

Questions from Committee:

(1) Does the current range of federally supported research adequately address the cyber security needs of industry as well as new and emerging threats? If not, what are the research gaps, and how would you prioritize federal research investments in cyber security?

(2) How does the private sector provide input regarding its research needs into the process by which the federal research portfolio is developed? Do you believe your needs are adequately addressed by the federal research agenda? How can the federal government more effectively partner with the private sector to address common research needs?

(3) What is the state of cyber security education? Are future cyber security professionals being adequately trained by colleges and universities to meet anticipated demands of the private sector? If not, what kind of cyber security training is appropriate and necessary for institutions to develop, and for what kinds of students?

June 10, 2009

Written Statement

of

**Liesyl I. Franz
Vice President, TechAmerica**

Before the

**Subcommittee on Research and Science Education
Committee on Science and Technology
U.S. House of Representatives**

Chairman Gordon, Chairman Lipinski, Ranking Member Ehlers, 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 *Cyber Security Research and Development*.

TechAmerica

601 Pennsylvania Ave. - Suite 600, Washington, DC 20004 ■ Phone: (202) 682-9110 Fax: (202) 682-9111
1401 Wilson Blvd. - Suite 1100, Arlington, Virginia 22209 ■ Phone: (703) 522-5055 Fax: (703) 525-2279

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 America 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 globe. 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, research and development, and science education in helping to secure cyberspace – one we share with our government partners, our customers and users around the world. As critical infrastructure owners and operators, the private sector is a key stakeholder – and partner – in improving our cyber security posture. While there are many things we collectively need to do on a real-time, operational basis, we also need to be working on longer-term, strategic initiatives that will ensure our cyber security posture and leadership for the future. Research and Development and education for a skilled work force are precisely those areas that are strategic in nature and require immediate and sustained attention. I will address both in my testimony today.

TechAmerica, or formerly ITAA, has been very engaged in cyber security effort from the beginning. We served as the IT sector coordinator and founder of the IT Sharing and Analysis Center (IT-ISAC) during the Clinton Administration, and we have been a leading industry voice since. We actively advocated for the Cyber Security Research and Development Act of 2002. We played a significant role for industry in the development of the *National Strategy to Secure Cyberspace* and the Cyber Security Summit that followed in 2003. We played a leading role in the establishment of the IT Sector Coordinating Council (IT SCC) under the National Infrastructure Protection Plan (NIPP), and I am honored to serve as the current Secretary. We have a long-standing and robust Information Security Committee that works on all manner of cyber security policy issues, and we are happy to provide our input today.

The State of Cyber Security Research and Development Funding

In 2002, the Congress passed, and President Bush signed into law the Cyber Security Research and Development Act, which provided for over \$900 million over 5 years in cyber security R&D funding for the National Science Foundation (NSF) and the National Institute for Standards Technology (NIST). That funding was sorely needed at the time and has contributed to the body of knowledge that we have today to address the kinds of threats we face in cyberspace.

Today, we understand that the federal government plans to spend about \$143 billion in 2009 on R&D. The Center for Strategic and International Studies' (CSIS) Commission of Cyber Security for the 44th Presidency noted that of that amount, two-tenths, or about \$300 million, would go to cyber security. "Given the important of cybersecurity to all aspects of our national defense and economy coupled with the more sophisticated cyber threats we face," the report stated, "a \$300 million R&D investment is in adequate."¹ By way of comparison with our global partners, Europe spends ***** on R&D funding, Asia, etc. *****.

The CSIS Report acknowledges the introduction of the Comprehensive National Cybersecurity Initiative (CNCI) and its recognition of the shortfalls in cyber security related R&D funding, along with its related efforts. The CNCI calls for increased cyber security R&D funding in the future and has embarked on a consultative process under the Networking Information Technology Research and Development (NITRD) program's Cyber Leap Year project to "identify the most promising game-changing ideas with the potential to reduce vulnerabilities to cyber exploitations."² Currently in its third phase, the NITRD request for information (RFI) process for Cyber Leap Year has canvassed the cybersecurity community for ideas, is holding workshops to explore the best ideas presented, and will publish its findings on game-changing ideas, technical strategies for needed research, productization and implementation of capabilities, and recommendations for success, including funding.³ We look forward to the results of the NITRD process.

Most recently, President Obama released his *Cyberspace Policy Review* on May 29, 2009. In addition to his welcome announcement that he would appoint a cyber security coordinator in the White House, the President also committed his Administration to "invest[ing] in the cutting-edge research and development necessary for the innovation and discovery we need to meet the digital challenges of our time."⁴ The cyber review itself recommended that R&D frameworks should be linked to infrastructure development and called about the federal government to (1) work with industry to "develop migration paths and incentives for the rapid adoption of research and technology development, including collaboration between academic and industrial laboratories," and (2) "in collaboration with the private sector and other stakeholders...use the infrastructure objectives and the R&D Framework to help define goals for national and international standards bodies." In its recommended near-term action plan, the report called for the development of "a framework for research and development strategies that focus on game-changing technologies that have the potential to enhance the security, reliability, resilience, and trustworthiness of digital infrastructure; provide the research community to event data to facilitate developing tools, testing theories, and identifying workable solutions."⁵ We were very pleased with the call for working with industry on these efforts.

¹ *Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency*, Center for Strategic and International Studies; page 74;

http://www.csis.org/media/isis/pubs/081208_securingcyberspace_44.pdf

² <http://www.nitrd.gov/leapyear/>

³ http://www.nitrd.gov/leapyear/NCLY_RFI-3.pdf

⁴ http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/

⁵ *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, p. 37, The White House; http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

Industry itself has coalesced its efforts around cyber security research and development efforts that seek to affect the greater needs. Of course, individual companies conduct R&D all the time on the products and services it needs to drive market solutions and meet the demands of their customers. In fact, the overwhelming bulk of cyber security R&D is provided by private sector entities seeking to develop the most innovative solutions to meet the broad market requirements. While the protection of our national critical infrastructures relies on these efforts, there are gaps in cyber security capabilities for which there is such limited market demand or the lack of market awareness. The Cyber Leap Year project under the CNCI and other efforts demonstrate the federal government's understanding that such a gap exists and we need to work together or fill it. Further, federal R&D will result in technology that can improve the Nation's security if that technology is transferred to industry – in accordance with existing Federal technology transfer policies – for further development and integration into cyber infrastructures.

In addition to discrete company R&D projects, the IT industry has been working together on the strategic side of R&D planning in the IT SCC's Research and Development Committee. The R&D Committee is charged with conducting annual reviews of R&D initiatives in the IT Sector and recommending updates to industry priorities based on changes in technology, threats, vulnerabilities, and risk. The sector has come a long way in the last three years informing the process of R&D prioritization through a risk assessment process. This process identifies the cyber risks in our IT infrastructure and evaluating what protective programs exist to cover those risks. R&D is leveraged to evaluate innovative ways to cover gaps in the protective programs and evolve programs with the risk. This R&D prioritization process is a collaborative one between IT Sector and our Government counterparts. Additionally, the IT risk assessment, protective programs, and R&D efforts are coordinated across all critical infrastructure and key resource sectors (CI/KR) through the Cross-Sector Cyber Working Group (CSCSWG).

Until recently, this coordination has been limited to the Department of Homeland Security (DHS) as the Sector Specific Agency (SSA) for the IT SCC; however, through joint collaborative success, the IT SCC has started coordinating prioritization with the Interagency Working Group (IWG) on Cyber Security and Information Assurance (CSIA). The purpose of this collaboration is to highlight the role of the private sector in cyber security R&D and reduce duplication of investment in private and public sector. The IT SCC R&D Committee has developed a cyber security R&D information sharing framework that highlights those risk areas that receive less private sector emphasis due to the limited market need for the investment. With an overwhelming amount of market R&D investment addressing commercially viable concepts, there are those risks that are of greater interest and need higher prioritization in government. The IT-SCC facilitates this information sharing between the private sector and the CSIA to help agencies better prioritize individual agency R&D spending, as well as project selection as well as coordinate cross-agency spending on risks that will receive less attention from private sector entities. As an example, through the IT-SCC R&D Committee work we have learned that there is not much private sector R&D on cyber forensics as it relates to law enforcement evidence trail. As such, this area of investment appears to be de-prioritized in the private sector and may need to be prioritized by government R&D programs to garner the innovation necessary to align with the need for the ability to analyze cyber incidents. We have also learned that there are cases

in which government has undertaken R&D in areas where the private sector is already making a significant investment, so the increased dialogue is important to avoid such duplication.

There is no institutionalized mechanism for the private sector to provide input into the process by which the federal research portfolio is developed. It is the vision of the IT-SCC R&D Committee to provide a collaborative, partnered environment that allows both government and private sector to break down existing barriers and promote collaboration in IT Sector security R&D. The goal is to better inform both government and industry about existing and prospective work – and needs – so that resources are allocated and used more efficiently and government can leverage the already existing commercial investment such that it can better target the limited R&D resources. While we believe these efforts are making a difference in the coordination and dialogue between industry and government, we strongly recommend a more formal mechanism be put in place for such input and collaboration. Such a mechanism should include all the elements of the R&D lifecycle: identification of current and prospective R&D in the industry; determination of the gaps in the market that need to be filled by government efforts; and, where necessary and feasible, joint industry and government collaboration on R&D projects. Collaboration should also take place with our global partners in government and industry so that we can leverage, rather than duplicate, efforts.

[question: list priority areas for R&D, such as attribution, authentication, others?]

As we note, there is discrete R&D occurring in industry and in government, respectively. Presumably these are geared toward new product development or solutions to problems in the existing environment. However, we believe there is now an opportunity for a more strategic public private partnership in research and development for greater cyber security into the future. We have yet to create a mechanism for true government-industry collaboration on specific projects, particularly those that will re-set the paradigm. 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.

Another notion that could be explored in order to help achieve greater coordination and collaboration is the creation and funding for a national clearinghouse to serve as an intermediary between government and industry on dialogue and collaboration for R&D and, even, other pertinent projects such as building a reference resource for standards, best practices, and collaboration opportunities. Notionally, such an entity could be created through a partnership between academia, industry and government and be administered by a broad based national nonprofit organization meeting such appropriate criteria as substantive expertise and a distributed network with operations in most states.

The State of Cyber Security Education

The exponential growth in the use of information technology for just about every aspect of our society and economy today has yielded remarkable results in innovation, efficiencies, productivity, and new business models for new product services. However, that growth has far outpaced our education system and training capabilities for developing a pool of skilled

information technology – and information security – professionals. So, we are short, both in industry and in government.

Certainly there have been efforts to incent universities to build robust information security programs, such as the National Centers for Academic Excellence in Information Assurance Education (CAEIAE) sponsored jointly by the National Security Agency (NSA) and DHS.⁶ Currently 93 universities have met the criteria for a national center, and students that graduate from these programs are eligible to apply for scholarships and grants through the Department of Defense Information Assurance Scholarship Program and the Federal Cyber Service Scholarship for Service Program. The Federal Cyber Service Scholarship for Service Program⁷ is a unique program designed to increase and strengthen the cadre of federal information assurance professionals that protect the government's critical information infrastructure. This program provides scholarships that fully fund the typical costs that students pay for books, tuition, and room and board while attending an approved institution of higher learning. Additionally, participants receive stipends of up to \$8,000 for undergraduate and \$12,000 for graduate students. The scholarships are funded through grants awarded by the National Science Foundation (NSF), and recipient students must serve at a Federal agency in an information assurance position for a period equivalent to the length of the scholarship or one year, whichever is longer.

These are laudable programs, but they are not without their own challenges. For example, designation as a national center does not guarantee grant funding, and students in the “cyber corps” program do not always find relevant, open positions in the government on a timely basis. An additional challenge for government cyber security professionals is that there is not a clear career path that includes training and advancement opportunities for cyberspace specialists in the federal government. Inevitably, skilled, trained, cyberspace professionals seek jobs in the private sector. While that is not bad for companies who are constantly looking for skilled cyber security personnel, it reflects an imbalance in the system and still sees shortages for everyone.

[question: is there a way to list – or reference a list of cyber security training appropriate to meet demands of industry and government?]

We cannot rely only on university education to help shore up our personnel resources for the future. We need to adjust our national education curriculum for K-12 years to reflect the new environment as well. Yes, it is science and math, certainly, and we welcome President Obama’s new commitment to education in science in math as part of a “national campaign to promote cybersecurity awareness and digital literacy from our boardrooms to our classrooms, and to build a digital workforce for the 21st century.”⁸ Specifically, the President’s Cyber Policy Review recommends, as part of its mid-term action plan, expanded support for key education programs (and R&D) and the development of a strategy to expand and train the workforce, including

⁶ http://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml

⁷ <https://www.sfs.opm.gov/>

⁸ http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/

attracting and retaining cybersecurity expertise in the Federal government.⁹ We welcome the recommendations, and industry looks forward to working with the government to help meet those objectives.

Conclusion

In sum, there are some key areas for short and longer term work on cyber security R&D and education and training needs.

We commend the Congress for its early focus on cyber security issues and this subcommittee for convening this panel today as part of your cyber security series. 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.

⁹ *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, p. 38, The White House; http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf