

# TechAmerica

WHERE THE FUTURE BEGINS

---

THE ASSOCIATION OF COMPANIES DRIVING INNOVATION WORLDWIDE

Statement of

Phillip J. Bond  
President and CEO  
TechAmerica

Cybersecurity: Assessing the Immediate Threat to the United States

Before the

Subcommittee on National Security, Homeland Defense and Foreign Operations

Committee on Oversight and Government Reform  
U.S. House of Representatives

May 25, 2011

Good afternoon, Chairman Chaffetz, Ranking Member Tierney and Members of the Subcommittee. My name is Phillip Bond, and I am President and CEO of TechAmerica. Thank you for giving me the opportunity to present the technology industry's views on the cybersecurity threats that we are facing today. Technology cuts across all sectors of the economy – from financial services, telecommunications and the bulk of the electric power industry to critical government services – and the majority of the population relies on technology in their everyday lives. As such, we are mindful that security has to be built in from the very beginning and that we must continue to innovate aggressively in order to stay ahead of cyber criminals. We also see cybersecurity as a vital part of continuing economic growth and economic security, innovation, and U.S. competitiveness, as well as national and homeland security.

TechAmerica is the leading voice for the U.S. technology industry, which is the driving force behind productivity growth and jobs creation in the United States and the foundation of the global innovation economy. Representing approximately 1,200 member companies of all sizes from the public and commercial sectors of the economy, it is the industry's largest advocacy organization. It is also the technology industry's only grassroots-to-global advocacy network, with offices in state capitals around the United States, Washington, D.C., Europe (Brussels) and Asia (Beijing). TechAmerica was formed by the merger of AeA (formerly the American Electronics Association), the Cyber Security Industry Alliance (CSIA), the Information Technology Association of America (ITAA) and the Government Electronics & Information Technology Association (GEIA).

TechAmerica's extensive track record of addressing issues related to cybersecurity is well documented, and we continue to maintain a robust program specifically focused on this critical area. Additionally, many of our member companies provide leading, state-of-the-art products and services that are instrumental in warding off cyber attacks. However, it is clear that cyber criminals respond rapidly to our technological advancements and are consistently developing new ways to try to infiltrate our private and public systems. In the Symantec Corporation's Internet Security Threat Report it was revealed that there was a 93 percent increase in web attacks, per day, in 2010 compared to 2009, with an average of 260,000 identities exposed in each of the data breaches caused by hacking throughout the year, and 42 percent more mobile operating system vulnerabilities.<sup>1</sup> In addition, RSA, the Security Division of EMC Corporation's 2011 Online Fraud Report reveals that the U.S. has consistently hosted not only the largest portion of worldwide attacks, but also the majority of those attacks in general (over 50 percent) since January, 2010.<sup>2</sup> These statistics make clear that this threat is a rapidly growing one.

Today's hearing is well-timed as it follows closely behind the recent White House release of its Cybersecurity Legislative Proposal and the U.S. International Strategy for Cyberspace. TechAmerica is in the process of reviewing the proposals with our members now, and as Congress deliberates incorporating some of those proposals into legislation, we look forward to further discussions about how to most effectively address the threats I will outline today.

---

<sup>1</sup> Symantec Internet Security Threat Report, Trends for 2010. Volume 16, April 2011.  
[https://www4.symantec.com/mktginfo/downloads/21182883\\_GA\\_REPORT\\_ISTR\\_Main-Report\\_04-11\\_HIRES.pdf](https://www4.symantec.com/mktginfo/downloads/21182883_GA_REPORT_ISTR_Main-Report_04-11_HIRES.pdf)

<sup>2</sup> RSA Online Fraud Report. April, 2011.  
[http://www.rsa.com/solutions/consumer\\_authentication/intelreport/11383\\_Online\\_Fraud\\_report\\_0411.pdf](http://www.rsa.com/solutions/consumer_authentication/intelreport/11383_Online_Fraud_report_0411.pdf)

### ***The Evolving Threat Landscape:***

Cybercrime represents today's most prolific threat. The threat landscape once dominated by the worms and viruses unleashed by irresponsible hackers that were largely designed to destroy data or gain notoriety is now ruled by a new breed of cyber criminals who are out to inflict real harm. They can be commercial entities breaking into competitors' records, or international crime rings stealing valuable data like credit card numbers and email passwords for their own financial gain. Cyber attacks are increasingly sophisticated, better organized, persistent and specifically designed to silently steal data for profit or advantage. Fraud, intelligence gathering, and access to vulnerable systems are now the clear motivation behind today's attacks.

Cyber attacks against major corporations over the last year have caught the attention of the public and our government leaders. However, these well-publicized attacks on large companies barely scratch the surface in the grand scheme of attacks on businesses. Corporations are constantly defending themselves against attack, and in most cases, they are doing so successfully. However, not only is the threat becoming more sophisticated and targeted, but the volume is rapidly increasing. A 2010 study by the National Cyber Security Alliance (NCSA), Norton by Symantec, and Zogby International found that 74 percent of small-and medium-sized U.S. businesses were targeted by cyber attackers in the past year.<sup>3</sup> In 2010, McAfee Labs identified more than 20 million new pieces of malware globally.<sup>4</sup> However, a survey conducted by the NCSA and Visa Inc. found that 53 percent of small business owners believe the high cost in time and money to fully secure their business is not justified by the threat.<sup>5</sup> This is something that we must change. The high volume of online activity and the interconnectivity of our networks requires that every company assess their own risks on a regular basis and take appropriate steps to mitigate that risk.

### ***The Economic Impact of Cyber Attacks:***

A central issue, in both public and private sectors, is whether we are devoting enough resources to information security. Part of the answer must come from economic analysis. What are the costs, both historical and potential, of security breaches? How frequently can attacks be expected? Can these factors be quantified precisely, so that organizations can determine the optimal amount to spend on information security and measure the effectiveness of that spending? Our present ability to measure the costs and probabilities of cyber attacks is challenging. There are no standard methodologies for cost measurement.

Investigations into the impact of cyber attacks on stock prices show that targeted firms suffer losses of one to five percent in the days after an attack. For the average New York Stock Exchange Corporation, price drops of these magnitudes translate into shareholder losses of

---

<sup>3</sup> 2010 NCSA/Norton by Symantec Online Safety Study. National Cyber Security Alliance, Norton by Symantec, Zogby International, October 2010. [http://www.staysafeonline.org/sites/default/files/resource\\_documents/FINAL+NCSA+Full+Online+Safety+Study+2010%5B1%5D.pdf](http://www.staysafeonline.org/sites/default/files/resource_documents/FINAL+NCSA+Full+Online+Safety+Study+2010%5B1%5D.pdf)

<sup>4</sup> McAfee Threats Report: Fourth Quarter 2010. <http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-2010.pdf>

<sup>5</sup> 2010 NCSA/Visa Inc. Small Business Study. National Cyber Security Alliance, Visa Inc., Zogby – 463, November 30, 2010.

between \$50 million and \$200 million.<sup>6</sup> On average, corporations lose over \$6 million a day when their sites are down because of a cyber attack.<sup>7</sup> It is estimated that the worldwide economy loses about \$86 billion a year due to cyber attacks.<sup>8</sup> Finally, a 2010 Poneman Institute study estimates that the median annualized cost of a cyber attack is \$3.8 million per organization per year.<sup>9</sup>

### ***The Public-Private Partnership is Essential:***

In the U.S., the private sector owns and operates most of the infrastructure on which information systems rely in order to function. As a partner, the U.S. Federal Government has an obligation to share specific and timely threat information with the private sector from which companies can manage their risk and help protect those critical systems. The government and private sector must leverage and improve the effectiveness of existing collaboration initiatives to address cyber risks, enhance preparedness and resiliency, improve trust and enable market growth. The private sector must be appropriately engaged with the government in the articulation, implementation, and refinement of strategic national cyber priorities, goals, and objectives.<sup>10</sup>

An important component of the public-private partnership is educating the public on the threats we are facing and what we can do to mitigate the risks posed by these threats. As explained in the multi-organization paper, of which TechAmerica was a participant, entitled, “Improving our Nation’s Cybersecurity through the Public-Private Partnership: A White Paper,” the “*Stop. Think. Connect.*” awareness campaign is a new public-private education program designed to help people stay safer and more secure online. It is an outgrowth of the Administration’s Cyberspace Policy Review to-do list. “*Stop. Think. Connect.*” seeks to achieve for online safety and security awareness what Smokey Bear does to prevent wildfires and “Click It or Ticket” does for seatbelt safety. And yet, more needs to be done. We recommend heeding the 2009 example of government and industry mobilization to halt the spread of the H1N1 flu. Simple and effective resources were made widely available to individuals and families, businesses, and communities to mitigate the impact of the outbreak. An array of media (TV, the workplace, and social media, among others) was used to provide public education and simple recommendations to control infections. The effort was a success because of sustained national leadership and years of planning and preparedness by the public and private sectors prior to the pandemic. This collaborative effort could serve as a model for cybersecurity education and awareness. This campaign could be strengthened by also emphasizing a holistic “people, process and technology” approach to cybersecurity, rather than focusing solely on the user. This would include education about new cybersecurity technologies and the importance of regularly applying security patches to systems.<sup>11</sup>

---

<sup>6</sup> *The Economic Impact of Cyber Attacks*. Brian Cashell, William D. Jackson, Mark Jickling, and Baird Webel. Government and Finance Division, the Congressional Research Service. April 2004.

<sup>7</sup> *In the Crossfire: Critical Infrastructure in the Age of Cyber War*. Stewart Baker, Shaun Waterman, George Ivanov. Center for Strategic and International Studies and McAfee, Inc. July 2010.

<sup>8</sup> *Britain Hires Ex-Hackers to Beef Up Cybersecurity*. The Associated Press. June 25, 2009

<sup>9</sup> *First Annual Cost of Cyber Crime Study, Benchmark Study of U.S. Companies*. The Poneman Institute. July 2010.

<sup>10</sup> TechAmerica Principles for Cybersecurity Policy. Appendix A.

<sup>11</sup> *Improving our Nation’s Cybersecurity through the Public-Private Partnership, A White Paper*. Presented by: Business Software Alliance, Center for Democracy & Technology, Internet Security Alliance, U.S. Chamber of Commerce, and TechAmerica.

### ***Advanced Persistent Threats:***

Advanced Persistent Threats (APTs) are one of the most menacing and fast-growing cyber security threats facing organizations of all sizes today. These attacks are advanced and normally employ clandestine means to gain access to a continual thread of intelligence concerning its target. Research has shown that many such attacks are executed with espionage on the mind against an individual or group of individuals such as a foreign nation state government or a private corporation. Those responsible for such attacks are different from many other threat actors in their perseverance and access to significant resources. APT threat actors commonly deploy malware that circumvents common and best practice safeguards such as anti-virus programs. Once a system has been compromised, they will search for and steal intellectual property from compromised computers and networks – including scouring email, network shares, and even defeating encrypted files in their search for sensitive data of interest. These attackers usually establish a long-term, persistent presence inside a company's perimeter. Stolen data is often compressed and then slowly and surreptitiously leaked back to the threat actors systems out of the home network using false headers and protocols designed to circumvent common security technologies such as intrusion detection sensors.

Many often associate APTs with political targets, but APT actors are increasingly aiming to strike enterprise targets for financial gain and other purposes, such as industrial espionage. Over the past few years, APTs have become increasingly sophisticated and diverse in their methodology and techniques, particularly in their ability to use an organization's own unwitting employees to penetrate IT systems and pull off attacks. While many traditional cyber attacks start with mapping networks and collecting intelligence on technical vulnerabilities, an APT actor often starts with mapping workers in the organization and collecting intelligence on employees that may provide the APT threat actor with an initial foothold into the target environment. This suggests that investing more in traditional perimeter defenses is not enough and that multi-layered defenses (including the appropriate education of all employees) and dynamic risk management processes are required.

These techniques have proven so successful and rewarding to attackers that today's organizations must operate under the assumption that being attacked in this manner is inevitable. While it may be impractical, even impossible, to prevent the launching of attacks by APT actors, organizations nevertheless can deflect such attacks by making themselves more difficult, unprofitable targets, or by discovering APT attacks early to prevent large-scale damage. This involves developing intelligent, comprehensive approaches to help organizations become faster and more efficient at detecting threats, neutralizing them and identifying perpetrators.

### ***Social Engineering and Spear Phishing:***

A range of threat actors including the APT actor are now 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. This is known as social engineering and it is popular, at least in part, due to the fact that it is the actual user being targeted, not

necessarily vulnerabilities on the machine. As such, a successful attack can occur regardless of any technical controls, such as a firewall, that might exist on the targeted user's computer.

An example of social engineering is spear phishing. APT actors and other cyber criminals use this as a way of attempting to acquire sensitive data such as usernames, passwords and credit card information by deceiving the target by appearing to be a trustworthy source (such as social website, bank, or even a colleague) via an electronic communication such as email or instant message – termed a “phishing lure.” A successful spear phishing attack usually involves the fraudulent source requesting some sort of verification by clicking on a link that requires the victim to enter in personal information like credit card numbers. Additionally, once the target has clicked on a link they may be tricked into downloading malicious codes or malware, often carefully disguised as something seeming innocuous. What distinguishes spear phishing from other cyber crimes is that it is specifically targeted. Meaning, instead of spamming thousands of people in the hopes of catching a few, spear phishers target select groups of people with something in common, like working at the same company or banking at the same financial institution. The end result is that personal information ends up in the hands of the cyber criminal, enabling them to steal funds, identities, and personal information from the victims.

The Anti Phishing Working Group (APWG) is a non-profit organization that offers assistance and resources to consumers.<sup>12</sup> Many of TechAmerica's members are also members of this organization working to combat internet scams and fraud. On their website, consumers can get advice on avoiding phishing scams and receive guidance on what to do if you have been the victim of an attack. Additionally, it is a place to report a phishing credential collector. Industry is dedicating resources to the APWG to try and combat this threat tactic and protect their customers. APWG is also a key contributor to the Stop. Think. Connect awareness campaign.

### ***Protecting Consumer Data -- The Need for a National Data Breach Law:***

Data breaches are of serious concern to industry as it puts a company's reputation and client base at risk. For organizations that have critical information assets such as customer data, intellectual property, trade secrets, and proprietary corporate data, the risk of a data breach is now higher than ever before. According to a study done by the Ponemon Institute, data breaches from malicious attacks and botnets doubled from 2008 to 2009 and cost substantially more than those caused by human intelligence or IT system glitches.<sup>13</sup> The same study found that the cost of a data breach to U.S. companies increased two percent in 2009 to \$204 per compromised customer record. Specifically, the average total cost of a data breach rose from \$6.65 million in 2008 to \$6.75 million in 2009. According to the Privacy Rights Clearing House, over 5.3 million records containing personally sensitive information have been breached since April 2005.<sup>14</sup> On a positive note, the study also found that most U.S. companies aim to prevent future breaches through training and awareness programs (67 percent).

---

<sup>12</sup> <http://www.antiphishing.org/>

<sup>13</sup> 2009 Annual Study: Cost of a Data Breach. Understanding Financial Impact, Customer Turnover, and Preventive Solutions.

<sup>14</sup> Privacy Rights Clearinghouse, —Chronology of Data Breaches, last updated May 20, 2011, <http://www.privacyrights.org/data-breach#CP>.

In light of the increased prevalence of data breaches, it is crucial that Congress act and pass national legislation addressing security and data breach. In 2009, the House passed H.R. 2221, the Data Accountability and Trust Act. TechAmerica has long supported this legislation as it includes key elements that mirror our Security and Data Breach Principles: a risk-based standard for breach notification to ensure that notice is required when the breach presents a significant risk of harm to consumers; federal preemption of state data and security breach notification laws in order to harmonize what is currently a patchwork of varying compliance and enforcement regimes; and an exemption to notification if personally identifiable information is rendered unusable through the use of best practices such as encryption, access controls, redaction, truncation, or other methods. Consumers stand to benefit greatly from this risk-based approach to data security and we would encourage that this legislation be re-introduced in this Congress and that it be passed by both Chambers and signed into law.

### ***Mobile Application Threats:***

As technology advances, so do the threats and risks that we are exposed to on a daily basis. We have all developed a reliance on our mobile devices. We use these devices to navigate our daily lives including everything from entertainment and communications, to finding driving directions and conducting financial transactions. With this increased reliance on mobile devices comes an increased opportunity for cyber criminals. McAfee found that the number of new mobile malware in 2010 increased by 46 percent compared with 2009.<sup>15</sup> It is important to note that mobile devices primarily originated as consumer personal devices with no interest in enterprise markets. As such, putting consumer devices with limited security capabilities on the enterprise makes the network defender's job more difficult. Another strike against the good guys is that mobile computing is more than 15 years old – as is much of the infrastructure that supports it. This legacy system makes mobile computing more susceptible to attacks. Applications downloaded by the user are not being properly vetted with systems administrators, and users are installing anything that seems fun. How does this affect business? Many employees intertwine the use of their mobile devices for both personal and professional purposes. If a personal application is infected with malware, it can open the door to a business, whether the attacker intended to do so or not. This affects the individual because it can open the door to their personal information falling into the hands of cyber criminals. User awareness is crucial if mobile device attacks are to be combated.

The lesson learned from the threats to our mobile devices is that we need to shift how we approach security. No matter what the next big thing is in technology, there will eventually be security risks. If we are to have any chance of keeping up with and beating the cyber criminals we need to view security as a platform and drive security into the infrastructure instead of bolting it on at the end. Many companies are increasingly taking those important steps, and more need to follow suit. Additionally, security solutions need to have a broad and varied ecosystem of

---

<sup>15</sup> McAfee Threats Report: Fourth Quarter 2010. <http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-2010.pdf>

complementary components that allows everyone from enterprises to individuals to participate in the defense of our collective networks.<sup>16</sup>

***Conclusion:***

These realities around APTs and other threats reinforce the U.S. Federal Government's transition from compliance-focused security programs to continuous monitoring and operational risk management. That same evolution is occurring rapidly in the private sector and is one of the principle reasons why TechAmerica advocates for a risk-based approach in cybersecurity legislation. We need organizations in both the public and private sector to be able to continuously monitor their systems and networks to understand what is happening and critically, to know when they are being attacked, and to be able to adjust their security controls and defenses accordingly. It is essential that organizations be able to effectively combat all threats, however, they will not be able to do so if they have static defenses in place that are focused primarily on compliance measures.

As Congress evaluates various cybersecurity proposals we recommend that the Committee consider TechAmerica's Principles for Cybersecurity Policy: cybersecurity needs to be viewed through a global lens; partnership is vital to cybersecurity; identify and protect critical functions; cybersecurity solutions must take into account the interdependent nature of cyberspace; efforts to secure critical systems must be risk-based; risk management must address people, processes, and technology; market forces should be leveraged to drive greater adoption of security standards and best practices; national governments must collaborate to bolster global cybersecurity and cooperate to investigate and prosecute crime; and cybersecurity must be a priority for the future.<sup>17</sup>

Specifically, we urge you to incorporate the following key elements of industry's views with regard to our cybersecurity:

- **Innovation:** Already, many private sector actors are responding and adapting to a complex and evolving threat environment, and it is important that private sector actors continue their innovation in a flexible environment that allows individual companies and other private sector entities to respond quickly and effectively to evolving challenges. Cybersecurity is ultimately a shared responsibility, and industry is committed to developing technology to protect users across the Internet, contributing research, facilitating industry initiatives and conversations, and empowering users through security education. Due to this shared responsibility, it is paramount that government allows the private-sector to lead and guard against increased balkanization which could impact continued innovation and growth within this vibrant global market place.
- **Outcome-focused measures:** The government should promote an outcome-based, layered security approach while encouraging its adoption by the private sector through voluntary means and avoiding a one-size-fits-all, mandated approach to cybersecurity.

---

<sup>16</sup> TechAmerica Cyber 101 Briefing on Capitol Hill- Part 2. <http://www.techamerica.org/cyber101-may>

<sup>17</sup> TechAmerica Principles for Cybersecurity Policy. Appendix A.



Additionally, it is vital that the government develop processes by which to measure performance and outcomes associated with its own cybersecurity efforts.

- **Risk-based security:** Organizations need to address cyber threats based specifically on the importance of the networks and systems involved. For this reason, government should address risks to our nation's critical infrastructure differently from its approach to systems and networks that are not. We encourage Congress to draw a bright line between critical and non-critical infrastructure. Industry and government need to work together to make the right determinations for what is critical, and what the implications are for that designation. Further, critical infrastructure should be narrowly defined to include only critical infrastructure that is of the utmost importance to national security.
- **Incentivizing best practices:** The government can provide certain incentives to encourage industry to invest in additional security and risk mitigation measures. Examples of such incentives could include providing a safe harbor (from data breach notification, for example) for organizations that take preventative and protective measures in advance of an incident that would reduce or eliminate harm to individuals or organizations (such as measures to render data unreadable if accessed by an unauthorized person). Any such safe harbor should be implemented in a technology-neutral manner.
- **Liability protection:** We appreciate efforts to provide for appropriate liability protections for the private sector in certain circumstances. If industry is to act at the behest of government, it is necessary that there be liability protections in place not only to protect industry in the case of unintended or unanticipated consequences of required action, but also to preserve the public-private partnership necessary for preparation and protective measures.
- **Updates to FISMA:** With the rapidly evolving threat environment, we must update our federal information security practices – and, in some cases, our legal framework, to perform in a more nimble environment. TechAmerica strongly supports updating the Federal Information Security Management Act (FISMA) to reflect a risk-based approach with a focus on continuous monitoring and greater responsibility and accountability of senior agency officials for managing and protecting the agency's infrastructure. The reporting requirements are time consuming and costly and have not been shown to increase security of government systems. Furthermore, the government will benefit from an update of the paper-based, check-the-box framework that exists under the current FISMA framework.
- **Education and awareness:** We must emphasize the important role of education and awareness as it relates to this complex topic. The Department of Homeland Security has taken a lead role in this area as a sponsor and active participant in the NCSA and [staysafeonline.gov](http://staysafeonline.gov). The purpose of NCSA, a 501(c)(3), is to educate consumers, K-12, higher education, and small-and medium-sized businesses on the steps they need to take in order to use the Internet safely and securely, protecting themselves, their data and the cyber infrastructure. As an industry, we recognize the good work of the NCSA which highlights the need for formal K-12 education and curriculum to address cyber safety,

cybersecurity and cyber ethics (C3) within schools. NCSA and DHS have worked with key stakeholders to develop this C3 framework. In addition to a K-12 curriculum framework, NCSA has established a volunteer program (C-SAVE) for computer security professionals to teach cybersecurity in schools and is working to conduct a small and medium-sized business study to identify current cyber practices, gaps, resource needs, and ways to communicate effectively with this important audience.

I would like to once again thank the committee for inviting me to testify, but more importantly, for focusing this hearing on the critical need for improved cybersecurity. TechAmerica and our member companies look forward to continuing to work with you on this important economic and national security issue. Thank you.

# Phillip J. Bond

## President & CEO



Phillip J. Bond is the President and Chief Executive Officer of TechAmerica. In 2008 as the President & Chief Executive Officer of the Information Technology Association of America (ITAA), a position he held since 2006, Bond partnered with Christopher W. Hansen -- then President & CEO of AeA -- to form TechAmerica. As President & CEO of ITAA, Bond helped to also drive the April 1, 2008 merger with the Government Electronics and Information Technology Association (GEIA).

Recently, Bond has been recognized as part of the Federal 100, Federal Computer Week's listing of the most influential people in government-technology, and as a 2011

Tech Titan by the Washingtonian.

Mr. Bond is also a Board Member of the World Information Technology and Services Alliance (WITSA), a network of industry associations representing 70 high-tech trade groups around the world.

Bond is a highly accomplished executive in both government and industry. Prior to joining ITAA, he served as Senior Vice President of Government Relations for Monster Worldwide, the world's largest online career site, and General Manager of Monster Government Solutions.

From 2001 to 2005, Bond was Under Secretary of the U.S. Department of Commerce for Technology and, from 2002-2003, served concurrently as Chief of Staff to Commerce Secretary Donald Evans. In his dual role, Bond worked closely with Secretary Evans to increase market access for U.S. goods and services and further advance America's technological leadership at home and around the world. He oversaw the operations of the National Institute of Standards and Technology (NIST), the Office of Technology Policy, and the National Technical Information Service. During his tenure the Technology Administration was the pre-eminent portal between the federal government and the U.S. technology industry. During that time, Bond was recognized in Scientific American magazine in its list of the Top 50 Tech Leaders of 2003.

Bond joined the Administration from the private sector, where he served as Director of Federal Public Policy for the Hewlett-Packard Company, and previously as Senior Vice President for Government Affairs and Treasurer of the Information Technology Industry Council.

From 1993 to 1998, Bond served as Chief of Staff to Congresswoman Jennifer Dunn (R-WA). He was Principal Deputy Assistant Secretary of Defense for Legislative Affairs from 1992 to 1993. Earlier, Bond was Chief of Staff and Rules Committee Associate for Congressman Bob McEwen (R-OH) from 1990 to 1992. From 1987 to 1990, he served as Special Assistant to the Secretary of Defense for Legislative Affairs.

He is a graduate of Linfield College in Oregon. Bond and his wife, Diane, have two daughters and reside in Fairfax Station, Virginia.

Committee on Oversight and Government Reform  
Witness Disclosure Requirement – “Truth in Testimony”  
Required by House Rule XI, Clause 2(g)(5)

Name:

Phillip Bond

1. Please list any federal grants or contracts (including subgrants or subcontracts) you have received since October 1, 2008. Include the source and amount of each grant or contract.

N/A

2. Please list any entity you are testifying on behalf of and briefly describe your relationship with these entities.

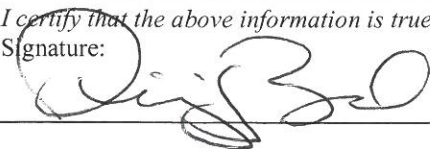
Technology Association of America, Inc. (d/b/a TechAmerica)

3. Please list any federal grants or contracts (including subgrants or subcontracts) received since October 1, 2008, by the entity(ies) you listed above. Include the source and amount of each grant or contract.

N/A

I certify that the above information is true and correct.

Signature:



Date:

5/18/11