Remarks at 17.

spikes in traffic due to external events (such as increases in Short Message Service ("SMS") traffic during American Idol), and malicious surges that could be produced by a Distributed Denial of Service ("DDoS") cyber attack.[19] Network monitoring is complemented by proactive and reactive defensive techniques aimed at ensuring that the network is as secure as possible. The result is that AT&T possesses the capability automatically to detect and mitigate many attacks within its network infrastructure before they affect service to customers.

AT&T builds upon these network management capabilities to offer a range of managed security services, tools and capabilities to its customers in the retail, small/medium business, and enterprise and public sector markets:

1. <u>Consumers</u>

AT&T provides consumers with both tools and information to protect themselves online. AT&T provides a large body of security information on its webpage, including cybersecurity tips, antivirus and firewall protections, email security, parental controls and protecting personal information.[20] AT&T also offers users easy access to up-to-date security alerts, hosts security and support discussion forums moderated by AT&T experts, and offers the ability to chat with an AT&T service representative live online.

AT&T has also taken steps to put proactive security tools into the hands of users. For example, AT&T makes its Internet Security Suite and SpamGuard available to all residential

[19] Nagengast Remarks at 18-22. *See also* FCC, A National Broadband Plan for Our Future, GN Docket No. 09-51 (AT&T Comments, June 8, 2009) at 34 (In a DDoS event, "[a]ttackers typically rent computer processing power, bandwidth, and storage online, which they then use to send a traffic overload to an online destination. This results in the destination becoming unavailable for its intended use.") (AT&T NBP Comments).

[20] *See, e.g.*, AT&T, "AT&T Support and Customer Service" http://www.att.com/esupport.

broadband Internet access customers – and for many customers these tools are provided free of charge. These suites provide a full array of consumer antivirus, firewall, and spam protection applications, which help users guard against cyber threats and unwanted communications. Moreover, AT&T continues to explore new approaches to communicate with users about known cybersecurity issues to empower them to be proactive in minimizing the damage that a cyber attack might produce. For example, if AT&T detects certain abnormal traffic patterns associated with a customer's connection, AT&T emails the customers that may be affected by a fast flux"[21] or other type of malicious attacks and provides them with information on the steps they can take to mitigate the problem.

2. <u>Small to Medium Sized Businesses</u>

AT&T offers an array of services that can aid small and medium sized businesses. For example, AT&T makes available a collection of security tools to our business class DSL high speed internet access customers, many of whom are small businesses, including anti-spyware, anti-spam, anti-virus, pop-up blocker, and firewall and e-mail virus protection.

Similarly AT&T provides a suite of managed security services to customers of our Managed Internet Service (MIS), which are typically small and medium-sized businesses. This includes, among other things, network and premises-based firewalls; web security including URL blocking and application filtering of malware for web and IM traffic; real-time reporting of service results and customer self administration via a web portal; a secure e-mail gateway service

[21] A "fast flux" refers to a technique used by botnets to hide malware delivery sites behind an ever changing network of compromised hosts acting as proxies. The technique works by associating numerous IP addresses with a single qualified domain name where IP addresses are swapped in and out with extremely high frequency.

that includes anti-virus, anti-spam, and content filtering services for inbound and outbound e-mail messages as well as message archiving and encryption options; intrusion prevention service that provides customers the ability to detect endpoints on their network that are propagating threats or violating their security policy and web security that provides network based web content filtering and screening for malware and spyware.

Additionally, AT&T makes available consulting services to small and medium sized businesses that provide assessments to identify vulnerabilities and threats likely to compromise business operations and also determine how well the client's security conforms to established industry norms. Virus and malware scanning for desktops can be provided as a hosted service in the network to stop malicious traffic before it ever reaches the customer's premises. Likewise, firewalls and DDoS defense can be deployed within the network abstracted from local machines. These managed security options may be more cost effective for small and medium business than in the past, and as discussed below, may provide even more protection since cybersecurity is managed centrally and automatically by skilled technicians, thus eliminating the risk that certain users' desktops will be compromised due to user inaction in downloading software upgrades.

3. Large Businesses

With respect to its enterprise customers, AT&T offers a comprehensive package of managed security services under its suite of Security and Business Continuity Services, which assesses vulnerabilities, helps provide network security, detects attacks, responds to suspicious activities, and provides for non-stop operations. These security services include encryption, firewall protection, intrusion detection, authentication, and other services designed to prevent attacks, as well as remote backup and recovery solutions that help ensure continuity of

operations and a quick recovery when attacks or other business disruptions occur. To assist business users in understanding AT&T's comprehensive approach to security and to maximize the benefits of the various security solutions available to them, AT&T provides the AT&T Information & Network Security Customer Reference Guide, which contains an extensive description of AT&T's cybersecurity practices and is attached hereto at Appendix A.

4. Government Solutions

AT&T's market-leading security services are also implemented in the government sector. Recently, AT&T Government Solutions became the first "Networx" contract holder to receive Authority to Operate ("ATO") from the General Services Administration ("GSA") for implementation of Managed Trusted IP Services ("MTIPS").[22] The ATO enables AT&T to offer its cloud-based cybersecurity services to federal agencies across the entire United States Government. AT&T Government Solutions has already confirmed MTIPS task orders with ten federal agencies, including the Federal Trade Commission and the Environmental Protection Agency.[23]

However, as is recognized by the Department, critical infrastructure and key resources are only one facet of the overall operational dynamic of the Internet, which also includes operating systems, applications, devices and human beings. To be effective, cybersecurity

[22] *See* Press Release, AT&T Inc., AT&T Is the First Networx Contract Holder to Receive Authority to Operate a Trusted Internet Connections (TIC) Compliant Service (June 2, 2010) *available at* http://www.att.com/gen/press-room?pid=17995&cdvn=news&newsarticleid=30856&mapcode=enterprise (last visited Sep. 20, 2010).

[23] See Press Release, AT&T Government Solutions Wins $29 Million Task Order from the U.S. Environmental Protection Agency (Apr. 1, 2010) *available at* http://www.corp.att.com/gov/newsevents/press_releases/press_040110.html (last visited Sep. 20, 2010), *and* Press Release, AT&T Government Solutions Wins $5 Million Award from the Federal Trade Commission (Feb. 11, 2010), *available at* http://www.corp.att.com/gov/newsevents/press_releases/press_021110.html (last visited Sep. 20, 2010).

requires the efforts of entities at every layer of the interconnected and interdependent Internet ecosystem, including the individual consumer. Therefore network based solutions alone are not sufficient to protect against cyber threats, as they secure only one aspect of the entire Internet ecosystem. Absent further comprehensive efforts, cyber attacks will continue to occur at other levels of the Internet ecosystem, typically the user level.

There are also a wide array of public sector efforts and public-private partnerships focused on enhancing cybersecurity. The public sector alone is involved in numerous initiatives on cyber safety, e.g., military (offensive/defensive cyber operations involving nation/state sponsorship); intelligence (providing attack sensing and warning capabilities); law enforcement (investigating and prosecuting cyber crime); and public/private sector partnerships (coordinating information sharing, risk assessments, and risk mitigation and remediation).

As noted by the NOI, there are various federal entities/agencies involved in initiatives related to cybersecurity including the White House's Cybersecurity Coordinator, the Office of Management and Budget ("OMB"), the Department of Homeland Security ("DHS"), the Department of Defense ("DOD") the Federal Bureau of Investigation ("FBI"), the National Science and Technology Council, the National Institute of Standards and Technology ("NIST"), and the National Telecommunications and Information Association ("NTIA"). As discussed in Appendix B each of these entities has their own role in defending cyber space and as such is pursuing a range of mitigation strategies. In addition, the public sector has partnered with the private sector on many cyber initiatives. As Melissa Hathaway, former Acting Senior Director for Cybersecurity at the National Security Council, pointed out, "a recent cursory review identified more than 55 government initiated

private-public partnerships in the area of cybersecurity. Over 30 of these emerged out of the DHS alone."[24] AT&T participates in or coordinates with many partnerships with government entities, both within the United States and internationally including the National Security Telecommunications Advisory Committee (NSTAC), USSS Cyber Crimes Task Force, FBI's InfraGard®, the Communications Security, Reliability and Interoperability Council (CSRIC), successor to the Network Reliability and Interoperability Council, Computer Emergency Response Team/Coordination Center (CERT/CC) – a global initiative, Communications Security, Reliability and Interoperability Council (CSRIC), Internet Engineering Task Force (IETF) and the World Wide Web Consortium (W3C) – global initiative, Forum of Incident Response and Security Teams (FIRST) – a global initiative, Communications - Information Sharing and Analysis Center (Communications-ISAC), and ATIS - Network Reliability Steering Committee (NRSC).

The multitude of federal programs and agency initiatives related to cybersecurity can create inefficiencies and, at times, be counterproductive. A recent U.S. Government Accountability Office ("GAO") report on the Comprehensive National Cybersecurity Initiative found that "[c]urrently, agencies have overlapping and uncoordinated responsibilities for cybersecurity activities that have not been clarified."[25] The sheer number of uncoordinated

[24] *See* Melissa Hathaway, "Why Successful Partnerships are Critical for Promotion Cybersecurity" http://www.thenewnewinternet.com/2010/05/07/why-successful-partnershipsare-critical-for-promoting-cybersecurity/ (May 7, 2010)(last visited Sep. 16, 2010).

[25] GAO, *Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative* at 2 (March 2010) *available at* http://www.gao.gov/new.items/d10338.pdf (last visited Sep. 16, 2010)

programs that attempt to address various aspects of cybersecurity presents the risk of diluting the impact of any one program.

V. HOW CAN GOVERNMENT POLICIES STRENGTHEN CYBERSECURITY?

1. Consolidate Existing Efforts

The private sector, as well as the public sector, would be better served by devoting their focus and limited resources to fewer, more coordinated programs. The GAO's July 2010 report on Critical Infrastructure Protection echoes this recommendation, "[b]ecause the private sector owns most of the nation's infrastructure – such as banking and financial institutions, telecommunications networks, and energy production and transmission facilities – it is vital that the public and private sectors form effective partnerships to successfully protect these cyber-reliant critical assets from a multitude of threats including terrorists, criminals, and hostile nations."[26]

Therefore, rather than adding another layer, or multiple layers, of complexity to the growing number of U.S. cybersecurity government initiatives, the government should help coordinate and inform existing industry efforts, public-private partnerships, and federal programs.

2. Preserve Private Sector Flexibility to Respond to Threats

Today, most ISPs monitor and analyze traffic flows to safeguard their networks and customers from harm. This flow information is a valuable indicator of changes in traffic patterns and characteristics which are indicative of suspicious cyber activity. When a cyber-security

[26] GAO, *Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed* at 1 (July 2010).

event is identified in its network, AT&T conducts forensics analysis to determine the source of the threat and take appropriate action.[27] In light of the ever-changing nature of cyber threats, network operators must retain the flexibility to react quickly and decisively when a vulnerability or attack is detected. Therefore, whatever policies are put in place, government should make it a priority to preserve private sector flexibility to act proactively and respond quickly to cyber security threats without being hamstrung by prescriptive regulation or other requirements that could slow response times and exacerbate cyber incidents.

Moreover, while networks have a significant role to play in response to cyber threats, networks are not in and of themselves the root cause of cyber incidents. As federal agencies look to establish policies to secure the CIKR sectors, a more pressing area where the Task Force could provide assistance is in the development of policies that will encourage better software development practices as discussed in more detail below.

Finally, government policies should recognize that "disconnecting" any particular element of the Internet could have a major impact on the function of critical infrastructures and Internet services. These policies should instead encourage collaborative processes between the public and private sectors to assess attacks and develop the best mitigation strategies.

3. Improve Strategic Information Sharing

Access to accurate, real time threat information is vital to all parties' efforts at combating cyber attacks. Building a mechanism where both the public and private sector can pool resources and information, in real time, will strengthen the nation's defenses against cyber attacks and

[27] AT&T does not inspect the contents of Internet traffic as it performs the traffic flow monitoring and information analysis necessary to fulfill this function. For a more thorough description of AT&T's monitoring and notice process, *see* FCC, Framework for Broadband Internet Service, GN Docket No. 10-127 (AT&T Comments, July 15, 2010) at 77.

allow for quick action and coordinated responses. While there have been attempts at collaboration and sharing to improve cyber security, not all have been successful. More such programs continue to be proposed, but few, if any, tackle the core issue: how to detect, analyze, and mitigate cyber attacks in near real-time.

Government policy should encourage the exchange of security-relevant information between various Internet stakeholders building upon existing government programs that includes all of the relevant cyber information from government networks, communications networks, other CIKR sectors and key non-CIKR sector participants and a structure to facilitate the coordination of response activities with government entities such as US CERT/NCC at DHS, the NSA National Threat Operations Center, and U.S. Cyber Command. U.S. CERT/NCC, in turn, could serve as a hub for sharing relevant information with other government agencies, including the Cyber Crimes Unit at the Department of Justice, the FBI's National Cyber Investigations Joint Task Force, and the Department of Defense Cyber Crime Center (DC3), as well as providing broad distribution of alerting information to other impacted parties. As information sharing programs are be enhanced to improve cybersecurity, private sector stakeholders must be encouraged to continue to make significant investments in their capabilities to detect, alert and mitigate cyber threats both to protect their networks and customers. At AT&T, investment in these areas is predicated upon AT&T's ability to offer a suite of managed security services, particularly to the enterprise and medium business markets. Any government facilitated information sharing program must be constructed in such as way to avoid undercutting the value proposition for these services or they will have the unintended consequence to remove the incentive for continued innovation in security capabilities at the network level.

A critical first step to the establishment of any information sharing program should be to determine what level of information should shared between which entities, which may differ between CIKR sectors, CIKR sector members and non-CIKR sector members. Moreover a mechanism should be put in place to ensure that any data exchanged between the public and private sector can be properly protected so that the source is not attributable. Similarly if the data is sensitive, proprietary or confidential in nature, the content may need to be modified to protect sensitive information. Finally any information sharing must be done in a way to avoid providing a roadmap to cyber-criminals.

4. Ensure Market Incentives Supporting Continued Investment and Innovation

The private sector, and in particular the communications sector, through substantial investment and innovation, has developed sophisticated cybersecurity practices—all without the burden of prescriptive regulation. These cybersecurity practices developed in the communications sector because communications services providers understand that those service providers which operate the most reliable and secure networks/facilities stand to gain the most in an open marketplace. Compromised networks are inherently unreliable and produce a lack of user trust in the network, which inevitably leads users to reject the providers' services. This dynamic provides substantial economic incentive for service providers to continually build greater protections into their networks for the users that rely on it.

Indeed, users of communications services increasingly demand protection from cybersecurity threats. Large business and government users, in particular, demand information about the cybersecurity practices of their communications service providers and adequate assurances that their sensitive data will be protected. In order to meet the demand for

information related to its cybersecurity practices, AT&T developed and distributes to business and government users the AT&T Information & Network Security Customer Reference Guide.[28] These business and government users also often demand contractual commitments that their information is secure. The Federal Government itself seeks these assurances by requiring communications service providers to obtain authority from the GSA to offer their MTIPS to federal agencies. Improvements to networks and cybersecurity practices that communications providers make in response to these market incentives also benefit individual consumers.

Even the prospect of a cyber attack that adversely affects individual consumers provides substantial incentives for communications providers to protect their networks. Successful cyber attacks produce a myriad of damages to communications service providers. Cyber attacks may cause service outages or the disclosure of confidential consumer information, either of which could cause consumers to switch service providers.[29] In addition to foregone revenue from lost customers, communications service providers also incur significant monetary costs to notify customers of an illicit disclosure.[30]

---

[28] Attachment A. While communications providers may provide users with information about cybersecurity measures the providers take to protect user information, providers should keep certain security information out of the public sphere and thus out of the hands of potential cyber criminals.

[29] Bruce S. Schaeffer, Henfree Chan, Henry Chan and Susan Ogulnick, "Cyber Crime and Cyber Security: A White Paper for Franchisors, Licensors, and Others," Wolters Kluwer Law & Business, *available at* http://business.cch.com/franlaw/cybercrime_whitepaper.pdf (last visited Sep. 16, 2010) ("*Cyber Crime White Paper*").

[30] *Cyber Crime White Paper* at 4.

Further, cyber attacks may lead to costly litigation, regulatory investigations, contract disputes, and reputation damage.[31] AT&T is one of multiple providers driven to ensure cybersecurity protection and innovation. AT&T faces significant competition in the managed security services market from numerous other entities, including IBM, British Telecom, Orange, Symantec, T-systems, Tata Communications, Verizon and Telefonica Multinational Solutions. For example, although AT&T received the first GSA authority to offer its MTIPS to federal agencies,[32] other major industry players, such as Qwest, Sprint and Verizon, have also received awards from DHS to be MTIPS providers.[33] The fierce competition in this area drives innovation and efficiency, as communications service providers must constantly strive to deliver the best security services to their customers as quickly as possible.

Policy makers should therefore continue to promote continued investment and competition in the private sector to make our technology, systems, and networks more robust and secure. As the Department considers how to improve cybersecurity within the private sector, it should do so through the development and adoption of industry best practices. A more prescriptive approach will never keep up with the dynamics of technology and the rapid

[31] *Cyber Crime White Paper* at 3. *See also* Ina Fried, "Lawsuits Filed Over Sidekick Outage," CNET News (Oct. 14, 2009), *available at* http://news.cnet.com/8301-13860_3-10375240-56.html (last visited Nov. 10, 2009) (describing lawsuits filed against T-Mobile and Microsoft relating to data loss caused by a service outage to the Sidekick phone); "AT&T E-mail Apologizes for iPad Data Breach, cnet news (June 13, 2010), *available at* http://news.cnet.com/8301-1009_3-20007564-83.html (last visited Sep. 16, 2010).

[32] *supra* note 22.

[33] *See* Jason Miller, "GSA, DHS Approve First Governmentwide Cyber Provider" *Federal News Radio* (June 7, 2010) *available at* http://www.federalnewsradio.com/?sid=1971233&nid+35 (last visited Sep. 16, 2010).

evolution of global threats. Indeed, there are significant public policy and practical reasons to believe that prescriptive norms would actually reduce the effectiveness of industry's cyber security efforts in the following ways:

- Mandated best practices may result in a static solution to a dynamic problem. Complying with the program's fixed standards, even if broadly drafted, could limit the flexibility of private sector entities to respond to evolving threats and chill the incentive to innovate.

- Standards set by government could establish a "least common denominator" of security measures that any industry member could satisfy and which would be practically meaningless.

- Adopting public standards could also expose network vulnerabilities, providing a map for cyber criminals.

- Resources necessary to develop comply with a prescriptive program would distract providers from participating in more effective government programs and public-private cyber security efforts.

- Even if these burdens are minimized, it is not clear whether any marginal cyber security gains resulting from the program would justify the significant logistical challenges involved in its adoption. In a recent paper on cyber security strategy, ISA directly addressed the low likelihood of success of a government-mandated cyber security program. As ISA points out "[a] system of regulatory mandates applied to the broad and diverse private sector is unlikely to be effective in generating . . . substantial improvements in private sector cyber security. In fact, such a system would almost certainly be counter-productive, from both a national economic, as well as a national cyber security perspective."[34]

Government should generally avoid policies that promote mandates, require that specific standards be adopted, or establish certification-based regimes. At the same time, however, the government does have a series of tools at its disposal to incent the adoption of best practices in the event that it believes that market forces are not driving towards desired outcomes:

- Implement appropriate best practices across government entities.

[34] *Supra* note 9 at 4.

- Leverage its purchasing power to stipulate cyber security requirements in the government procurement process – thus creating market-based incentives for the adoption of private sector best practices.

- Promote incentives for the adoption of best practices across industry sectors such as liability protections and tax incentives.

5. Encourage Development of Industry Best Practices

Government should rely upon market forces to ensure innovation in cybersecurity, and government can and should play a substantial role in convening industry stakeholders to facilitate the development of cyber security best practices, particularly with regard software design. While competitive pressures have resulted in communications providers' ever evolving efforts to offer effective cyber security solutions, it is less clear if the same market dynamics and incentives exist in the case of software application design. The Department should therefore examine this area with care, and in particularly address the security concerns created by poorly written or insecure applications or operating system software.

Indeed, perhaps the most effective step government can take to improve cyber security is to create the proper incentives for, and ensure the development of, best practices that will improve software development and encourage the use of more secure code. Many software vendors rush software to the marketplace only to discover security vulnerabilities after the fact, followed by a series of patches to correct for the coding errors. This pattern is unsustainable. Security must become a priority in the software development process.[35]

A potential example of best practices development is the effort the Department has conducted through the National Institute of Standards and Technology's ("NIST") in regards to smart grid cyber security strategy requirements. This effort has been focused upon the

[35] An analogy may be drawn to developments in online privacy, as "privacy by design" is embraced by more and more entities throughout the Internet ecosystem. Privacy by design is used to generally describe the integration of privacy considerations into business models, product development cycles and new technologies. A similar focus should be placed upon security in throughout the software development cycle.

establishment of guidelines and standards for cyber security that will enable efficient and effective Smart Grid deployment. The guidelines and standards being discussed are not requirements but are providing guidance on how to constructively address the cyber security challenges that Smart Grid presents.[36] A similar effort could be undertaken in regards to software or website development that, while not mandating particular solutions or technology, facilitates an information exchange between developers on current practices to secure newly developed software and applications. This task would of course be challenging in that there are infinitely more software developers, from large corporations to individuals, writing code today. However aggregating information on current software development practices as it relates to security and potentially educating developers on these practices could help improve upon software design.

Within the communications sector itself there are already multiple examples of the government playing a role to convene industry stakeholders. For example the FCC established the Communications Security, Reliability and Interoperability Council ("CSRIC") in 2009.. CSRIC working group 2A is taking a fresh look at cyber security best practices, intending to update the best practices that were previously developed by the Network Reliability and Interoperability Council ("NRIC") several years ago, including focusing on all segments of the communications industry and public safety communities. CSRIC Working Group 8 (WG8) is looking into Internet Service Provider (ISP) network protection practices, investigating current practices that ISPs use to protect their networks from harm caused by the logical connection of computer equipment, as well as desired practices and associated implementation obstacles. The intent of WG8 is to address techniques for dynamically identifying computer equipment that is

[36] The NIST guidelines are fairly extensive and the exact extent of their implementation is yet to be determined. It is therefore critical that government at any level resist interpreting them as a mandate that discourages industry stakeholders from continuing to develop best practices.

engaging in a malicious cyber attack, notifying the user, and remediating the problem, and to conclude with a set of proposed recommendations to the FCC.[37]

While the best practices developed at CSRIC would be voluntary for industry participants, the FCC is playing a convening role to facilitate information sharing around current security practices. This process of benchmarking and recognizing existing practices allows sector participants to better understand where they stand *vis-a-vis* their competitors and facilitates the development of appropriate market based incentives as discussed above.

6. Increase Consumer Awareness and Education

The Department could make an immediate and beneficial impact by participating with other government agencies and the privacy sector in a strategic consumer education campaign with the goal of directly impacting one of the key struggles in cybersecurity—the low rate of user adoption of proven protection mechanisms. This is one area where the government could positively influence the trajectory of cybersecurity by engaging in a comprehensive education and outreach campaign to inform consumers about security best practices and how to protect themselves and their sensitive information. In this regard, AT&T especially commends the National Initiative for Cybersecurity Education ("NICE").[38]

Significant vulnerabilities exist and attacks often spread solely because many users neglect to take appropriate precautions to protect their devices. Indeed, according to a four-year study conducted by Verizon, 87% of data breeches were considered avoidable through the use of reasonable controls.[39] The tools users need in order to protect themselves are widely available,

---

[37] *See* CSRIC Charter, *available at* http://www.fcc.gov/pshs/docs/advisory/csric/CSRC_charter_03-19-2009.pdf (last visited Sep. 20, 2010).

[38] *Supra* note 3.

[39] Verizon Business Risk Team, *2008 Data Breach Investigations Report* at 2-3 *available at* http://www.verizonbusiness.com/resources/security/databreachreport.pdf (last visited Sep. 16, 2010).

but they need to be used and kept up to date to be effective. Unless users develop and implement healthy computing practices, the cyber security efforts undertaken by the communications industry are inevitably undermined. For example, if users were more diligent in keeping their Microsoft Windows operating systems up-to-date, the Conficker worm would not have spread as significantly.[40] Further the National Cyber Security Alliance ("NCSA"), of which AT&T is a partner, recently reported survey results indicting that 90% of respondents stated that they want to learn more about keeping safer on the Internet; when asked why they don't always do all the things they can or should do to stay safer online, one of the most cited factors was that respondents simply lacked the information or knowledge.[41]

AT&T and other communications service providers work with a variety of external organizations to promote online safety education and awareness.[42] To augment those industry efforts, the government should engage in a consumer education program to communicate to users a few simple steps—such as using antivirus software, diligently applying security patches, and operating only legally licensed applications and operating systems—that, if adopted, would make a dramatic difference in overall cybersecurity. Such government efforts have been quite effective in other contexts. For example, the FCC demonstrated the success of its consumer outreach capabilities in the lead-up to the digital television transition, wherein the FCC implemented a coordinated and strategic educational campaign that succeeded in delivering essential information about the transition to millions of Americans. The Department should partner with other agencies to coordinate a comprehensive education/awareness effort to alert

---

[40] *See, e.g.*, Bowden, *supra* note 10.

[41] *See* Press Release at http://staysafeonline.mediaroom.com/index.php?s=43&item=62 (last visited Sep. 20, 2010).

[42] *See, e.g.*, AT&T NBP Comments, at 40-41.

consumers to the wealth of useful information, links, and free tools for consumers to ensure their devices are secure.

For example, NCSA is participating in a public-private partnership between DHS and a broad cross-section of industry representatives including major hardware, software, defense, research and telecommunications companies. Through its website StaySafeOnline.org and its other efforts, NCSA strives to "educate and therefore empower a digital society to use the Internet safely and securely at home, work, and school, protecting the technology individuals' use, the networks they connect to, and our shared digital assets."[43] By coordinating with an existing effort like NCSA, the Department can ensure that the public is receiving a clear, uniform and effective message.

7. Encourage the Adoption of New Technologies That May Improve Security Such as Identity Management

Another area where the Department can influence cybersecurity is through the encouragement of new technologies, in particular related to identity management services. Adoption of identity management by consumer and enterprise users within the private sector has been low due to the complexity of the Internet ecosystem, lack of knowledge and difficulty of use. In addition, identity management has been historically focused on traditional identity theft issues. To aid in the successful implementation of innovative privacy tools, which in turn will strengthen overall cybersecurity efforts, the government should work with the private sector to promote expansion of the field to address additional privacy concerns and the development of user-friendly tools and interfaces and to increase education of both consumers and members of the ecosystem.

[43] *See* National Cyber Security Alliance, "About Us – STAYSAFEONLINE.ORG" http://www.staysafeonline.org/content/about-us (last visited July 2, 2010).

In the online privacy space, AT&T has supported the further development of user-centric identity management tools ("IDM tools"), an emerging technology that can enhance consumer privacy online by giving consumers the ability to determine how much of their identity to reveal, when and to whom. As AT&T detailed in its December 21, 2009 comments to the FTC's Privacy Roundtables Project[44] the two most prominent IDM tools, OpenID[45] and Information Cards[46] put the user in control of all identity-based interactions and potentially provide a uniform user-driven approach to data collection and use, including the kinds of information generally valuable to advertisers. Continued industry development and exploration of these and other user-driven identity technologies could potentially have numerous benefits for consumers and industry stakeholders:

- Could offer users the ability to control all identity-based interactions and the login becomes a one-click experience.

[44] FTC, Privacy Roundtables Project, No. P095416, Comments of AT&T (Dec. 21, 2009).

[45] OpenID is a Web registration and single sign-on protocol that lets users register and log on to OpenID-enabled websites using their chosen OpenID identifier. With OpenID, a user can operate his/her own OpenID service (such as a blog), or he/she can use the services of a third-party OpenID provider (for example, most major Web portals, such as AOL, Goggle, and Yahoo!, now offer OpenID). One key advantage of OpenID is that it requires no client-side software – it works with any standard Internet browser. OpenID is a community-developed open standard hosted by the non-profit OpenID Foundation.

[46] Information Cards are a new approach to Internet-scale digital identity in which various aspects of a user's identity, whether self-created or established by third-party identity providers (e.g., employer, financial institution, school, government agency, etc.) are uniformly represented as visual "cards" in a software application called a card selector. Cards can contain information you may commonly share with a website, like name, address, interest information, etc., and can contain data relevant to and able to be shared with advertisers and retailers, such as loyalty club membership information or interest profile information. The cards themselves may be stored on the same computer as the card selector, on a mobile device, or "in the cloud." Cards may be exchanged with websites using a variety of protocols and formats. All card selectors support at least the IMI protocol developed by OASIS IMI TC 7; however, Information Cards are now being adapted to other protocols as well (including OpenID). Information Card technology is developed and promoted by the non-profit Information Card Foundation,

- Could offer consumers enhanced consumer privacy by providing
    - a single place to establish privacy preferences,
    - the ability to use pseudonyms,
    - the possibility of minimum disclosure of personal, identifying information, and
    - the promise of consumer choice regarding the nature and amount of data to be shared, when it will be shared, and the timing and manner of updating and withdrawing data.

- Could offer websites a secure, standardized means of authenticating users.

- Could offer websites and advertisers a uniform way to access a user's privacy preferences, as well as other information about the user that would allow for personalization of the Internet experience.

Because of the potential value of these technologies to the consumer online experience, and the added potential to further protect consumer privacy data and security, we encourage NTIA to support the use and future development of these technologies by the industry.

A recent draft report by the White House sets out to further advance this important goal - "to establish an ecosystem of interoperable identity service providers and relying parties where individuals have the choice of different credentials or a single credential for different types of online transactions"[47] as a way to combat the alarming rise of online fraud, identity theft and misuse of online information. The White House Report calls this environment the "Identity Ecosystem" – "an online environment where individuals, organizations, services, and devices can trust each other because authoritative sources establish and authenticate their digital identities."[48] While privacy and voluntary participation are two pillars of the proposed Identity Ecosystem,[49] another, and probably the most important pillar, is interoperability:

---

[47] National Strategy for Trusted Identities in Cyberspace, Creating Options for Enhanced Online Security and Privacy- Draft, June 25, 2010 at 6. ("Strategy").

[48] *Id*. at 1.

[49] *Id*.

> The Identity Ecosystem leverages strong and interoperable technologies and processes to enable the appropriate level of trust across participants. Interoperability supports identity portability and enables service providers within the Identity Ecosystem to accept a variety of credential and identification media types. The Identity Ecosystem does not rely on the government to be the sole identity provider. Instead, interoperability enables a variety of public and private sector identity providers to participate in the Identity Ecosystem.[50]

The interoperability concept rests on two ideals: 1) widespread standardized and reliable credentials and identity media; and 2) trust - if an individual, device or software presents this credential, any qualified relying party could accept the credential as proof of identity and attributes.[51]

Importantly, the Strategy challenges the government to be the first adopter and first enabler of the Identity Ecosystem and envisions the designation of a lead federal agency to ensure its implementation – "actively seek interagency collaboration, harness multi-disciplinary and multi-sector contributions and provide collective thought leadership across Government in order to harmonize and integrate various public and private sector policies and efforts. [52]

The Department should embrace the challenge outlined in the Strategy and recommend that government agencies lead by example and develop their own best practices for incorporating privacy by design principles and data protection in the design of their online services, consistent with the Strategy and the President's recent Open Government Initiative for government online

---

[50] *Id*. at 2. The Draft Report analogizes service providers' acceptance of a variety of credential and identity media to the way bank ATMs accept credit and debit cards from different banks. *Id*. at 8. *See also*, United States Senate, Committee on Commerce Science and Transportation, Hearing: Consumer Online Privacy (Testimony of Dorothy Attwood, Senior Vice President and Chief Privacy Officer, AT&T July 27, 2010) at 3. *Available at* http://commerce.senate.gov/public/index.cfm?p=Hearings&ContentRecord_id=0bfb9dfc-bbd7-40d6-8467-3b3344c72235&Statement_id=4d9c66e7-082f-4639-9af4-b32f22a661b9&ContentType_id=14f995b9-dfa5-407a-9d35-56cc7152a7ed&Group_id=b06c39af-e033-4cba-9221-de668ca1978a&MonthDisplay=7&YearDisplay=2010 (last visited Sep. 20, 2010).

[51] Strategy, *supra* n.46. at 8.

[52] *Id*. at 26.

services.[53] Through those initiatives, government and industry could encourage digital identity providers to further enhance IDM tools through a range of network, web and mobile based identity solutions and interoperable standards, in order to allow consumers to access and interact with government content using log-in and other personal information they have provided to digital identity providers. Enabling consumers to control the collection and use of their personal data in this manner, particularly as they navigate multiple government websites, would materially advance consumer privacy objectives and help maintain the security of these consumers' data.

8. Strengthen International Cooperation

The Department should adopt policies encouraging the development of a U.S. strategy for global coordination to address cybersecurity issues. However, formalizing such protocols in a treaty, without private sector interests and participation, is unworkable and could be devastating to current private sector actions to combat cyber threats.

As the White House recently pointed out, working with our international partners is the best way to move international cyber protections forward:

> The Nation needs a strategy for cybersecurity designed to shape the international environment and bring like-minded nations together on a host of issues, such as technical standards and acceptable legal norms regarding territorial jurisdiction, sovereign responsibility, and use of force. International norms are critical to establishing a secure and thriving digital infrastructure. In addition, differing national and regional laws and practices – such

[53] Lipowicz, *Trust, but Let Google Verify: Companies Join Government in Identity Authentication Experiment*, Federal Computer Week (Sep. 2009) *available at* http://fcw.com?Articles/2009/09/09Open-identity-groups-collaborate-with-federal-agencies.aspx? (last visited Sep. 16, 2010).

> as laws concerning the investigation and prosecution of cybercrime; data preservation, protection, and privacy; and approaches for network defense and response to cyber attacks – present serious challenges to achieving a safe, secure and resilient digital environment. Only by working with international partners can the United States best address these challenges, enhance cybersecurity, and reap the benefits of the digital age.[54]

Cybersecurity issues, both domestic and international, should be addressed through multi-stakeholder cooperation. In developing international standards and strategies, the government should focus on educating, advising and assisting other Federal and international governmental cybersecurity initiatives; provide for direct private sector participation; and establish international partnerships to enable real-time global coordination in addressing cyber attacks. The administration should develop polices for global Internet governance that encourage public and private sector entities to remain involved in international Internet dialog.[55]

The benefit of this type of international cooperation amongst stakeholders is evidenced on the law enforcement front. The FBI led an international law enforcement group which dismantled several international cyber criminal organizations. These activities include the take-down of a Russian-led organization which penetrated over 300 financial institutions, including the Royal Bank of Scotland (RBS), where the actors coordinated the withdrawal of nearly $10 million in less than 24 hours from more than 2,100 ATMs in 280 cities around the world[56] Another FBI investigation brought down the perpetrators of a scheme that executed more than $4 million of unauthorized transfers from over 5,000 victims' accounts; this investigation

---

54 *NSC Policy Review, supra* n.5 at IV.

55 NSTAC recently recommended the development of international cyber-incident warning and response capabilities. Development of these capabilities would provide a scalable, coordinated international structure for all stakeholders to respond to an international cyber threat. NSTAC, NSTAC Response to the Sixty-Day Cyber Study Group (Mar.12, 2009) at 21.

56 *Id*

culminated with the arrest of more than 100 conspirators by the FBI and Egyptian law enforcement. [57] Finally, a third FBI investigation, conducted jointly with Italian authorities, led to the arrest of five Pakistani nationals who operated an Italian-based money transmitter company that supported the 2008 Mumbai attacks by funding the terrorist acts and activating the VoIP (Voice over IP) accounts that the terrorists used during the attacks.

Continued focus on coordination and cooperation among domestic and international stakeholders – both public sector and private sector alike – is the best way to make progress on identifying and responding to global cyber threats.

9. Enhance Privacy Protections as a Component of Safeguarding Security

One of the biggest challenges with enhancing security is the perception that enhancing security, and in particular sharing information between the public and private sectors, inherently reduces reducing individual privacy. Any programs that involve the sharing of information between the public and private sector must strike the right balance between protecting subscriber privacy, ensuring the protection of proprietary data and securing the nation's critical infrastructure. As discussed above the U.S. government could play a key role in striking this balance by supporting the development of identity management systems and industry privacy control tools through establishing broad goals for these technologies. Moreover while at the same time enacting new programs designed to enhance security government can take additional steps to modernize existing laws, such as the Electronic Communications Privacy Act ("ECPA") that would ensure that as additional security measures are taken that adequate protections are in

[57] *Id*

place to ensure individual privacy. AT&T is a member of Digital Due Process, which has started a dialogue about the need for potential reform of the Electronic Communications Privacy Act in light of technological advances and changes such as cloud computing. [58]

VI. CONCLUSION

In light of the varied, nefarious and adaptive nature of the threat, the greatest weapons in the cybersecurity fight are innovation and flexibility, and preserving these dynamics should be paramount to any effort. The Department should take the lead in establishing policies that will encourage private sector investment in such innovation and flexibility, as set forth above.

Respectfully Submitted

/s/

Keith M. Krom
Theodore R. Kingsley
AT&T Inc.
1133 21st Street, N.W.
Washington, D.C. 20036
(202) 463-4148
(202) 463-4627

September 20, 2010

[58] *See* www.digitaldueprocess.org (last visited Sep. 20, 2010).