TechAmerica
WHERE THE FUTURE BEGINS
THE ASSOCIATION OF COMPANIES DRIVING INNOVATION WORLDWIDE

May 5, 2009

Written Statement

of

Liesyl I. Franz
Vice President for Information Security and Global Public Policy
TechAmerica

Before the

Subcommittee on Management, Organization, and Procurement
Committee on Oversight and Government Reform
U.S. House of Representatives

Chairwoman Watson, Ranking Member Bilbray, and distinguished members of the Subcommittee, my name is Liesyl Franz, and I am Vice President for Information Security and Global Public Policy at TechAmerica. Thank you for giving us the opportunity to testify today and to provide the technology industry's perspective on *Cybersecurity: Emerging Threats, Vulnerabilities, and Challenges in Securing Federal Information Systems*.

TechAmerica is a trade association with the strongest advocacy voice for the technology industry in the U.S. formed by the January 2009 merger of four major technology industry associations – the Information Technology Association of America (ITAA), AeA (formerly the American Electronics Association), the Government Electronics and IT Association (GEIA), and the Cyber Security Industry Alliance (CSIA). The new entity brings together over 1500 member companies in an alliance that spans the grass roots – with operations in nearly every U.S. state – and the global – with relationships with over 70 national IT associations around the world. The U.S. technology industry is the driving force behind productivity growth and jobs creation in the United States and the foundation of the global innovation economy. TechAmerica's members are the very companies – both hardware and software manufacturers – that serve as the foundation of our national digital infrastructure, as well as those that are providing systems integration services, enterprise IT and management solutions, and a wide variety of information security solutions for small, medium, and large companies, consumers, and government agencies.

I am here today to highlight the critical role of technology in helping to secure cyberspace – one we share with our government partners, our customers and users around the world. As products and service providers and critical infrastructure owners and operators, the private sector is a key stakeholder – and partner – in improving our cyber security posture. 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 cyber security as a vital part of continuing economic growth and economic security, innovation, and U.S. competitiveness, as well as national and homeland security.

I will address the need for a national strategy under the auspices of a newly created position of Cyber Security Advisor in the White House, TechAmerica's continued call for improving the Federal Information Security Management Act of 2002 (FISMA), and the importance of the public private partnership and how it can be enhanced to address the challenges we face today and those we will face in the future.

Information Security Threats Continue to Evolve

First, let me characterize aspects of the current threat and vulnerability environment, based on reports from our members that monitor and address those threats and vulnerabilities every day. While specific attribution of an attacker is often elusive, we know that all manner of attackers are part of the threat picture, from individual hackers and spammers to fraudsters, from virtual criminal networks to established criminal organizations, and, reportedly, even nation states.

- According to Symantec Corporation's semi-annual *Global Internet Security Threat Report* published in April 2009, the key trend to note is that malicious activity is increasingly web-based. That means that attackers wanting to take advantage of client-side vulnerabilities no longer need to actively compromise specific networks to gain access to those computers; instead, they are focused on attacking and compromising websites in order to mount additional, client-side attacks. Attacks can be more targeted, which makes it more efficient and effective for the attackers.

  Another notable trend is based on the increasing complexity of methods used by the attackers. For example, rather than only exploiting high-severity vulnerabilities, attackers are able to string together exploits for medium-severity vulnerabilities to achieve the same goal as exploiting a high-severity vulnerability. This means that organizations that only defend against exploits to high-severity vulnerabilities will miss some of these new multi-exploits.[1]

- The volume of cyber attacks continues to increase significantly. According to RSA's Anti-Fraud Command Center (AFCC), the volume of phishing attacks detected by RSA, The Security Division of EMC, grew an astonishing 66 percent over 2007.[2]

[1] *Symantec Global Internet Security Report: Trends for 2008;* Volume XIV, April 2009: http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf

[2] *RSA Anti-Fraud Command Center's 2008 Phishing Trends Report,* January 2009: http://www.rsa.com/solutions/consumer_authentication/intelreport/FRARPT_DS_1208.pdf

- Further demonstrating the evolution of cyber criminal behavior, Microsoft notes in its April 2009 Security Intelligence Report that the threat landscape in the U.S. was dominated by malware, which accounted for 67 percent of all exploits detected on infected computers in the second half of 2008. In addition, Microsoft also saw an increase in rogue security software infections of more than 48 percent compared with the first half of 2008.[3]

- In its 2009 trends analysis, McAfee notes the exploitation of web-based applications through social networking sites and consumer devices, as well as the growing distribution of malware in languages other than English.[4]

- According to Verizon's 2009 Data Breach Investigations Report, over 285 million records were compromised in 2008, and in 38 percent of those breaches, "malware" was utilized.[5]

- The challenges to securing federal systems are not only technological ones. In their recent report on *The 2009 State of Cybersecurity from a Federal CISO's Perspective*, (ISC)², Cisco, and Government Futures presented the results of a recent survey of agency Chief Information Security Officers (CISOs). They noted not only the external threat, but the insider threat as well.[6] In addition, while many CISOs feel they are more empowered today than they have been, many still cited bureaucratic constraints and staffing and resource concerns.[7]

These data points help illustrate the challenges that risk managers in both the private and public sector face in combating the growing sophistication, volume, and apparent success of a wide range of cyber attacks and information security breaches.

Organizing Effectively to Address the Information Security Challenge

The new Administration and the new Congress present an opportunity for a new National Strategy for Cyber Security that builds upon and enhances the work that has been done to date. We commend President Obama for calling for a White House 60-Day Review on cyber security, and we call on him to meet his campaign pledge to appoint a senior cyber security advisor in the White House.

I would like to emphasize two important points in this regard. The first is a fundamental issue regarding the synergy between cyber security and economic growth. As TechAmerica iterated in

---

[3] *Microsoft Security Intelligence Report,* Volume 6: July through December 2008: http://www.microsoft.com/protect/computer/SIR/Vol6.mspx

[4] McAfee White Paper: *2009 Trend Predictions: Slumping economy drives malware threats*: www.mcafee.com/us/local_content/reports/2009_threat_predictions_report.pdf

[5] *2009 Data Breach Investigations Report: A study conducted by the Verizon Business Risk Team*; http://securityblog.verizonbusiness.com

[6] *2009 Data Breach Investigations Report:* 20 percent of the breaches investigated in 2008 were from insiders.

[7] *The 2009 State of Cybersecurity from the Federal CISO's Perspective – An (ISC)² Report*, April 2009

our response to the 60-Day Cyber Security Review, the relationship between security, prosperity, and innovation should be viewed and leveraged as a synergistic one.[8] In essence, in today's digital economy, information security contributes to the reliability of the critical infrastructure on which productivity and innovation depend, and the integration of security and privacy and civil liberties concerns engenders trust and confidence in the information infrastructure; by fostering reliability, trust, and confidence, security helps drives economic growth. In turn, a dynamic innovation economy drives an evolution in cyber security solutions that is critical to staying one step ahead of the threats.

Second, TechAmerica encourages the President to appoint a senior cyber official immediately. Doing so will provide a cyber security leader in the White House with the political leadership needed to develop and execute an updated national strategy to ensure coordinated, comprehensive, and effective implementation across the federal government and in partnership with industry. This first step is crucial to effective execution of the recommendations that may come out of the 60-Day Review.

As part of the public dialogue on cyber security, some have expressed concern that a new advisor in the White House would take authorities or responsibilities away from the Department of Homeland Security (DHS) or other agencies, but we do not believe that is the case. Certainly, DHS and other agencies will have a large role to play in providing strategy input and implementing key elements of it. For example, the U.S. Computer Emergency Readiness Team (US-CERT) plays an increasingly important role in protecting federal systems while working with the private sector to improve situational awareness, and those capabilities should be expanded. But, to date, there has not been an on-going, coordinated, national approach with senior White House leadership that would drive strategy development and cohesive implementation, bringing the strengths and capabilities of the various agencies and the concerns and input of stakeholders to bear. It is also important to note that such a position provides for a sustained voice in the White House for the cyber security component of issues of national concern.

Certainly an effective national strategy should include a strong focus on improving the security of federal information systems. TechAmerica (previously as ITAA) was a champion of FISMA when it was enacted in 2002, and we remain committed to the intent of the legislation. However, we do believe that in order to address the risk management challenges that federal agencies face today, FISMA needs to be updated to reflect the current organizational and operational environment. FISMA compliance grades may have improved over the years, but there does not seem to be a correlation between an agency's FISMA compliance and the state of its cyber security posture.

In 2007, TechAmerica testified before this Committee's Subcommittee on Information Policy, Census, and National Archives on FISMA and outlined six areas for update and improvement:

[8] *TechAmerica Response to the White House Cyber Security 60-Day Review:* http://www.techamerica.org/GovernmentAffairs/TechAmericaInput_CyberSecurity60_DayReview_FINAL.pdf

- Reform the annual agency information security program approval process
- Remove barriers to innovation
- Increase accountability
- Enhance federal cyber risk management
- Harmonize and enhance audit and oversight methods
- Expand federal cyber response capabilities.

We continue to advocate these areas for improvement, and we see many of them are being addressed in subsequent legislative proposals and in implementation. Of crucial importance is empowering the federal agency CISO and holding the agency leadership accountable for information security management.[9]

One specific area where important steps have been taken has been the implementation of the Office of Management and Budget's (OMB) guidance on Federal Desktop Core Configuration (FDCC) that set requirements for security settings for computers connected directly to federal agency networks. While we concur with the goals of the FDCC requirements, the process that was initially undertaken to promulgate the guidance did not include adequate consultation with industry. Subsequently, the National Institute for Standards and Technology (NIST) has invited vendors to participate in the development of standards for their products that would lead to appropriate requirements or controls. For any future engagement, we strongly encourage collaboration with industry partners from the beginning of the process to help articulate the problem and identify solutions. Such a collaborative process may require additional resources for NIST, which we believe should be considered and supported.

In order to effectively address the emerging threats, vulnerabilities, and challenges to federal information systems and, indeed, to our entire digital infrastructure, it is critical to engage in a public private partnership that is both strategic and operational.

On the strategic front, we have a partnership in place under the auspices of the National Infrastructure Protection Plan (NIPP), with its risk management framework for the 18 critical infrastructures and key resources, and the Critical Infrastructure Partnership Advisory Council (CIPAC). TechAmerica was instrumental in the establishment of the Information Technology Sector Coordinating Council (IT SCC), and I am honored to serve as the current Secretary. We have made strides in our risk management efforts for the sector, both in assessing our own risk and in working with the other sectors that depend on the products and services that our sector provides. The partnership has not been without its challenges, and there is always room for improvement, but we have organized ourselves well and continue to reach out to others to participate in our coordinated efforts.

Frankly, one early challenge was the government's own slow adoption of the NIPP framework as a partnership mechanism, except for discrete sector specific agencies like the National Cyber Security Division (NCSD) for the IT Sector and the National Communications System (NCS) for

[9] TechAmerica (ITAA) testimony before the Subcommittee on Information Policy, Census, and National Archives, June 2007: http://www.itaa.org/upload/news/docs/testimonybond060707.pdf

the Communications Sector, which have been committed to the NIPP partnership mechanism since the beginning. We do see increasing government engagement in the NIPP framework, but getting active agency participation in the Government Coordinating Council part of the partnership remains a challenge that needs to be addressed.

Also changing for the better is the federal government's improved outreach to the Sector Coordinating Council framework for input to strategic initiatives at the earliest possible point. Despite a rocky start, the SCCs were subsequently well-leveraged for input into Project 12, the critical infrastructure piece of the Comprehensive National Cyber Initiative (CNCI). The DHS Office of Cybersecurity and Communications has been an important part of that outreach. In addition, The White House reached out to the IT and Communications Sector Coordinating Councils as well as the NIPP's Cross Sector Cyber Security Working Group (CSCSWG) early in the consultative process for the 60-Day Cyber Security Review. We are seeing progress and more transparency in these processes, and we should insist upon even more collaboration along these lines.

Another strategic opportunity for public private partnership is in the area of research and development for greater cyber security into the future. While we are taking important steps in identifying where government and industry R&D is occurring and what the needs are, we have more to do in that area. In addition, we have yet to create a mechanism for true government-industry collaboration on specific projects. That will take some effort to define, fund, and implement, but it will be crucial for addressing longer term challenges and cyber security measures for the future.

A key element of the public private partnership is the operational component. The operational component is the day-to-day defense against, mitigation of, response to, analysis of, and recovery from cyber incidents in the broad eco-system. And, that component is made up of a series of relationships between operations centers and responders. To illustrate, both private and public enterprises often have network operation centers for cyber security, often referred to as Computer Security Incident Response Teams (CSIRTs), Computer Emergency Response Teams (CERTs), or other similar entities. On occasion there are formal agreements for collaboration or information sharing between these CSIRTs, but for the most part, cooperation is informal or episodic. Relationships exist among the federal agency CSIRTs, among companies in Information Sharing and Analysis Centers (ISACs) and otherwise, between government and industry operations centers, and even among CSIRTs of all kinds (including government, industry, and academic) on a global basis in the Forum of Incident Response Security Teams (FIRST). The relationships are there and growing; we need to enhance and leverage them more fully, and we need to foster domestic and international collaboration and trust.

I will focus my comments here on the IT-ISAC, which serves as the operational focal point for the IT SCC.

The IT-ISAC is a trusted community of security specialists from companies across the IT industry dedicated to protecting the IT infrastructure that propels today's global economy by identifying threats and vulnerabilities to the infrastructure, and sharing best practices on how to

quickly and properly address them. The IT-ISAC's 24x7 Operations Center serves as a centralized hub for sharing information and providing analysis on threats and vulnerability information through secure communication channels.[10]
The notable elements of the IT ISAC are that it serves as an industry response and analysis center, and it provides a way for sharing information with – and from – the government. The IT ISAC works closely with the US-CERT which, in turn, provides a conduit for other government agencies. However, we can still improve upon that mechanism. US-CERT has improved its operational capabilities and processes over the past year, and the DHS Office of Cybersecurity and Communications should be commended for their efforts. However, the Department desperately needs an appropriate facility and more skilled manpower not only to manage the volume and complexity of incidents that are occurring, but also to take strategic steps to prevent them.

Ideally, we should build a joint industry/government operations center that includes a combined government watch center with, at a minimum, US-CERT and NCC/NCS and representation from each of the 18 critical infrastructures. Co-location would help to achieve productive, targeted, and purposeful information exchange and real-time analysis and collaboration between the government and industry. However, obstacles remain to co-location of analysts and responders from industry and government. Government has been reluctant to find ways to share actionable threat information with industry, and industry has not felt comfortable with government's ability to protect proprietary information. We have the opportunity to address those challenges and make change right now.

This is not to say that information exchange and cooperation does not occur. In a recent example, industry leaders galvanized their collaborative efforts around the Conficker worm. A "Conficker Working Group" was quickly established, and industry and government worked together on various aspects of the issue throughout its duration. The achievements and lessons learned from response to that incident could positively inform a path forward for collaboration that has predictable channels for communication and collaboration while maintaining the flexibility needed to address incidents on a case-by-case basis. In addition to providing its own independent analysis of Conficker, the IT-ISAC reached out to other critical infrastructure sectors and worked in tandem with other private sector organizations, such as the Financial Services ISAC, to raise awareness of the threat.

Lastly, I would also like to say a word about additional efforts underway in the private sector to address the challenges to securing critical infrastructure assets.

Industry is leveraging the partnership framework to facilitate collaborative efforts within and among sectors. For example, as part of its Sector Specific Plan (SSP), the IT Sector is completing an IT Sector Baseline Risk Assessment that evaluates risk to the IT Sector, focusing on the sector's critical IT Sector functions, rather than physical assets. The IT Sector's Baseline Risk Assessment is intended to provide an all-hazards risk profile that IT Sector partners can use to inform resource allocation for protection of the critical IT Sector functions and to serve as a baseline of national-level risk based on input received from subject matter experts from across

[10] http://www.it-isac.org

the IT Sector. While the assessment does not address all threat scenarios faced by IT Sector entities or their users and customers, it does address those operational or strategic risks to the IT Sector infrastructure that are of national concern. By increasing the awareness of risks across the public and private sector domains, the baseline risk assessment serves as a foundation for ongoing national-level collaboration to enhance the security and resiliency of the critical IT Sector functions.

The technology industry has been rapidly expanding its efforts to proactively address building security in to products, services, and platforms and to develop robust product assurance initiatives. Technology companies are strongly dedicated to increasing trust in information and communications technology products and services through:

- advancing effective assurance methods;[11]
- driving a new generation of security response and engineering;[12] and
- developing standards and best practices through participation in various standards making bodies and processes and leveraging those standards and best practices in their business operations and in the products and services they provide. We encourage the U.S. Government to engage more fully in the international standards making activities as well.

Conclusion

In sum, there are some key steps that can be taken to better secure government information systems. First, the Administration can act quickly to appoint a senior cyber security advisor with authority needed to develop, coordinate, and implement the President's cyber security priorities. Second, FISMA reform can enable and empower federal CISOs to understand their information security risks and take appropriate mitigation measures according to their organization's needs, including effective security controls that reduce exposure to a majority of vulnerabilities. Third, we can strengthen the public private partnership to address both strategic and operational concerns, both here at home and globally.

We commend the Congress for its early focus on cyber security issues and this subcommittee for convening this panel today. This congressional session provides a significant opportunity to make progress, and we look forward to working with you and your colleagues to develop proposals for meaningful change.

Thank you for the opportunity to appear before you today and express industry's perspective on this important issue. I would be happy to answer any questions you may have.

---

[11] One example of an industry group effort is the Software Assurance Forum for Excellence in Code (SAFECode), a non-profit organization exclusively dedicated to increasing trust in information and communications technology products and services through the advancement of effective software assurance methods: http://www.safecode.org.

[12] One example of an industry group effort is the Industry Consortium for Advancement of Security on the Internet (ICASI), which intends to be a trusted forum for addressing international, multi-product security challenges. This trusted forum extends the ability of information technology vendors to proactively address complex security issues and better protect enterprises, governments, and citizens, and the critical IT infrastructures that support them: http://www.icasi.org