CYBER SECURITY R&D

HEARING

BEFORE THE

SUBCOMMITTEE ON RESEARCH AND SCIENCE EDUCATION

COMMITTEE ON SCIENCE AND TECHNOLOGY

HOUSE OF REPRESENTATIVES

ONE HUNDRED ELEVENTH CONGRESS

FIRST SESSION

JUNE 10, 2009

Serial No. 111–31

Printed for the use of the Committee on Science and Technology

Available via the World Wide Web: http://www.science.house.gov

U.S. GOVERNMENT PRINTING OFFICE

49–966PS WASHINGTON : 2009

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON SCIENCE AND TECHNOLOGY

HON. BART GORDON, Tennessee, *Chair*

JERRY F. COSTELLO, Illinois
EDDIE BERNICE JOHNSON, Texas
LYNN C. WOOLSEY, California
DAVID WU, Oregon
BRIAN BAIRD, Washington
BRAD MILLER, North Carolina
DANIEL LIPINSKI, Illinois
GABRIELLE GIFFORDS, Arizona
DONNA F. EDWARDS, Maryland
MARCIA L. FUDGE, Ohio
BEN R. LUJÁN, New Mexico
PAUL D. TONKO, New York
PARKER GRIFFITH, Alabama
STEVEN R. ROTHMAN, New Jersey
JIM MATHESON, Utah
LINCOLN DAVIS, Tennessee
BEN CHANDLER, Kentucky
RUSS CARNAHAN, Missouri
BARON P. HILL, Indiana
HARRY E. MITCHELL, Arizona
CHARLES A. WILSON, Ohio
KATHLEEN DAHLKEMPER, Pennsylvania
ALAN GRAYSON, Florida
SUZANNE M. KOSMAS, Florida
GARY C. PETERS, Michigan
VACANCY

RALPH M. HALL, Texas
F. JAMES SENSENBRENNER JR., Wisconsin
LAMAR S. SMITH, Texas
DANA ROHRABACHER, California
ROSCOE G. BARTLETT, Maryland
VERNON J. EHLERS, Michigan
FRANK D. LUCAS, Oklahoma
JUDY BIGGERT, Illinois
W. TODD AKIN, Missouri
RANDY NEUGEBAUER, Texas
BOB INGLIS, South Carolina
MICHAEL T. MCCAUL, Texas
MARIO DIAZ-BALART, Florida
BRIAN P. BILBRAY, California
ADRIAN SMITH, Nebraska
PAUL C. BROUN, Georgia
PETE OLSON, Texas

SUBCOMMITTEE ON RESEARCH AND SCIENCE EDUCATION

HON. DANIEL LIPINSKI, Illinois, *Chair*

EDDIE BERNICE JOHNSON, Texas
BRIAN BAIRD, Washington
MARCIA L. FUDGE, Ohio
PAUL D. TONKO, New York
PARKER GRIFFITH, Alabama
RUSS CARNAHAN, Missouri
BART GORDON, Tennessee

VERNON J. EHLERS, Michigan
RANDY NEUGEBAUER, Texas
BOB INGLIS, South Carolina
BRIAN P. BILBRAY, California

RALPH M. HALL, Texas

DAHLIA SOKOLOV *Subcommittee Staff Director*
MARCY GALLO *Democratic Professional Staff Member*
MELÉ WILLIAMS *Republican Professional Staff Member*
BESS CAUGHRAN *Research Assistant*

CONTENTS

June 10, 2009

Page

Witness List 2

Hearing Charter 3

Opening Statements

Statement by Representative Daniel Lipinski, Chairman, Subcommittee on Research and Science Education, Committee on Science and Technology, U.S. House of Representatives 9

Written Statement 10

Statement by Representative Vernon J. Ehlers, Ranking Minority Member, Subcommittee on Research and Science Education, Committee on Science and Technology, U.S. House of Representatives 11

Written Statement 12

Prepared Statement by Representative Eddie Bernice Johnson, Member, Subcommittee on Research and Science Education, Committee on Science and Technology, U.S. House of Representatives 12

Witnesses:

Dr. Seymour E. Goodman, Professor of International Affairs and Computing; Co-Director, Georgia Tech Information Security Center, Georgia Institute of Technology

Oral Statement 13

Written Statement 15

Biography 17

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

Oral Statement 17

Written Statement 19

Biography 22

Dr. Anita D'Amico, Director, Secure Decisions Division, Applied Visions, Inc.

Oral Statement 23

Written Statement 24

Biography 33

Dr. Fred B. Schneider, Samuel B. Eckert Professor of Computer Science, Department of Computer Science, Cornell University

Oral Statement 33

Written Statement 34

Biography 40

Mr. Timothy G. Brown, Vice President and Chief Architect, CA Security Management

Oral Statement 41

Written Statement 43

Biography 49

Discussion 49

Page

Appendix: Answers to Post-Hearing Questions

Dr. Seymour E. Goodman, Professor of International Affairs and Computing; Co-Director, Georgia Tech Information Security Center, Georgia Institute of Technology 68
Ms. Liesyl I. Franz, Vice President, Information Security and Global Public Policy, TechAmerica 73
Dr. Anita D'Amico, Director, Secure Decisions Division, Applied Visions, Inc. . 76
Dr. Fred B. Schneider, Samuel B. Eckert Professor of Computer Science, Department of Computer Science, Cornell University 80
Mr. Timothy G. Brown, Vice President and Chief Architect, CA Security Management 87

CYBER SECURITY R&D

WEDNESDAY, JUNE 10, 2009

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON RESEARCH AND SCIENCE EDUCATION,
COMMITTEE ON SCIENCE AND TECHNOLOGY,
Washington, DC.

The Subcommittee met, pursuant to call, at 10:04 a.m., in Room 2318 of the Rayburn House Office Building, Hon. Daniel Lipinski [Chairman of the Subcommittee] presiding.

BART GORDON, TENNESSEE
CHAIRMAN

RALPH M. HALL, TEXAS
RANKING MEMBER

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE AND TECHNOLOGY
SUITE 2320 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6301
(202) 225-6375
TTY: (202) 226-4410
http://science.house.gov

Subcommittee on Research and Science Education

Hearing on

Cyber Security R&D

Wednesday, June 10, 2009
10:00 a.m. – 12:00 p.m.
2318 Rayburn House Office Building

Witness List

Dr. Seymour Goodman
Professor of International Affairs and Computing and Co-Director,
Georgia Tech Information Security Center,
Georgia Institute of Technology

Ms. Liesyl Franz
Vice President, Information Security and Global Public Policy,
TechAmerica

Dr. Anita D'Amico
Director, Secure Decisions Division, Applied Visions, Inc.

Dr. Fred Schneider
Samuel B. Eckert Professor of Computer Science,
Department of Computer Science, Cornell University

Mr. Timothy Brown
Vice President and Chief Architect, CA Security Management

HEARING CHARTER

SUBCOMMITTEE ON RESEARCH AND SCIENCE EDUCATION
COMMITTEE ON SCIENCE AND TECHNOLOGY
U.S. HOUSE OF REPRESENTATIVES

Cyber Security R&D

WEDNESDAY, JUNE 10, 2009
10:00 A.M.–12:00 P.M.
2318 RAYBURN HOUSE OFFICE BUILDING

1. Purpose

The purpose of this hearing is to explore the state of federal cyber security research and development (R&D). The Subcommittee will receive testimony from a panel of outside experts about priorities and existing gaps in the cyber security research portfolio as well examine the adequacy of cyber security education and workforce training programs.

2. Witnesses:

- **Dr. Seymour Goodman,** Professor of International Affairs and Computing and Co-Director, Georgia Tech Information Security Center, Georgia Institute of Technology
- **Ms. Liesyl Franz,** Vice President, Information Security and Global Public Policy, TechAmerica
- **Dr. Anita D'Amico,** Director, Secure Decisions Division, Applied Visions, Inc.
- **Dr. Fred Schneider,** Samuel B. Eckert Professor of Computer Science, Department of Computer Science, Cornell University
- **Mr. Timothy Brown,** Vice President and Chief Architect, CA Security Management

3. Overarching Questions:

- Does the federal cyber security R&D portfolio adequately address existing security concerns as well as new and emerging threats? If not, what are the research gaps? Do the existing priorities for federal research investment reflect any risk assessment of current and future threats? Is the cyber security R&D portfolio appropriately balanced between long-range, game changing research, and research targeted toward incremental improvement?
- How can the Federal Government facilitate effective public-private partnerships and increase private sector engagement in addressing common research needs for cyber security? How can the Federal Government ensure that stakeholder outreach and the process for input into cyber security R&D planning are adequate?
- Is the "human factor" sufficiently integrated into the cyber security R&D strategy? If not, what new and continuing areas of basic research in the social and behavioral sciences could significantly improve our ability to design more effective technologies?
- What is the state of cyber security education? Are future cyber security professionals being adequately trained by colleges and universities to meet the demands of the private sector? What role can the Federal Government play in supporting formal cyber security education and training, and in educating the general public about protecting themselves and their networks against cyber threats?

4. Background

Information technology (IT) has evolved rapidly over the last decade, leading to markedly increased connectivity and productivity. The benefits provided by these advancements have lead to the widespread use and incorporation of information technologies across major sectors of the economy. This level of connectivity and the dependence of our critical infrastructures on IT have also increased the vulner-

ability of these systems. Reports of cyber criminals and nation-states accessing sensitive information and disrupting services have risen steadily over the last decade, heightening concerns over the adequacy of our cyber security measures. For example, in 2008 the payment processors of an international bank were penetrated allowing fraudulent ATM transactions. In 2007, a U.S. retailer was the victim of a cyber attack and the personal information of 45 million credit and debit card holders was compromised.

According to Symantec's *Government Internet Security Threat Report,* the telecommunications infrastructure was the predominant target of cyber attack in 2008. Some estimate that the number of cyber attacks is actually much higher because companies avoid reporting incidents due to fear over plummeting stock prices and the possibility of further attack. Firms that are subject to cyber attack typically observe a decline of one to five percent in their stocks, which translates into a loss of between $50 and $200 million for large companies.

In January 2008, the Bush Administration established through a series of classified executive directives the Comprehensive National Cybersecurity Initiative (CNCI). While the details of the CNCI are largely classified, the goal of the multifaceted initiative was to secure federal systems.[1] A number of security experts have expressed concern that the classified nature of the CNCI has prohibited active engagement with the private sector despite the fact that 85 percent of the Nation's critical infrastructure is owned and operated by private entities. While experts are concerned by the lack of transparency and public-private cooperation under the CNCI, they have also urged President Obama to build upon the existing structure rather than starting from scratch. In February 2009, the Obama Administration called for a 60-day review of the national cyber security strategy. The President's review required the development of a framework that would ensure that the CNCI was adequately funded, integrated, and coordinated with the private sector and Congress.

On May 29, 2009, the Administration released its 60-day review of cyberspace policy. The review team acknowledged the difficult task of addressing cyber security concerns in a comprehensive fashion due to the wide array of federal departments and agencies with cyber security responsibilities and overlapping authorities. According to the review, cyber security leadership must come from the top. To that end, the President plans to appoint a "cyber czar" who will oversee the development and implementation of a national strategy for improving cyber security. The appointee will report to both the National Security Council and the National Economic Council and will chair the Information and Communications Infrastructure Interagency Policy Council (ICI–IPC), an existing policy coordinating body to ensure "a reliable, secure and survivable global information and communications infrastructure." The review also emphasizes the need for the Federal Government to partner with the private sector to guarantee a secure and reliable infrastructure. Furthermore, it highlights the need for increased public awareness, the education and expansion of the IT workforce, and the importance of advancing cyber security research and development. The review contains the following action items that are relevant to the Committee's work.

Near-Term Action Items:

1. Initiate a national public awareness and education campaign to promote cyber security.
2. In collaboration with other Executive Office of the President entities, develop a framework for R&D 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 access to event data to facilitate developing tools, testing theories, and identifying workable solutions.

Mid-Term Action Items:

1. Expand support for key education programs and R&D to ensure the Nation's continued ability to compete in the information age economy.
2. Develop a strategy to expand and train the workforce, including attracting and retaining cyber security expertise in the Federal Government.

---

[1] The objectives of the CNCI have been assembled from various press releases and media reports. An overview of the CNCI is available in the CRS report entitled, *"Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations."*

3. Develop a set of threat scenarios and metrics that can be used for risk management decisions, recovery planning, and prioritization of R&D.
4. Encourage collaboration between academic and industrial laboratories to develop migration paths and incentives for the rapid adoption of research and technology development innovations.
5. Use the infrastructure objectives and the R&D framework to define goals for national and international standards bodies.

Cyber Security R&D

Cyber security related activities are conducted across the Federal Government, but three key agencies, NSF, DHS and DOD (specifically DARPA) fund the majority of cyber security R&D.

The task of coordinating unclassified cyber security R&D has been assigned to the Networking and Information Technology Research and Development (NITRD) program. The NITRD program, which consists of 13 federal agencies, coordinates a broad spectrum of IT R&D activities, but includes an interagency working group and program component area focused specifically on cyber security and information assurance (CSIA) R&D. The NITRD agencies have requested a total of $343 million for CSIA R&D in FY 2010.

In 2006, the interagency working group produced a federal plan for cyber security R&D. The recommendations of the working group were that federal CSIA agencies: should explore high-impact threats; should assess the security implications of emerging technologies; should examine ways to build security in from the beginning; and should create metrics for assessing cyber security. The working group also recommended sustained interagency coordination and collaboration; individual agency as well as interagency prioritization of cyber security R&D; the targeting of R&D investments into strategic needs; strengthened partnerships, including international partners; and more effective coordination with the private sector. Finally, the working group recommended the development of a subsequent roadmap or implementation document, which to date has not been produced. There is concern that while the NITRD program provides a mechanism for coordination and collaboration among agencies, a lack of strong leadership by the Office of Science and Technology Policy will result in a patchwork of mission-driven objectives that fail to advance a comprehensive cyber security R&D strategy. These concerns may be mediated by the release of the 60-day review and the President's pledge to make cyber security one of his key management priorities.

Federal Investments in Cyber Security and Information Assurance R&D

Agency	FY 2009 (dollars in millions)	FY 2010 (dollars in millions)	Change over FY 2009 Amount	Change over FY 2009 % Change
NSF	63.3	67.4	4.1	6.5%
NIH				
DARPA	125.4	143.6	18.2	14.5%
OSD & DoD research orgs.	71.1	70	-1.1	-1.5%
NSA	36.9	32.2	-4.7	-12.7%
NIST	23.4	29.3	5.9	25.2%
Total	320.1	342.5	22.4	7.0%

Agency Roles in Cyber Security R&D

NSF

With a budget of $127 million for FY 2010, NSF is the principal agency supporting unclassified cyber security R&D and education. NSF's request is an 8.6 percent increase above FY09 levels.

NSF's cyber security research activities are primarily funded through the Directorate for Computer & Information Science & Engineering (CISE). CISE supports cyber security R&D through a targeted program, Trustworthy Computing, as well as through a number of its core activities in Computer Systems Research, Com-

puting Research Infrastructure, and Network and Science Engineering. The cyber security portfolio supports both theoretical and experimental research.

The Trustworthy Computing program, funded at $67 million for FY 2010, is an outgrowth of NSF's Cyber Trust program, which was developed in response to the *Cyber Security R&D Act of 2003*. The program supports research into new models, algorithms and theories for analyzing the security of computer systems and data components. It also supports investigation into new security architectures, methodologies that promote usability in conjunction with protection, and new tools for the evaluation of system confidence and security.

In addition to its basic research activities, NSF's Directorate for Education & Human Resources (EHR) manages the Scholarship for Service program which provides funding to colleges and universities for the award of two-year scholarships in information assurance and computer security fields. Scholarship recipients are required to work for two years in the Federal Government, upon completion of their degree. EHR also supports the development of cyber security professionals through the Advanced Technological Education (ATE) program, which focuses on the education of technicians for high-technology fields.

DHS

Cyber security research in DHS is planned, managed, and coordinated through the Cyber Security Research and Development Center. The center not only supports the research efforts of the Homeland Security Advanced Research Projects Agency (HSARPA), but helps to coordinate the testing and evaluation of technologies, as well as technology transition. The FY 2010 budget includes $37.2 million for cyber security R&D at DHS; this is an increase of $6.6 million over FY 2009.

In addition to conducting R&D, DHS has an operational and coordination role in securing cyber space. The National Cyber Security Division (NCSD) is the operational arm of DHS's cyber security group and handles a host of tasks, including the analysis of cyber threats, the dissemination of cyber threat warnings, the facilitation of cyber security exercises, and the reduction of software vulnerabilities. The budget request for the NCSD is $400 million, an increase of $87 million above FY 2009. Within NCSD, The United States Computer Emergency Readiness Team (US–CERT) is tasked with monitoring federal non-classified computer systems and issuing warnings to both federal agencies and the public when an attack occurs. Recent GAO reports have criticized US–CERT, citing a lack of a national strategy, an absence of operational relationships with other key cyber security groups, both federal agencies and private entities, and an insufficient level of action in response to a cyber attack.

DARPA

DARPA is the principal R&D agency of the DOD; its mission is to identify and develop high-risk, high-reward technologies of interest to the military. DARPA's cyber security activities are conducted primarily through the Strategic Technology Office and the Information Assurance and Survivability project, which is tasked with developing technologies that make emerging information systems such as wireless and mobile systems secure. The budget request for the Information Assurance and Survivability project is $113.6 million in FY 2010. The project includes a variety of targeted programs, for example the Intrinsically Assured Mobile Ad-Hoc Network (IAMANET) program is tasked with designing a tactical wireless network that is secure and resilient to a broad range of threats, including cyber attacks, electronic warfare and malicious insiders. The budget request for IAMANET is $14.5 million. The goal of the Trustworthy Systems program, with a budget request of $11.1 million, is to provide foundational trustworthy computer platforms for Defense Department systems. DARPA is also examining potential supply chain vulnerabilities in the Trusted, Uncompromised Semiconductor Technology program (TrUST) by developing methods to determine whether a microchip manufactured through a process that is inherently "untrusted" (i.e., not under our control) can be "trusted" to perform just the design operations and no more. The budget request for TrUST is $33.5 million.

Finally, DARPA is developing the National Cyber Range (NCR). The NCR will provide a revolutionary environment for research organizations to test the security of information systems. The NCR will be capable of supporting multiple, simultaneous, segmented tests in realistically configured or simulated testbed environments and will produce qualitative and quantitative assessments of the security of various cyber technologies and scenarios. According to DARPA officials, the intent is have the NCR available for both classified and unclassified research. The budget request for the NCR is $50 million for FY 2010.

NIST

NIST conducts limited cyber security research to identify improvements in the development of standards and maintains a checklist of security settings for federal computers. Cyber security activities are conducted through NIST's Information Technology Laboratory which has a budget request of $72 million for FY 2010, including $15 million in support of the CNCI and $29 million for CSIA R&D. NIST's primary mission in cyber security is to protect the federal information technology network by creating cyber security standards for federal non-classified computer systems, identifying methods for assessing the effectiveness of security requirements, and conducting tests to validate security in information systems. These tasks were appointed to NIST in the *Computer Security Act of 1987.* The federal standards for computing systems help establish a base level of protection against intrusion, disruption and theft.

5. Questions for Witnesses:

Dr. Goodman and Dr. Schneider

- Does the current range of federally supported research adequately address existing cyber security threats 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?
- How can the Federal Government foster effective partnerships between academia and the private sector?
- 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?
- What role can the Federal Government play in educating the general public about protecting themselves and their networks against cyber threats?

Dr. Anita D'Amico

- How can the behavioral and social sciences contribute to the design and evaluation of more secure information technologies? What new and continuing areas of basic research in the social and behavioral sciences could significantly improve our ability to design more effective technologies in cyber security? Are there promising research opportunities that are not being adequately addressed?
- What is the nature of interactions and collaborations between behavioral and social scientists, and computer scientists and engineers? Is the Federal Government playing an effective role in fostering such collaboration?
- Does the current range of federally supported research adequately address existing 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?
- 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?

Ms. Franz and Mr. Brown

- 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?
- 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?
- What is the state of cyber security education? Are future cyber security professionals being adequately trained by colleges and universities to meet an-

ticipated 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?

- What role can the Federal Government play in educating the general public about protecting themselves and their networks against cyber threats?

Chairman LIPINSKI. This hearing will come to order.

Good morning, and I welcome you to today's hearing entitled *"Cyber Security R&D."*

Welcome to the Research and Science Education Subcommittee hearing on cyber security research and development. Information technology is an integral part of our daily lives. Computers, cell phones and the Internet have greatly increased our productivity and connectivity. Unfortunately, this connectivity and the dependence on our critical infrastructures on information technologies have increased our vulnerabilities to cyber attacks. For example, last year the Pentagon reported more than 360 million attempts to break into its networks, and just two weeks ago, a cyber attacker accessed the design plans for the $300 billion Joint Strike Fighter project.

But it is not just the Pentagon that needs to worry about cyber security. Cyber crime is a problem for businesses large and small, and for every single American. The FCC estimates that identity theft costs consumers about $50 billion annually, and even more alarmingly, it is the fastest-growing type of fraud in the United States. These are not just individual crimes or individual criminals. Increasingly, globalization and the Internet mean that sophisticated organized crime groups can mine information, selling it both nationally and internationally.

In 2007, nearly 50 million credit card records were taken when cyber criminals broke into computer systems used by the retailer TJ Maxx. Some analysts put the total cost of the breach at over $4 billion, and the stolen card data was used to defraud retailers nationwide. As a result of this, Walmart lost almost $8 million to fraudulent gift cards. Ultimately, 11 people were indicted including three U.S. citizens, two individuals from China, one from Belarus, one from the Ukraine and one from Estonia. This is what cyber attacks are about. It is a worldwide challenge to law enforcement and it can affect any American.

Improving the security of cyberspace is of the utmost importance and it will take the collective effort of the Federal Government, the private sector, our scientists and engineers, and every American to be able to accomplish this.

In order to realize the full benefits of information technology, we need advances in cyber security R&D. Cyber threats are constantly evolving and cyber security R&D must evolve in concert through a combination of near-term fixes and long-term projects that build a more secure foundation.

People are perhaps the most important part of our IT infrastructure, and according to experts, they are also the weakest link in many systems. Better cyber security education for both the general public and for current and future IT professionals is vital. However, there is still a lot we don't know about how humans interact with technology. Therefore, more research into social and behavioral sciences has the potential to significantly improve the security of our IT systems.

Today we will hear from witnesses who are actively engaged in efforts to improve the security of our digital infrastructure. I look forward to the witnesses providing valuable insight into the chal-

lenges we face in tackling this complex issue and the role of cyber security R&D and education in any comprehensive solution.

The Science and Technology Committee has a key role to play in improving cyber security, and to that extent, we are holding a series of hearings to examine various aspects of this issue. After we focus on R&D and education, next week our subcommittee will hold a joint hearing with the Technology and Innovation Subcommittee to hear how federal agencies are responding to the Administration's 60-day cyberspace policy review. And later this month, the Technology and Innovation Subcommittee will hold a hearing to assess the efforts of DHS and NIST.

There is no doubt that our use of the Internet and other communication networks is continuing to grow and evolve, and that threats from individual hackers, criminal syndicates and even other governments are growing and evolving too. I am glad the President is taking an active role, and there is no doubt in my mind that Administration leadership will help better define and prioritize cyber threats, coordinate the federal response and develop effective partnerships with the private sector. As chairman of this subcommittee, I look forward to working with my colleagues and the Administration to ensure the development of a strong cyber security strategy.

I want to thank all of our witnesses for taking the time to appear before the Subcommittee this morning and I look forward to your testimony.

Now the Chair will recognize Dr. Ehlers for an opening statement.

[The prepared statement of Chairman Lipinski follows:]

PREPARED STATEMENT OF CHAIRMAN DANIEL LIPINSKI

Good morning. Welcome to this Research and Science Education Subcommittee hearing on cyber security research and development.

Information technology is an integral part of our daily lives. Computers, cell phones, and the Internet have greatly increased our productivity and connectivity. Unfortunately, this connectivity and the dependence of our critical infrastructures on information technologies have increased our vulnerability to cyber attacks. For example, last year the Pentagon reported more than 360 million attempts to break into its networks. Just two weeks ago, a cyber attacker accessed the design plans for the $300 billion Joint Strike Fighter project.

But it's not just the Pentagon that needs to worry about cyber security. Cybercrime is a problem for businesses large and small, and for every single American. The FTC estimates that identity theft costs consumers about $50 billion annually, and that even more alarmingly, it's the fastest growing type of fraud in the United States. These aren't just individual criminals. Increasing globalization and the Internet means that sophisticated organized crime groups can mine information, selling it both nationally and internationally.

In 2007, nearly 50 million credit card records were taken when cyber criminals broke into computer systems used by the retailer TJ Maxx. Some analysts put the total cost of the breach at over $4 billion, and the stolen card data was used to defraud retailers nation-wide. Walmart lost almost $8 million to fraudulent gift cards. Ultimately 11 people were indicted, including three U.S. citizens, two individuals from China, one from Belarus, one from the Ukraine, and one from Estonia. This is what cyber-attacks are about: it's a world-wide challenge to law enforcement, and it can affect any American.

Improving the security of cyberspace is of the utmost importance and it will take the collective effort of the Federal Government, the private sector, our scientists and engineers, and every American to be able to accomplish this.

In order to realize the full benefits of information technology we need advances in cyber security R&D. Cyber threats are constantly evolving and cyber security

R&D must evolve in concert through a combination of near-term fixes and long-term projects that build a more secure foundation.

People are perhaps the most important part of our IT infrastructure, and according to experts, they are also the 'weakest link' in many systems. Better cyber security education for both the general public and for current and future IT professionals is vital. However, there's still a lot we don't understand about how humans interact with technology; therefore, more research into the social and behavioral sciences has the potential to significantly improve the security of our IT systems.

Today, we will hear from witnesses who are actively engaged in efforts to improve the security of our digital infrastructure. I look forward to the witnesses providing valuable insight into the challenges we face in tackling this complex issue and the role of cyber security R&D and education in any comprehensive solution.

The Science and Technology Committee has a key role to play in improving cyber security, and to that end, we are holding a series of hearings to examine various aspects of this issue. After we focus today on R&D and education, next week our subcommittee will hold a joint hearing with the Technology and Innovation Subcommittee to hear how federal agencies are responding to the Administration's 60-day cyberspace policy review. And later this month, the Technology and Innovation Subcommittee will hold a hearing to assess the efforts of DHS and NIST.

There is no doubt that our use of the Internet and other communication networks is continuing to grow and evolve, and that threats from individual hackers, criminal syndicates, and even other governments are growing and evolving too. I am glad that the President is taking an active role, and there is no doubt in my mind that Administration leadership will help better define and prioritize cyber-threats, coordinate the federal response, and develop effective partnerships with the private sector. As Chairman of this subcommittee, I look forward to working with my colleagues and the Administration to ensure the development of a strong cyber security strategy.

I want to thank all of our witnesses for taking the time to appear before the Subcommittee this morning and I look forward to your testimony.

Mr. EHLERS. Thank you, Mr. Chairman. Almost a decade ago, I was serving as a rapporteur for the NATO Parliamentary Assembly Committee on Science and was charged with the responsibility for writing a position paper on cyber security, and that was a real eye-opener to me. I had never investigated and obviously had to do a great deal of work to prepare the paper. We were of course dealing with more than just the commercial cyber security concerns, which are largely the concern today. We were dealing not only with people trying to find out what was on the federal cybernet but also how people could do damage to our entire cyber superstructure in the United States through various nefarious schemes. That was a real eye opener to me and today continues my education on this program.

Cyber security is of great concern to both the Federal Government and private industry, and that is quite a change from a decade ago when it was considered entirely the concern of the Federal Government. But this is an especially timely hearing since a little over a month ago the House passed a measure reauthorizing the *Networking and Information Technology Research and Development Act of 2009,* better known as NITRD. As you know, the NITRD program is responsible for the coordination of all the unclassified federal research and development efforts in federal security. However, cyber security efforts are only a small part of the overall NITRD mission, and I am glad that this hearing will focus special attention on this subject.

As we become more dependent on virtual information and services, security becomes more and more challenging to maintain. Fostering trust between the public and private sector will allow for the type of research partnerships necessary to keep our information secure and exchanging information between stakeholders is critical.

I am also particularly interested in learning how we are supporting the education and training of students in this rapidly changing field and whether the current mechanisms are adequate to ensure our national cyber security interests.

I look forward to learning from our witnesses today about their experiences in cyber security research, development and education and how we can strengthen our federal efforts in this area. I certainly thank you for your attendance and I am hoping to learn much more than I learned a decade ago when I first got involved in this field.

Thank you much for being here and I look forward to your testimony. I yield back.

[The prepared statement of Mr. Ehlers follows:]

PREPARED STATEMENT OF REPRESENTATIVE VERNON J. EHLERS

Cyber security is of great concern to both the Federal Government and private industry. This is a timely hearing, since a little over a month ago the House passed the measure reauthorizing the *Networking and Information Technology Research and Development Act of 2009* (NITRD). As you know, the NITRD program is responsible for the coordination of all the unclassified federal research and development efforts in cyber security. However, cyber security efforts are only a small part of the overall NITRD mission and I am glad that this hearing will focus special attention on this subject.

As we become more dependent on virtual information and services, security becomes more and more challenging to maintain. Fostering trust between the public and private sector will allow for the type of research partnerships necessary to keep our information secure, and exchanging information between stakeholders is critical. I am also particularly interested in learning how we are supporting the education and training of students in this rapidly changing field, and whether the current mechanisms are adequate to ensure our national cyber security interests.

I look forward to learning from our witnesses today about their experiences in cyber security research, development and education, and how we can strengthen our federal efforts in this area. Thank you for your attendance.

Chairman LIPINSKI. Thank you, Dr. Ehlers, and I always learn a great deal from you. It is always great to have you here. You always have better stories to tell.

Mr. EHLERS. Just remember they are stories.

Chairman LIPINSKI. If there are Members who wish to submit opening statements, your statements will be added to the record at this point.

[The prepared statement of Ms. Johnson follows:]

PREPARED STATEMENT OF REPRESENTATIVE EDDIE BERNICE JOHNSON

Good morning, Mr. Chairman and Ranking Member.

Cyber security is an area that is worthy of federally-funded research.

I appreciate you holding today's hearing. Members will be interested to know the status of research in this area as well the areas where there are knowledge gaps.

Consider the amount of communication and business that is done using computers and the Internet.

E-mail, music, social networking, shopping, and banking: all of these activities are conducted online.

Air traffic control is done using computers. Software manages electronic patient records. Imagine the chaos that would occur if part of that information was altered or otherwise compromised.

Our daily lives are so different from even twenty years ago. Internet security attacks can happen on a large scale and with serious consequences.

For example, in 2007, a U.S. retailer was victimized by a cyber attack. As a result, 45 million credit and debit card holders were compromised.

This past February, the Obama Administration called for 60-day review of the national cyber security strategy.

The review will require the development of a framework to ensure that the Comprehensive National Cybersecurity Initiative is adequately funded and coordinated.

The review has since been released, and some of the action items in it fall under the purview of the Science Committee.

Cyber security research is funded through several federal agencies, including the Defense Advanced Research Projects Agency (DARPA) and National Science Foundation.

This subcommittee will be interested to know whether the current range of federally-funded research is sufficient to understand and prepare for cyber security threats.

Members will also be interested to know whether there exists a strong pipeline of educated people to study cyber security.

If not, the Committee will want to know what federal programs are best suited to cultivate a next generation of cyber security analysts and researchers.

I would like to welcome today's witnesses.

The Committee values the depth of expertise represented on this panel and looks forward to your testimony.

Chairman LIPINSKI. At this time I would like to introduce our witnesses. First, Dr. Seymour Goodman is a Professor of International Affairs and Computing and Co-Director of the Georgia Tech Information Security Center at the Georgia Institute of Technology. Ms. Liesyl Franz is the Vice President of Information Security and Global Public Policy at TechAmerica. Dr. Anita D'Amico is the Director of the Secure Decisions Division at Applied Visions Inc. Dr. Fred Schneider is the Samuel B. Eckert Professor of Computer Science in the Department of Computer Science at Cornell University. And finally, Mr. Timothy Brown is the Vice President and Chief Architect for Security Management at CA Incorporated. As our witnesses should know, you will each have five minutes for your spoken testimony and your written testimony will be included in the record for the hearing. When you have all completed your spoken testimony, we will begin with questions and each Member will have five minutes to question the panel, and right now it is about 10:15. We are expecting votes at about 11:15, so we would appreciate if the panelists could stick to that five-minute timeframe and we will have a good amount of time then for questions.

So we will start here with Dr. Goodman. Dr. Goodman.

STATEMENT OF DR. SEYMOUR E. GOODMAN, PROFESSOR OF INTERNATIONAL AFFAIRS AND COMPUTING; CO-DIRECTOR, GEORGIA TECH INFORMATION SECURITY CENTER, GEORGIA INSTITUTE OF TECHNOLOGY

Dr. GOODMAN. Thank you, Mr. Chairman, Ranking Member Ehlers, distinguished Members and staff of the Subcommittee. In addition to my academic positions at Georgia Tech, I also serve or have recently served as Chair of the National Research Council Committee that authored *"Towards a Safer and More Secure Cyberspace,"* and as Vice Chair of the Institute for Information Infrastructure Protection—a research consortium of 27 universities, national labs and federally funded non-profits—and as the principal investigator of Georgia Tech's NSF-funded Scholarship for Service Program.

A large fraction of the American people, its businesses and government institutions have become increasingly dependent on network information technologies. We are at risk because these infrastructures are riddled with vulnerabilities and cannot be fully trusted, and there are malicious people greatly enabled by network

connectivity seeking to exploit those vulnerabilities. Like auto safety or public health, cyber security should be viewed as a broad societal issue requiring continued improved responses to dynamically changing circumstances.

These responses will require better, larger and more agile education and research programs and the effective and broad deployment of the output of those programs in timely ways. Technical progress will be of extreme critical importance but not in itself sufficient. Policy, economic and behavioral issues must also be addressed. In particular, market forces have failed to provide the Nation with a level of cyber security adequate for its needs. An authoritative, interdisciplinary study of how this may be changed would be of enormous benefit to the Nation.

I would like to raise two other specific subjects of both near- and long-term urgency and importance. The first is what I fear is a coming tsunami of insecurity due to the spread of cellular telephones and other mobile devices. The second concerns educating a professional workforce.

The ubiquitous spread of cell phones and other small increasingly powerful computers with wireless connections is likely to result in unprecedented opportunities for criminals, stalkers, industrial spies, foreign intelligence agencies and other unfriendly actors. Cell phone users number over 3.5 billion, already a majority of the world's population and vastly outnumber traditional Internet users. This is leading to increased possibilities for information insecurity, not least because of the huge increase in the number of connected potential malicious actors and potential victims. Attacks employed against other computers will be deployed against the mobile devices, especially as they become primary means of access to the Internet. There are many additional vulnerabilities because of battery limitations, the use of airwaves instead of wires, the ease with which devices and the information on them may be lost or stolen, particular forms of denial of service attacks and new target applications such as digital wallets.

The vulnerability of mobile devices potentially affects almost every American citizen and organization. Its international dimensions are without precedent. Research, development and deployment efforts to improve security will necessitate a solution to a large number of interdependent technical and business problems, and require researchers from multiple disciplines, and will depend on strong forms of involvement with the private sector and international institutions to ensure effective and widespread implementation.

A safer and more secure cyberspace will also demand many more professionals in the workforce on the front-lines defending organizations and infrastructures. This will require new faculty and curricula at a wide range of educational institutions.

I conclude by drawing your attention to one of the few efforts to grow this workforce on a national scale, the NSF Scholarship for Service Program. It provides scholarship support to U.S. citizens who must start their careers in the Federal Government. The results of this modestly funded program on the order of about $10 million per year have been impressive. Since 2003, 970 mostly Master's-level professionals from 34 universities across the country

have been placed in agencies. Many of them would not have chosen to study cyber security or work for the Federal Government without it. The government has done well in establishing this program. It should be continued and carefully augmented to have a more extensive impact.

Thank you for inviting me to testify. I will be happy to try to answer any questions that you have.

[The prepared statement of Dr. Goodman follows:]

PREPARED STATEMENT OF SEYMOUR E. GOODMAN

Mr. Chairman, Ranking Member Ehlers, and distinguished Members of the Subcommittee: Thank for you for the opportunity to appear before you today to discuss the subjects of *Cyber Security R&D* and Education.

I am Professor of International Affairs and Computing at Georgia Tech, where I Co-Direct two centers: the Georgia Tech Information Security Center and the Center for International Strategy, Technology, and Policy. I also serve, or have recently served, as chair of the National Research Council Committee that authored *Toward a Safer and More Secure Cyberspace* in 2007; as Vice Chair of the Institute for Information Infrastructure Protection (I3P), a research consortium of 27 universities, national labs, and federally funded non-profits; and as the Principal Investigator for Georgia Tech's NSF-funded Scholarship for Service Program.

A large fraction of the American people, its businesses, and government institutions have become increasingly dependent on networked information technologies. We are at risk because these infrastructures are riddled with vulnerabilities and cannot be fully trusted, and there are malicious people who are greatly enabled by network connectivity seeking to exploit those vulnerabilities. Cyber security must be viewed as a broad societal issue, in part because vulnerabilities in the general commercial or home computing environments have profound consequences for the vulnerability of many prominent or critical targets. It must also be recognized that cyber protection will be an ongoing need, requiring continually improved responses to dynamically changing circumstances.

These responses will require better and larger education and research programs, and the effective and broad deployment of the output of those programs in timely ways. Technical progress will be of critical importance, but not in itself sufficient. Policy, economic, and behavioral issues must also be addressed. In particular, as discussed in the NRC report, market forces have failed to provide the Nation with a level of cyber security adequate for its needs. An authoritative interdisciplinary research study on how this may be changed could be of enormous benefit to the Nation. We must also ensure that federally supported research has a broad impact on current and future security challenges. The 2007 NRC report, and the recently released NRC report *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* both note that much of cyber security research is classified, and thus unlikely to have much impact in improving civilian security.

I would like to address two particular subjects of both near- and long-term urgency and importance. The first is what I fear is a coming tsunami of insecurity due to the spread of cellular telephones and other mobile devices that contain substantial computing capabilities. The second addresses difficulties and progress with efforts to build the capacity to educate a professional workforce that is necessary to help achieve a safer and more secure cyberspace.

The ubiquitous spread of cell phones and other small, increasingly powerful computers with wireless connections is likely to result in unprecedented opportunities for criminals, hackers, terrorists, industrial spies, foreign intelligence agencies, and other unfriendly actors. Cell phone users currently number over 3.5 billion, a majority of the world's population, and vastly outnumber traditional Internet users, especially in developing nations. And cell phone use is growing faster than Internet use. In the next five to ten years, most of the people on the planet will likely be using powerful mobile devices for more personal and professional functions. And these devices may supplant desktop and laptop computers as the primary form of access to a much larger Internet.

This is leading to increased possibilities for information insecurity, not least because of the huge increase in the number of connected potential malicious actors and potential victims. Forms of attack currently employed against desktops and laptops will be deployed against mobile devices. In addition, there are many vulnerabilities more specific to them, because of battery limitations, the use of airwaves instead of wires, the ease with which they and the information on them may

be lost or stolen, particular forms of denial of service attacks, and new and attractive target applications like digital wallets and pocket ATMs.

The vulnerability of mobile devices potentially affects almost every American citizen and organization. Its international dimensions are without precedent. Any research, development, and deployment effort to improve security will necessitate solutions to a large number of interdependent technical and business problems, will require researchers from multiple disciplines, and will depend on strong forms of involvement with the private sector and international institutions to ensure effective and widespread implementation.

So we have warning of looming security problems in a rapidly expanding domain. We have lots of experience and mistakes with the Internet. This time, will we be able to get ahead of the problem and make the world of mobile cyberspace safer and more secure before the Tsunami forms, builds momentum, and hits us?

A safer and more secure cyberspace will also require many more professionals in the workforce on the front lines defending organizations and infrastructures. To produce these people, we need to increase the capacities of a wide spectrum of educational institutions, adding capable faculty and extensive new curricula, neither of which can be created overnight.

I want to draw your attention to one of the few efforts to grow this workforce on a national scale: the National Science Foundation Scholarship for Service Program (SFS). This program provides some support for universities to build their faculty and curriculum to enable the offering of concentrations in information security and assurance. It primarily provides up to two-year scholarship support to U.S. citizens in the best of these programs who must (although most see it as an opportunity, rather than an obligation) work in the Federal Government for at least the same number of years as they were supported by the scholarship. For embryonic information security programs many universities find that these students help provide a critical mass for enrollments for several early years. Graduates help improve the security of the government's information systems and the agencies that depend on them, but more broadly these programs, once established, graduate others who work elsewhere to improve security postures.

The results of this modestly funded program (recently on the order of $10 million per year) have been impressive. Since 2003, 970 mostly MS-level professionals from 34 universities across the country have been placed in agencies. Many programs at these universities may not have become viable without the NSF support, and the majority of the scholarship students would not have chosen to study cyber security and work for the Federal Government without the visibility and inducements of the program. Some of these universities have become assets to other regional educational institutions, including schools for law enforcement and two-year colleges.

Most of the curriculum being developed and offered is in the form of computer science courses. These are necessary, but not sufficient, to the educational needs. There is a need for multi-disciplinary courses that introduce important matters relating to management, law, policy, human behavior, and the international dimensions of cyber security. Only a small number of universities have serious courses of this kind. They should be designed with the intention of facilitating export to many institutions since few have faculty in positions to work on these aspects at this time. Perhaps an NSF program might help address such needs?

The government has done well in establishing this program, to its own direct benefit and the country's more generally. It should be continued and carefully augmented to have a more extensive impact. Thoughts along those lines might include the range of degrees supported with the scholarships, and the range of employment options permitted, for example, teaching at two-year colleges or in parts of the country with particular needs.

A major capacity building bottleneck that affects all levels of educational and research needs is the production of Ph.D.s in this area. Today, at most levels of tertiary education, a Ph.D. is a necessary credential for a long-term career. Many who are working these problems as researchers and educators are recent additions to the ranks, as newly minted Ph.D.s or converts from other fields. Building the doctoral ranks takes time and others who can provide close supervision. However the task is not insurmountable; it will take a concerted effort that should be pursued with national-level vigor.

This concludes my statement. I will provide some additional written material to the Subcommittee's staff.

Thank you for inviting me to testify. I would be happy to try to take any questions you have.

BIOGRAPHY FOR SEYMOUR E. GOODMAN

Seymour (Sy) E. Goodman is Professor of International Affairs and Computing at the Sam Nunn School of International Affairs and the College of Computing, Georgia Institute of Technology. He also serves as Co-Director of the Center for International Strategy, Technology, and Policy and Co-Director of the Georgia Tech Information Security Center.

Prof. Goodman studies international developments in the information technologies and related public policy issues. In this capacity, he has over 200 publications and served on many academic, government and industry advisory, study, and editorial committees. He has been the International Perspectives editor for the Communications of the ACM for almost 20 years, and has studied computing on all seven continents and in about 90 countries. He recently served as Chair of the Committee on Improving Cybersecurity Research in the United States, National Research Council, Computer Science and Telecommunications Board, National Academies of Science and Engineering.

Immediately before coming to Georgia Tech, Prof. Goodman was the Director of the Consortium for Research in Information Security and Policy (CRISP), jointly with the Center for International Security and Cooperation and the School of Engineering, Stanford University. He has held appointments at the University of Virginia (Applied Mathematics, Computer Science, Soviet and East European Studies), The University of Chicago (Economics), Princeton University (The Woodrow Wilson School of Public and International Affairs, Mathematics), and the University of Arizona (MIS, Soviet and Russian Studies, Middle Eastern Studies).

Prof. Goodman was an undergraduate at Columbia University, and obtained his Ph.D. from the California Institute of Technology where he worked on problems of applied mathematics and mathematical physics.

Chairman LIPINSKI. Thank you, Dr. Goodman.

The Chair now recognizes Ms. Franz.

STATEMENT OF MS. LIESYL I. FRANZ, VICE PRESIDENT, INFORMATION SECURITY AND GLOBAL PUBLIC POLICY, TECHAMERICA

Ms. FRANZ. Chairman Lipinski, Ranking Member Ehlers and distinguished Members and staff of the Subcommittee, thank you for the opportunity to testify and to provide the technology industry's perspective on cyber security research and development and on the cyber workforce. I respectfully submit my written statement for the record.

As innovators of technologic solutions as well 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. R&D and education for a skilled workforce are precisely those areas that are strategic in nature and require immediate and sustained attention. I will address both in my testimony today.

Currently, we expect about two-tenths of the Federal Government's 2009 budget to go towards cyber security R&D. That amounts to about $300 million, which in today's highly networked and highly interdependent environment is deemed by most to be inadequate. We welcome the Comprehensive National Cybersecurity Initiative's R&D efforts under the Cyber Leap Year project to identify the most promising game-changing ideas to reduce vulnerabilities and we look forward to the results of that process. We also welcome the R&D focus in President Obama's Cyberspace Policy Review. We are very pleased with the report's inclu-

sion of R&D, its acknowledgment of the need for public-private collaboration and we view this new impetus for a framework as an opportunity to pursue greater cooperation.

Companies conduct R&D all the time to develop products and services needed in the marketplace. On the more strategic side, many companies also participate in partnership efforts to assess and mitigate risk to the IT sector including R&D under the National Infrastructure Protection Plan partnership framework. However, there is no institutionalized mechanism for providing input into the federal R&D portfolio development but through increased collaboration we are enhancing the mutual understanding on R&D efforts between industry and government. Increased coordination is crucial to identify gaps and fill them and to avoid unnecessary duplication between the projects that industry might undertake and those that the government might undertake. That is why we recommend a more formal mechanism be put in place for industry's input, and importantly, for public-private collaboration where necessary and feasible—and especially in projects that are national in nature and will reset the paradigm.

Another interesting concept is a national clearinghouse to serve as an intermediary between government, industry, and other stakeholders on dialogue and collaboration for R&D and related projects.

I would like to take my remaining time to focus on the cyber security workforce. The adoption of technology has far out-paced our education and training capabilities for developing a pool of skilled IT security professionals, so we are short everywhere. Interestingly, on the way home from work yesterday I was behind a city bus in D.C. and there was an advertisement for a job fair for IT professionals for DISA and JTFGNO, the DOD joint taskforce global network operations. Believe me, that is something I never thought I would see on the back of a bus, but it is one example of active government recruiting efforts in this area.

Existing federal cyber-related education and service corps programs like the one that Dr. Goodman mentioned are laudable ones but they are not without their own challenges. Recruitment and retention are both difficult. We need to continue efforts to improve our university and existing job programs and develop a relevant government career path to help meet and retain the demand. In addition, we cannot rely only on a university education to help shore up our personnel resources for the future. We need to adjust our national education curriculum for the K through 12 years to reflect the new environment as well. Kids today are much more computer savvy than we ever dreamt of being so we need to match and magnify that capability for our future.

In sum, we have much to do but we welcome recent efforts and are optimistic about the opportunity to work together to leverage the momentum and make progress.

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

[The prepared statement of Ms. Franz follows:]

PREPARED STATEMENT OF LIESYL I. FRANZ

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 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 1,500 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 five 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 cyber security 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]

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

[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/csis/pubs/081208_securingcyberspace_44.pdf*

(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 cyber security 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.

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 invest-

---

[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

ment 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 life cycle: 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.

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 out-paced 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 Program[7] 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.

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 cyber security 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 attracting and retaining cyber security 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.

BIOGRAPHY FOR LIESYL I. FRANZ

Liesyl Franz is Vice President for Information Security and Global Public Policy at TechAmerica, working with industry and government leaders on such issues as cyber security, critical infrastructure protection and Internet Governance. In this role she leads TechAmerica's strategic and tactical efforts on public policy in these areas with the Administration, Congress, and international organizations. In addition, she represents TechAmerica in the Information Technology Sector Coordinating Council (IT SCC) under the National Infrastructure Protection Plan (NIPP), where she currently serves as Secretary.

---

[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/*

[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*

Liesyl joined TechAmerica (previously ITAA) from the Department of Homeland Security, where she served as Deputy Director for Outreach and Awareness and Director for International Affairs and Public Policy at the National Cyber Security Division (NCSD). She led programs in the areas of global affairs, public policy, communications and messaging as well as stakeholder outreach, including building international partnerships, coordinating public relations for key events such as the Cyber Storm National Cyber Exercise and conferences, and managing events for National Cyber Security Awareness Month held annually in October.

Prior to her service at DHS, Liesyl was Director for Global Government Affairs at EDS Corporation working on cyber security, privacy, financial services, and trade issues, and she worked with the Coalition of Service Industries where she managed industry's participation and input into services trade negotiations in the World Trade Organization (WTO).

Liesyl was recognized in 2005 by the Women's High Tech Coalition with the Women in Cyber Security Award for her contribution to public-private partnerships and international collaboration in cyber security. She holds a BA in Political Science from the University of Texas at Austin and an MA from the Elliott School of International Affairs at George Washington University.

Chairman LIPINSKI. Thank you, Ms. Franz.

The Chair now recognizes Dr. D'Amico.

STATEMENT OF DR. ANITA D'AMICO, DIRECTOR, SECURE DECISIONS DIVISION, APPLIED VISIONS, INC.

Dr. D'AMICO. Thank you, Mr. Lipinski and Mr. Ehlers and the Subcommittee. I am the Director of Secure Decisions, a division of Applied Visions, which is a small business in New York. We specialize in improving the situational awareness of cyber defenders. We help them understand what is going on in the network, find suspicious activity and figure out what to do about it.

I would like you to note the name of my division, Secure Decisions. As a psychologist, I wanted the name to reflect the importance of human decisions of security professionals. I have since learned we need to improve the decisions of a lot of people, not just security professionals. We must teach programmers to make secure design decisions that build security into software from the beginning and not just tacked on at the end. Home users need to be educated about the risks of their Internet decisions before they click on the interesting ad. Students need to learn the ethics of using computers for entertainment and online socializing. We need to change the culture to make good security second nature to all of us and not something that we try to avoid.

But this change in culture is not going to be achieved by a bunch of smart engineers designing new intrusion detection systems. This cultural shift requires the expertise of those who understand how to change minds, that is, the social sciences. So my first take-away to this committee is that cyber security education is not just for security wonks. We need to broaden the base of those we teach and involve the social sciences in the education of this larger audience.

My second take-away is that we have to get better at training the people whose job is computer security. New graduates with information security degrees have little opportunity to learn by doing as prior generations had to do. Young soldiers in particular have little time to become proficient before rotating out to their next assignment. How do we improve this? First, we need to formalize the mentorship of the new generation. Before the old guard retires, they need to share their knowledge with the newbies but

mentorship is not something that comes naturally to everyone and that is where the social sciences can help.

Second, we need better ways for security practitioners to share information with their own peers. New collaboration techniques developed with social scientists can make a difference.

Third, we need to train professionals on realistic yet safe training networks where they can practice their skills without bringing down eBay. This is also needed for researchers to test out their new technologies. And speaking of research, few results of federally funded cyber R&D ever make it into the real-world operations. As a taxpayer, I find this disturbing. Little research funding is directed at technology transition. Once the paper is published, many researchers and government program managers feel their job is done. The rest of the work, making the technology affordable and usable, is abandoned in the hope that someone else will pay for it. Furthermore, academicians are judged by their publication history but few scientific journals consider technology transition worthy of their attention.

And finally, computer scientists are often just not into the softer side of security, that is, how people use the technology, yet studying how people use cyber security technology is exactly what is needed to improve technology transition. We need to study the usability of systems and to test them in operational environments where real people get to try them out. So my third take-away to the Committee is that the government should fund projects through the technology transition phase and should use transition to evaluate both researchers and the government program managers.

My last message is about how little input the private sector has in the federal research portfolio. With the exception of a few ISACs, the private sector has no voice. Furthermore, the private sector cannot easily tap into the results of the federally funded research. I believe the government should require researchers to publish their results in the trade magazines and the online forums where security professionals communicate, not just in the scientific journals.

In closing, please keep in mind what information security experts often say: Cyber security is about people, processes and technology. As educators and researchers, we must look at all three of these things, not just technology. I am one of the few psychologists actively engaged in cyber security R&D. I am surrounded by computer scientists and engineers, but I hope with this committee's support that in the future my position as a psychologist in cyber security will just be a bit less lonely. Thank you.

[The prepared statement of Dr. D'Amico follows:]

PREPARED STATEMENT OF ANITA D'AMICO

Introduction

Thank you Chairman Lipinski, Ranking Member Ehlers, and Members of the Subcommittee for the opportunity to testify on this important topic.

I am the Director of the Secure Decisions division of Applied Visions, Inc. I was educated as an experimental psychologist; applied my skills as a human-factors psychologist in maritime ship operations, manned spacecraft and surveillance aircraft; and for more than 15 years have been involved in various aspects of cyber R&D. For the past nine years I have been directing the Secure Decisions division of AVI

to enhance the situational awareness of those defending our critical computing infrastructure.

As a small business engaged in custom software development, Applied Visions recognized over a decade ago the frailty of our country's IT infrastructure and the importance to our country of instilling and monitoring good cyber security practices. AVI invested in a new division dedicated to improving the situational awareness of those responsible for defending our critical IT infrastructure. In under ten years the Secure Decisions division has become, even as a small business, a leader in cyber situational awareness R&D.

We perform R&D sponsored by the Department of Defense, the Intelligence Community, and the Department of Homeland Security. And from my perspective one of our most valuable contributions is when we transfer that R&D into usable products for use in both DOD and in industry. We publish research results—those that we are permitted to disseminate—in peer-reviewed journals. We partner with large companies like Raytheon and ITT, universities including Johns Hopkins and George Mason, and other small businesses.

We owe our continued growth in cyber security research in part to the U.S. Government's *Small Business Innovation Research* (SBIR) program. Our company is a testimony to the valuable role that SBIRs play in transforming cyber security research into operationally usable software systems and products. Unlike many federally-funded R&D programs that have little accountability for the ultimate operational utility of their research, the SBIR structure holds us accountable for—and rewards—the transition from early stage innovative concepts to prototype development and technology transition planning, all within a typical SBIR lifespan of three years.

The Human Element in Cyber Security

We named our division "Secure Decisions" to recognize the importance of *human decisions* in cyber security. As a psychologist working in a field predominated by computer scientists, I chose a name that reflected our goal to enhance the *situational awareness* and decision-making of cyber security practitioners. Of course, security practitioners are not the only individuals whose decisions make our critical computing infrastructure more or less secure. Many others, including home-users of computers, policy-makers, cyber lawyers, software developers, and educators, make us all more or less secure through their individual actions.

The current emphasis in cyber security R&D has been technological: creating or improving tools to enforce security. While this is indeed necessary, there is a significant *human* element to the problem that cannot be ignored. As researchers and educators, we must address all the many different roles that we humans play in cyber security, beyond just the security practitioner who administers firewalls, tunes intrusion detection systems, and monitors networks. We must also educate the software developer, lawyer, policy-maker, and all of us users who are unwitting accomplices of the attacker. The recommendations in the Cyberspace Policy Review just issued by the White House[1] recognize this.

Let's look at the software developer as one example of the need for enhanced security education. From the very start of the software life cycle—creating the software itself—software developers are inadequately schooled in how to program securely; security is often added on afterwards. Rewards are given for speed to market, not for creating secure software. For example, just two programming errors resulted in more than 1.5 million web site security breaches during 2008.[2] And all too often, the developer's initial response to the discovery of a vulnerability is something akin to "gee, we never thought a user would do *that* with it." We must change the way that programmers go about understanding the needs and behaviors of us as users, and in creating the software that we use.

Technical solutions must be easily deployable and usable. Gaining a deeper understanding of how people use technology by bringing together computer science and the behavioral sciences can make our technological breakthroughs actually useful and relevant to society.

We then must educate the cyber policy-makers and legal professionals in the fundamentals of confidentiality, integrity, and availability of information systems so that they understand the context in which they regulate and prosecute. The law generally has lagged far behind technology; we need technology-savvy courts to keep

---

[1] Cyberspace Policy Review (2009); *http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf*

[2] SANS Security Leadership Essentials for Managers: Experts Announce Agreement on the 25 Most Dangerous Programming Errors—And How to Fix Them, January 12, 2009; *http://www.sans.org/top25errors/?utm_source=web&utm_medium=text-ad&utm_content=Announcement_Bar_20090111&utm_campaign=Top25&ref=37029*

pace with the changing landscape. Few lawyers are sufficiently schooled in technology and security issues to be able to understand the problem well enough to decide whether or not proposed solutions to the problem are legal—and as a result, the usual answer is "no."

And finally, we must educate the rest of us—the teeming masses who actually *use* the software and cyber infrastructure of the Nation—in how to better understand the risks associated with that use, and how to make better decisions.

The cornerstone to this good security decision-making is our understanding of risk. Like most of life, security is about making decisions and choosing between options—making trade-offs between security and convenience, risk and comfort, safety and freedom. Overall, we're not bad at making security trade-offs.[3] The problem we have right now is that our understanding of risk, our basis for making these choices about security; is still based primarily on our physical environment and life as it has been for thousands of years. Our ability to understand, evaluate, and react to risks has not yet acclimated to our *current* environment, meaning the realities of the 21st century and cyberspace. Our *perceived* risk and the *actual* risk do not match, and we often make the wrong decisions as a result.

Therefore, part of raising the awareness of our citizens is to educate them in the actual, rather than the perceived, risks of traveling through cyberspace.

The State of Cyber Education

The current approach to cyber education falls far short of adequately preparing this universe of developers, practitioners, and users for life in the cyber world. Current education is focused on training security practitioners and educating computer scientists, but little is being done for all of the other roles: security practitioner, home user, business owner, software and hardware designer/developer, policy-makers, legal professionals, and even young students using the Internet.

Emphasis on Technology and Not People

Information security is often said to be about "people, process, and technology." Technological change can almost be taken for granted, given the natural inclination of engineers and technologists to constantly improve things. Instead, *changing how people think and the process by which we go about doing things should be our primary concern.* We *should* be developing a new breed of multi-disciplinary cyber security experts educated in the areas of *people,* such as psychology and organizational behavior, and *processes,* such as management, business process, and the law.

There has indeed been an increase in the number of academic institutions offering undergraduate and graduate degrees related to cyber and information security, but the majority of these programs are still technology-focused: computer science, computer engineering, electrical engineering, and so forth. *This is not enough.* Technology can shore up our defenses, but an emphasis on the *social* sciences can change the way we look at things: how we as a society view the risks and trade-offs in the digital world, and how we make those day-to-day decisions that have such a significant impact on the safety of our travels in cyberspace.

Unfortunately, there are not many examples of the collaboration between the social sciences and the computer sciences required to achieve this shift in education. Conferences like the *Workshop on the Economics of Information Security* and the *2008 Workshop on Security and Human Behaviour* are initiating a dialogue between technologists and social scientists, and we are beginning to see encouraging signs of this collaboration at the educational level. In addition, a workshop next month at the National Academy of Sciences, *Usability, Security, and Privacy of Information Systems,* is focused on identifying new research areas in "usable security" and will influence the research agendas of both NSF and NIST, which are sponsoring the workshop.

Visionary leadership is needed to achieve these changes in educational philosophy. As long as technology is viewed as the end-all of cyber security research and education, the focus will remain on problems in that area. And even if technology development remains the focus of our cyber security research and education, we have several major hurdles to overcome. One hurdle is the shortage of U.S. citizens who are acquiring the requisite math and science skills needed to teach and conduct hard research in cyber security.[4] This leaves many of the hard technology questions

---

[3] Schneier, Bruce. (2008) *The Psychology of Security. http://www.schneier.com/essay-155.html*, Published Online.

[4] Zweben, Stuart. Computing Degree and Enrollment Trends, from the 2007–2008 CRA Taulbee Survey, 2008, at 4, *www.cra.org/taulbee/CRATaulbeeReport-StudentEnrollment-07-08.pdf*

unanswered by our own citizens. Another hurdle—and this one I feel very strongly about—is the limited transfer of research findings into real-world use. Advanced education programs (such as for a Ph.D. in Computer Science or Information Systems) emphasize *publication* rather than transfer of findings into real practice. The system of grants that fund the work of students and their professors places more value on prior publications than practical results. We need to transition the research into the everyday world of Information Technology.

There are encouraging examples of such visionary leadership in interdisciplinary security. New York University, for example, recently merged with Brooklyn Polytechnic University, and quickly set out to build bridges between their engineering and social science communities. They now have a program combining Economics with Computer Science. Georgia Tech Information Security Center (GTISC) also recognizes the importance of interdisciplinary studies, and has launched a cooperative effort between their College of Computing and the Sam Nunn School of International Affairs. Despite these forward-thinking programs, there are few if any educational opportunities in cyber security that combine psychology, anthropology, or sociology with computer science.

Educational Challenges in the Military

The military is also wrestling with this problem, although from a different perspective: they see the need for cross-disciplinary education to incorporate the social sciences into cyber operations in order to better understand the impact of cyber operations on both friend and foe—a form of "battle damage assessment" for cyber warfare. This interdisciplinary approach needs to become the norm rather than the exception: cross-disciplinary education needs to be not only encouraged, but required.

The DOD faces other educational challenges that are somewhat unique to their organizational model. In fact, there are two characteristics of the DOD model that work together to make things quite difficult: incoming technical staff are more often chosen by aptitude than by experience, so that training must start at the most rudimentary level. And, the military tends to rotate people through posts on a regular basis, so that once they achieve some level of competency in cyber security they are likely to be transferred to some other discipline. This is further exacerbated by the fact that technical positions—such as Computer Network Defense—are not known to be a path to advancement (as opposed to traditional combat roles), and hence suffer high turnover.

Conti and Surdu[5] cite these challenges, among others, in their rationale for creating a fourth branch of the service—a peer to Army, Air Force, and Navy—to take on Cyberspace. This has cultural significance. They propose that top-notch cyber talent will clamor to join a service where cyber excellence is viewed as a path to advancement, and where just being a member of that service is a point of pride (as the Marines have achieved with their image as "The Few, The Proud . . ."). They observe that many young technically-talented individuals make critical decisions in their formative years that influence the direction of their lives. Perhaps the most important decision made by these rising cyber stars is whether or not to engage in illegal activity, like hacking. Creating an elite cyber organization, complete with positive role models, will give these people a chance to make the right choices in their lives.

Educating the Practitioners

Security practitioners have traditionally been *trained* rather than *educated:* the emphasis has been on the practical application of tools and techniques to defend the network, rather than on gaining understanding of the principles and behaviors that inform cyber security. The "old guard" practitioners learned about computer security *after* their formal education was completed, through a form of on-the-job-training as they "wrote the book" on security best practices in the early years. Current practitioners may have had *some* formal education or training, perhaps a degree in computer science or a few courses that led them to obtain some certification, but most of their real learning still happens on-the-job. What neither group realizes is that much of that on-the-job training—which they view as "learning the ropes" with tools and techniques for security—is in fact teaching them about the behavioral and social characteristics of their adversaries. The newest; upcoming generation is indeed getting more formalized education—for example, an MS in Information Security is

[5] Conti, Lt. Col. Gregory and Surdu, Col. John "Buck." "Army, Navy, Air Force, and Cyber—Is it Time for a Cyberwarfare Branch of the Military?" *IA Newsletter,* Vol. 12 No. 1, Spring 2009, *http://iac.dtic.mil/iatac*

now an option at many universities—but they lack the *context* for that education. Without real-world experience, and without including behavioral and social sciences in their education, they too will not gain a real understanding of the problems or of their adversaries until they have been on the job for a while.

A few years ago we had an opportunity to conduct a formal Cognitive Task Analysis of nearly eighty information assurance analysts in the DOD and the Intelligence Community.[6,7] We learned from that analysis that *mentorship* of network defenders is very important. Rapidly transferring corporate knowledge typically acquired through years of experience from old guard to new guard will be particularly important in the coming years as the first generation of network defenders retires. One area ripe for research is how to improve this mentorship to maximize the value of learning from the more-experienced to the less-experienced practitioner. Social science work on learning, mentorship, and collaboration can serve this need.

We also learned that the *personality characteristics* of entry-level network defenders are perceived by experts as equally or more important than their technical education. Such characteristics as curiosity, perseverance, assertive questioning, and good communication skills were considered strong markers of future success of an entry level defender. How do we select for and train these characteristics in our future cyber workforce to ensure that our defenses are as strong as possible? This is answered by the social sciences as much as by the technical disciplines.

Educating the Developers

The emphasis on "securing the perimeter" of networks is a side-effect of a more fundamental issue: security is all too often an afterthought. We build flawed software and then expend countless resources trying to patch the cracks and shore up the defenses. And when we do build flawed software products, the pressure to bring these products to market causes many to be released before adequate security testing has taken place. All of this raises questions about current software engineering pedagogy.

We need to teach secure coding practices—and, more importantly, we need to convey a fundamental understanding of the importance of security—from the very start, in high school computer science classes. Most of our computer science programs in higher education teach students the fundamentals of developing software and systems, and culminate with students building some hardware or software object, but little attention is generally given to the design and implementation of security within these objects.

Systems sometimes fail because the engineers considered a very narrow range of threats; again, the issue is a lack of understanding of the actual risks in the modern world. Information security needs to be an integral part of the core curriculum of computer science for both programmers and engineers. We must teach software developers and systems engineers how to go beyond just functional requirements in the design phase. They need to understand and anticipate all of the ways that experts and non-experts may use their systems. Usability and security testing needs to be performed side-by-side with functional and performance testing during development; students need this as part of their basic education.

Educating the Users

The most difficult audience to get a handle on, but one that desperately needs more education, is "the rest of us"—all of us who use these technologies, who suffer the consequences of failed security, and who all-too-often serve as unwitting accomplices to an attack.

We Need Realistic Test Data

Another challenge relevant to the whole educational and research spectrum is the need for more realistic testing and evaluation of cyber technologies and processes. In most disciplines some form of real-world experimentation eventually becomes practical and necessary; for example, psychologists can evaluate human subjects and compare the results against control groups. In the cyber world this is exceptionally difficult: one cannot perform security experiments on an operational network (let

[6] D'Amico, A. & Whitley, K. (2005). Achieving cyber situational awareness: A cognitive task analysis of information assurance analysts. In *Proceedings of the Human Factors and Ergonomics Society 49th Annual Meeting,* Orlando, FL, pp. 229–233.

[7] D'Amico, A. & Whitley, K. (2007). The real work of computer network defense analysts: The analysis roles and processes that transform network data into situation awareness. In *Proceedings of the Workshop on Visualization for Computer Security,* Springer-Verlag Berlin Heidelberg, pp. 19–37.

alone on the Internet), yet "simulating" such an environment is a huge challenge. Many researchers have built small-scale simulated networks in the lab, but the human element—real people using the network for real tasks—is completely missing and quite difficult to simulate. Realistic training and test data that can scale to the size of large networks is needed to add operational realism to training and research, and to increase the applicability to real world conditions and the potential transfer to implementation. With this sort of realistic simulation and test data we can properly prepare practitioners and developers to operate in the cyber world; without it, they have no other choice but to "learn by doing" in the "real world," with risks and inefficiencies that implies.

The Contribution of Social Sciences to Computer Security

The social and behavioral sciences can play a valuable role in studying and changing the various cultures—software developers, college students, and especially home computer users—so that individuals and societies engage in secure practices almost without ever thinking about them.

We need to understand why our perception of security risk does not match reality. Risk perception is critical to helping us understand how to motivate secure behavior, make better decisions, and create policies that discourage destructive or invasive behavior through real consequences.

We need to apply what we know about cultural influence to creating cultures that are supportive of secure and private computing.

Collaborative Techniques

Human collaboration is an important means for analyzing information about potential attacks. There are numerous instances where one government agency or commercial organization was aware of a serious attack but did not have the authority, means or motivation to share that information.

One group working to bridge this gap at the *organizational* level is the *Information Sharing and Analysis Centers* (ISAC) Council. There are several individual member councils that focus on various areas of critical infrastructures, such as Communications and Information Technology, but this group and its members represent the exception, not the norm, and information-sharing is particularly problematic within the government.

But we also must foster collaboration at the *individual* level, and this is where the social sciences can help bring about positive change. Individual network defenders and law-enforcement agents struggle every day to find attackers. Often, several individuals are working at the same time in pursuit of the same perpetrator, but they have no idea of each other's existence or of their common goal. And worst of all, they don't know that each of them holds a different piece of the puzzle that carries the answer. If they had an effective means of communication, whether through online collaboration or shared visualizations, and if they have the understanding that they do not have to—and should not—solve this problem alone, they would be able to work together more effectively. It is at that individual collaboration level that psychology and sociology can play a significant role.

So in addition to all of the effort that is currently being applied to getting *organizations* to collaborate more effectively (as described in the President's Cyberspace Policy Review), we must also work just as hard to improve the ability of *individuals* to collaborate effectively within and across organizational boundaries. Assuming that policies allow for information sharing, we need to have media in place for collaboration and shared situational awareness.

Usability to Enhance Security

There is a never-ending tug-of-war between security and usability. The more protections that are built into our systems, the harder they are to use. Apple famously lampooned Microsoft's attempts at improving the security of Windows Vista by asking users to "cancel or allow" a wide range of what users perceive as "normal" activities. And human nature being what it is, users do their utmost to find ways of circumventing these controls so they can get on with their work, including developing a knee-jerk response to "allow" everything that comes along.

A lot of attention is being paid to usability of computing systems in general—making applications or web-sites more "user friendly," for example—yet the concept is often ignored when security controls are designed in. Think of the most basic problem of remembering passwords. More stringent passwords, requiring nonsensical strings of numbers, letters and special characters, are at odds with people's innate ability to remember short, meaningful sequences of information. As a result, people simply write them down on post-it notes and stick them to their monitors for all

to see. There are some encouraging sparks of innovation in this area: for example, graphical passcodes[8] for user authentication. These new types of password, which use pictorial elements, take advantage of people's visual memory recall and are remembered better than meaningless strings of alphanumerics.[9] This sort of forward-thinking research needs to be applied across the entire security problem.

Need for Research on How People Value Information

The crux of information security is securing information that has been designated as valuable. Nevertheless, we have little understanding of what makes information valuable to people. Security practitioners tend to "guard the perimeter," treating everything within the boundaries as if it is of equal value. Yet all information assets behind a firewall are not equal. Some workstations or servers are more valuable than others—perhaps because of the role of its user, the content of its storage device, or the service it provides to the enterprise. People want to protect the most valuable information; yet there are no metrics or even basic insights into how the value of information is determined.[10]

If we knew how to *measure* the value of information, we would be able to apply security measures that follow the high-value information, even as it moves through a network. Just as the President's bodyguards follow him as he moves, so too should security be able to move along with important information. If U.S. network defenders can provide greater protection to the most valued assets, adversaries may be deterred by the extra time and resources required to break into well-protected cyber assets. Of course, this requires the defender to know which information systems contain high-value information—something that is difficult without methods to value information and the means to locate where the high-value information currently resides in a dynamic network configuration.

If we better understood how *people* placed value on information, we would be able to use that valuation to motivate individuals to comply with security practices and change the culture of security. We could also use that understanding of information value to support the calculation of the Return on Investment of security. The ability to recognize and quantify the value of information resident on a network will help security practitioners better secure and protect information and network assets, allow cyber defenders to prioritize their defensive actions by focusing on the most critical net-work assets, and allow business owners to immediately assess the impact of an attack on those assets.

Understanding the relative value of information underlies all of these decisions. But there is no current methodology used in the DOD for assigning an actual value to information. Current work[11,12] on cyber information valuation within DOD has advanced the theoretical discussion but remains only conceptual. Metrics are not *usable* unless they have been validated against real-world observations.

Research is needed to better understand how people place value on information, to identify the most promising metrics for valuing information, to apply those metrics to information observed in a real-world environment, and to determine whether or not the conceptual metrics are verifiable in real data.

The Private Sector's Role in the Cyber Security Research Agenda

Security practitioners in the private sector are on the front line of cyber defense. These individuals write the security policies, deploy the technologies, and attempt to compute ROI for security expenditures. They have direct influence on the security practices of individual U.S. workers and business owners whose inattention to security could have cascading effects on our country's computing infrastructure. Security practitioners deal with the *people* side of security, far more than any of today's educators or researchers. Yet the security practitioners have virtually no influence on the cyber security research agenda and only indirect influence on the curriculum of computer science programs.

---

[8] *http://www.passfaces.com*

[9] Johnson, K. & Werner, S. (2008) Graphical user authentication: A comparative evaluation of composite scene authentication vs. three competing graphical passcode systems. In *Proceedings of the 52nd Annual Meeting of the Human Factors and Ergonomics Society.* New York, NY.

[10] Stevens, J. (2005) *Information Asset Profiling.* Pittsburgh, PA, Carnegie Mellon University.

[11] Grimaila, M.R. and L.W. Fortson. (2007) *Towards an Information Asset-Based Defensive Cyber Damage Assessment Process,* Computational Intelligence in Security and Defense Applications.

[12] Hellesen, D. (2008) *An Analysis of Information Asset Valuation (IAV) Quantification Methodology for Application with Cyber Information Mission Impact Assessment (CIMIA),* Master's thesis, AFIT.

The government does not actively solicit input from the private sector in crafting its R&D or education agenda, nor does the government actively promote dissemination of the research results to media and forums usually consulted by private security practitioners. As a member, Board Director, and Advisor of the New York Metropolitan Chapter of the Information Systems Security Association (ISSA), I regularly meet with hundreds of chapter members who are security professionals in New York-based businesses. We have never been asked for input into a national research agenda. Our membership has been genuinely surprised when they've heard about the results of my own work sponsored by DHS, IARPA, the Air Force, and DARPA. Furthermore, these members of the private sector are *willing to participate in the technical transition of the R&D*—but they are rarely asked to do so.

Additionally, the ISACs and other organizations, such as the National Academy of Sciences, could be tapped as conduits for collaboration between the private sector and government in developing the cyber security research agenda.

Conclusion

Effective cyber security is often said to be about "people, process, and technology." Although "people" come first in this description, the emphasis in federally funded cyber security education and research has been on the development of technology within the academic environment of computer science and electrical engineering. This needs to change.

Broaden the Base of Those Receiving Cyber Security Education

The current approach to cyber security education falls far short of adequately preparing the universe of people who every day take actions that make our computing infrastructure more or less secure. We must offer information to—and influence the behavior of—software developers, business owners, soldiers maintaining network-centric systems, policy-makers, lawyers, students, and home-users. The source of this education must go beyond college computer science courses. The education and training of security awareness, good practices, and cyber ethics should start in our elementary schools and extend beyond the academic environment into the training programs offered by professional organizations.

Schools of law and law enforcement must not only teach cyber law and policy, but teach the foundations of the Internet and computer usage that underlie the laws and policies.

Social science experts in cultural influence should be consulted on how to raise our national awareness of cyber risks and change the security practices of average Americans.

Experts in learning should advise the retiring old guard security practitioners on how to effectively mentor new security professionals and expedite the transfer of their corporate knowledge.

Computer science curricula must include building security into the entire life cycle of software development.

We must increase the number of U.S. citizens who master the math and science needed to advance cyber security technologies, and who enroll in advanced degrees in information security.

Use Interdisciplinary Approaches to Make the Cyber Culture More Secure

Changing how people value security and behave with computer systems and networks should be a primary concern of our cyber education and research. It is clear that technological change will happen; it already does. But safe and ethical behavior is not keeping pace with the pervasiveness of computing for work, entertainment, and socializing. Interdisciplinary approaches, which combine computer science with the more people-centric disciplines of psychology, sociology and anthropology, can extend our understanding of how to create a more secure computing culture.

We need research on how people value information. Understanding how people place value on information will help security professionals to motivate compliance with security practices; it will inform the security architects on where to place the greatest defense; and it will form the foundation for security metrics.

Security must be more usable. Interdisciplinary approaches to usability can make it easier for practitioners to install and tune security technology, and for users to comply with security policies and practices.

Human factors psychologists with expertise in collaborative media should work with computer network defenders to develop effective means for timely information sharing needed to rapidly detect cyber attacks within and across organizations.

The disciplines of economics, business administration, and information systems must study the interdependencies of computing assets and business processes so

that accurate ROI for security investment can be computed, and data-driven plans for continuity of operations can be developed.

Foster Technology Transition of Cyber Security Research

The existing research agenda, framed by and for computer scientists, emphasizes publication of research results above technology transition. Little current research and education funding is directed to the operational implementation of the advanced technologies. The problems encountered in getting a technology to work in the real world—accreditation, affordability, usability—are not deemed worthy of peer-reviewed publications and are therefore dismissed by many professors, students, and funding agencies who measure their achievements through publication history.

There is a short supply of U.S. citizens with security-related advanced degrees who can transition technology into the DOD where security clearances are required. Non-academic research institutions who have U.S. citizens to transition technology, such as research contractors or government laboratories, do not have the streamlined Institutional Review Board processes required for technology evaluation studies involving people; hence the human element is all too often left out of the research.

To increase the likelihood of technology transition we must take several steps:

- Realistic, scalable test data must be provided to the researchers by the funding agencies.
- Funding agencies should include measures of technology transition in their evaluation of grants and research contracts.
- Funds should be available for crossing the chasm from prototype to operational deployment. This includes funding for accreditation and usability evaluations.
- The government should foster collaboration between university researchers and nonacademic research organizations. The universities can use their Institutional Review Boards to guide corporations anal government laboratories in testing new technologies with human subjects. Research companies with personnel who have security clearances can assist universities with technology transition into DOD sites that are not ordinarily accessible to university students and professors.

Increased the Private Sector's Voice in Cyber Security Education and Research

The private sector, which is a conduit both for attacks on our critical information infrastructure as well as the prevention of those attacks, has no significant influence on the federal R&D agenda in cyber security. Security practitioners in the private sector, where they can influence U.S. workers and businesses, are neither consulted on the national agenda nor given easy access to the results of federally sponsored R&D. This can be addressed in several ways:

- The sponsors of cyber security R&D should conduct outreach activities to professional societies of security practitioners including ISSA, ISACA (*Information Systems Audit and Control Association*), and (ISC)2 (*International Information Systems Security Certification Consortium*).
- Researchers must be encouraged by the sponsors of their research to publish the results of their work in trade magazines and on-line forums where private security professionals communicate.
- The government should incentivize the private sector to bring interns from academia into their IT infrastructure to gain on-the-job experience prior to their graduation.
- ISACs should be used as a medium for connecting private sector needs with federally funded research.

In sum, there are many substantive ways in which the social sciences can assist us in improving cyber security. My thanks to the Committee for allowing me an opportunity to share my viewpoints.

Acknowledgements

I would like to acknowledge the contributions of Laurin Buchanan and Frank Zinghini of AVI, and Geoff Mumford of the American Psychological Association, to the preparation of this testimony.

BIOGRAPHY FOR ANITA D'AMICO

Dr. D'Amico is the Director of Secure Decisions, a division of Applied Visions, Inc. She is a human factors psychologist and an information security specialist, with interests in improving situational awareness of information security analysts through visualization and cognitive analysis. Her most recent work has been in the area of combining geographic information with network security and network management information to improve security and preserve continuity of operations.

Dr. D'Amico joined Applied Visions in 2000 to help create and grow the Secure Decisions division, building upon information visualization technology developed by Applied Visions under an Air Force research contract. The Secure Decisions division of Applied Visions is now recognized as a leading provider of information visualization research and technology development to the Department of Defense, the Intelligence Community, and the Department of Homeland Security.

Prior to joining Applied Visions, Dr. D'Amico ran the Information Warfare Group for Northrop Grumman, where she was responsible for developing that new business area. In the years before that she had applied her human factors and psychology training to a variety of domains, all centered about the interaction between humans and machines, including such disparate domains as aircraft design and ship handling.

Dr. D'Amico has published widely on the topic of cyber security, particularly from the perspective of human factors and the impact of situational awareness on the effectiveness of cyber security practitioners. She is a frequent keynote speaker on the topic at industry conferences, and she chaired the 2003 Forum on Information Warfare, presented by the Management Information Systems Training Institute, Washington, DC. Recently, she conceived and conducted a joint industry/government workshop on understanding and determining the impact of cyber security breaches on organizational mission.

Dr. D'Amico received a B.A. from the University of Pennsylvania, and an M.S. and Ph.D. in psychology from Adelphi University. She served five years as a member of the Board of Directors of the New York Metro chapter of the Information Systems Security Association (NYMISSA).

Chairman LIPINSKI. Thank you, Dr. D'Amico.

Dr. Schneider.

STATEMENT OF DR. FRED B. SCHNEIDER, SAMUEL B. ECKERT PROFESSOR OF COMPUTER SCIENCE, DEPARTMENT OF COMPUTER SCIENCE, CORNELL UNIVERSITY

Dr. SCHNEIDER. Thank you for inviting me here to testify today. In the few minutes I have, I want to summarize the key points in my written testimony.

I start with the observation that computing systems we deploy today are not as trustworthy as they could be, and we don't know how to make them as trustworthy as they need to be. As the United States increases our dependence on these systems, they become ever more attractive to attackers. Our defenses don't keep up so we operate in a reactive mode and we improve defenses only after they have been penetrated. We thus prepare to fight the last battle rather than the next one. We need to move beyond this reactive stance to a proactive one. In short, we must build systems whose trustworthiness derives from first principles. This proactive approach requires having a science base for cyber security. We don't have one and we need to develop one. Doing that will require making significant investments in research and the investments will have to be made on a continuing basis. Cyber security will never be a solved problem. We are not going to find a magic bullet solution. We have accepted this reality for medical research and for defense. The same reality applies to cyber security.

The analogy with public health and medical research highlights two disconnects between cyber security research today and what is

really needed. The first was the lack of science base I just discussed. The second disconnect concerns the policy part of the picture. Technology solutions that ignore policy questions risk irrelevance as do policy initiatives that ignore the limits and capabilities of technology. This means that we should also be supporting research in policy and research that aims to bridge the gap between technology and policy.

Let me make two further observations about cyber security research. First, when the work is classified, it cannot engage many of the country's top researchers. It necessarily receives less scrutiny by a diverse community of experts and it will be slow to impact the civilian infrastructure on which we increasingly depend. Second, cyber security research once was funded by a diverse ecology of agencies. This was valuable because different agencies have different needs, goals, cultures, styles and criteria for reviewing proposals; but that diversity has been eroding. Getting that diversity restored should be a priority and it would undoubtedly bring better value per research dollar spent.

I earlier made the observation that today's systems are not as trustworthy as they could be. There are many reasons for this, and university education certainly has an important role to play in the solution here. With significant increases in research funding, more faculty will be working on system trustworthiness so more faculty will be available to teach these subjects, and that is crucial; but understand that like any new discipline, this field is in flux. There is not yet a widespread agreement on the core, so we would be ill advised to be legislating what gets taught. We would also be ill advised to be legislating that everyone be taught. Only a fraction of the students that our computer science department teaches end up in system-building jobs. Also, many who are building our nation's critical infrastructures were not computer science majors. What I think we need is a new graduate professional degree program. Lawyers, doctors, teachers and most other professionals in our society are a good model. We need a post-Bachelor's degree for systems trustworthiness professionals. On the university side, this would mean developing courses, texts and other teaching materials, and outside the university it would mean creating a force field so people are compelled to invest the time and money to pursue this new degree.

In closing, let me say how encouraged I am by all the recent interest and activity at the federal level regarding cyber security; but let me caution, long-term activities that will require long-term investments are the only way to get a long-term solution to this problem. We need to be making long-term investments in research, and we need to be making long-term investments in education.

Thank you. I look forward to your questions.

[The prepared statement of Dr. Schneider follows:]

PREPARED STATEMENT OF FRED B. SCHNEIDER

Good morning Mr. Chairman and Members of the Committee. I appreciate this opportunity to comment on cyber security research and education. I am Fred B. Schneider, a Computer Science professor at Cornell University and Chief Scientist of the NSF-funded TRUST[1] Science and Technology Center, a collaboration involv-

[1] Team for Research in Ubiquitous Secure Technology.

ing researchers at U.C.–Berkeley, Carnegie-Mellon University, Cornell University, Stanford University, and Vanderbilt University.

I have been a Computer Science faculty member since 1978, actively involved in research, education, and in various advisory capacities for both the private and public sectors. Besides teaching and doing research at Cornell, I today serve as member of the Dept. of Commerce Information Security and Privacy Advisory Board (ISPAB), as a member of the Computing Research Association's board of directors, and as a council member of the Computing Community Consortium. I also co-chair Microsoft's TCAAB external advisory board on trustworthy computing.

Our nation's increasing dependence on computing systems that are not trustworthy puts individuals, commercial enterprises, the public sector, and our military at risk. If anything, this dependence will accelerate with new initiatives such as the "smart grid" and electronic health care records. Increased data, increased networking, and increased processing all mean increased exposure. These systems need to work as we expect—to operate despite failures and despite attacks. They need to be trustworthy.

The growth in attacks we are seeing today should not be surprising. The more we depend on a system, the more attractive a target it becomes to somebody intent on causing disruption; and the more value that is controlled by a system, the more attractive a target it becomes to somebody seeking illicit gain. But more disturbing than the growth in attacks is that our defenses can't keep up. The core of this problem is the asymmetric nature of cyber security:

- Defenders are reactive; attackers are proactive. Defenders must defend all places at all times, against all possible attacks (including those not known about by the defender); attackers need only find one vulnerability, and they have the luxury of inventing and testing new attacks in private as well as selecting the place and time of attack at their convenience.
- New defenses are expensive to develop and deploy; new attacks are cheap. Defenders have significant investments in their approaches and business models, while attackers have minimal sunk costs and thus can be quite agile.
- The effectiveness of defenses cannot be measured; attacks can. Since we cannot currently quantify how a given security technology or approach reduces risk from attack, there are few strong competitive pressures to develop defenses. So vendors frequently compete on the basis of ancillary factors (e.g., speed, integration, brand development, etc.). Attackers see their return-on-investment and have strong incentives to improve their offerings.

The result has been a cyber security mentality and industry built around defending against known attacks. Our defenses improve *only* after they have been successfully penetrated. And this is a recipe to ensure some attackers succeed—not a recipe for achieving system trustworthiness. We must move beyond reacting to yesterday's attacks (or what attacks we predict for tomorrow) and instead start building systems whose trustworthiness derives from first principles.

Yet today we lack the understanding to adopt that proactive approach; we lack a "science base" for trustworthiness. We understand that the landscape includes attacks, defense mechanisms, and security properties. But we are only now starting to characterize the lay of the land in terms of how these features relate—answers to questions like: What security properties can be preserved by a given defense mechanism? What attacks are resisted by a given mechanism? How can we overcome the inevitable imperfections in anything we might build, yet still resist attacks by, for example, forcing attackers to work too hard for their expected pay-off. Having a science base should not be equated with implementing absolute security or even concluding that security requires perfection in design and implementation. Rather, a science base should provide—independent of specific systems—a principled account for techniques that work, including assumptions they require and ways one set of assumptions can be transformed or discharged by another. It would articulate and organize a set of abstractions, principles, and trade-offs for building trustworthy systems, given the realities of the threats, of our security needs, and of a broad new collection of defense mechanisms and doctrines. And it would provide scientific laws, like the laws of physics and mathematics, for trustworthiness.

An analogy with medicine can be instructive here. Some maladies are best dealt with in a reactive manner. We know what to do when somebody breaks a finger, and each year we create a new influenza vaccine. But only after significant investments in basic medical sciences are we starting to understand the mechanisms by which cancers grow, and developing a cure seems to require that kind of deep understanding. Moreover, nobody believes that disease will some day be a "solved

problem." We make enormous strides in medical research yet new threats emerge and old defenses (e.g., antibiotics) are seen to lose their effectiveness.

Like medicine and disease, system trustworthiness is never going to be a "solved problem". There will be no "magic bullet" trustworthiness solution, just as there is not going to be a miracle cure for all that ails you. We must plan to make continuing investments, because the problem will continue evolving:

- The sophistication of attackers is ever growing, so if a system has vulnerabilities then they will find it. Any assumption made when building a system does, in fact, constitute a vulnerability, so every system will have vulnerabilities of one sort of another. And with enough study, attackers will find these vulnerabilities and find ways to exploit them.
- The technology base used by our systems is rapidly changing. Systems are replaced on a three- to five-year time span, not because computers or software wear out but because newer software and hardware offers improved functionality or better performance (which is then leveraged into new functionality). New systems will work differently, will involve different assumptions, and therefore will require new defenses.
- The settings in which our computing systems are deployed and the functionality they provide is not static. With new settings come new opportunities for attack and disruption, whether it is creating a blackout by attacking the "smart grid" or stalking somebody by planting a virus on a GPS-equipped cell phone.

We can expect to transcend the constant evolution only through the understanding that a science base provides. A science base is also our only hope for developing a suite of sound quantitative trustworthiness measures, which in turn could enable intelligent risk-management decisions, comparisons of different defenses, and incentivize investments in new solutions.

A science base for trustworthiness would not distinguish between classified and unclassified systems, nor would it distinguish between government and private-sector systems. The threats and trade-offs might be different; the principles are going to be the same. But even an understanding of how to build trustworthy systems for the private sector would by itself be useful in military and government settings, simply because so-called COTS (commercial off the shelf) technologies that are developed by the private sector for the private sector are widely used within the government too.

Many equate cyber security research with investigations solely into technical matters. This oversimplifies. Achieving system trustworthiness is not purely a technology problem. It also involves policy (economic and regulatory). Technological solutions that ignore policy questions risk irrelevance, as do policy initiatives that ignore the limits and capabilities of technology. So besides investing in developing a science base for trustworthiness, we must also invest in research that bridges the technical and the non-technical. We need to understand when we might get more traction for trustworthiness from a policy solution than from a technology one. For example, identifiers—your mother's maiden name, your credit card number, your bank account number, and your social security number—are not a good basis for authentication because they will be known to many. So regulation that prohibits the use of identifiers as authenticators might more effectively defend against identity theft than new technology could. As another example, there is talk about making the Internet more secure by adding the means to trace packets back to their senders. But the Internet is as much a social construct as a technological one, and we need to understand what effects proposed technological changes could have; forgoing social values like anonymity and privacy (in some sense, analogous to freedom of speech and assembly) in order to make the Internet more-trustworthy might significantly limit the Internet's utility to some, and thus not be seen as progress.

Investments in cyber security research are best accompanied by investments in cyber security education, because this provides an efficient path for the research to reach industry where it can be applied. In particular, research undertaken in academia not only engages some of our nation's best and brightest researchers but because these researchers are also teachers, new generations of students can be exposed to the latest thinking from the people who understand it best. And when these students graduate and move into the workplace, they will bring this knowledge and understanding with them. Moreover, faculty in this dual role of researchers and teachers have incentives to write textbooks and prepare other teaching materials that allow dissemination of their work to a very wide audience, including teachers elsewhere.

Question: *Does the current range of federally supported research adequately address existing cyber security threats 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?*

Federal expenditures for unclassified cyber security research do not match the severity of the threat. IT security expenditures are estimated to reach $79 billion annually by 2010.[2] According to the NITRD Networking and Information Technology Research and Development Program,[3] $342.5M is being requested for FY 2010 "Cyber Security & Information Assurance." This means federal budget requests for unclassified research in system trustworthiness total roughly .4 percent of the expenditures that might be leveraged by the research. Moreover, anecdotal information about specific funding programs at various key federal agencies suggests that only a portion of the $342.5M is spent on academic research in cyber security. It then comes as no surprise to find the recent National Research Council CSTB report *Toward a Safer and More Secure Cyberspace*[4] stating that funding levels for cyber security research are low, preventing researchers from pursuing their promising research ideas. And this echoes the findings in the President's Information Technology Advisory Committee's independent report *Cyber Security: A Crisis of Prioritization*[5] which stated that (i) cyber security solutions would emerge only from a vigorous and well funded program of research and (ii) that levels of funding were dangerously low to solve problems or to sustain a community of researchers.

The NRC CSTB report also states that, excepting the National Science Foundation (NSF), federal funding agencies predominantly target short-term problems rather than addressing the harder, longer-term challenges that constitute our only hope to win this war. A culture that targets easily quantifiable progress is particularly dangerous, because it discourages funding research efforts that, being more forward-looking, could provide the real pay-offs.

The PITAC report also noted damage being caused by the lack of continuity in cyber security funding and by the inadequate oversight and coordination exerted by Federal Government over its cyber security research programs. For example, a lack of funding continuity stymies the development of a research community, because younger faculty and graduate students are disinclined to enter fields where future funding is uncertain. This, in turn, leads to a national shortage in cyber security expertise.

PITAC argued, in vain, for a significantly increased investment in "fundamental research in civilian cyber security," noting that civilian systems comprise the lion's share of our nation's critical IT infrastructure, and that the government and military rely in large measure on civilian hardware and software components and systems. Moreover, expenditures by the private sector for long-term cyber security research have historically been quite small, probably because return on such investments is expected to be low. If the Federal Government doesn't make these investments then nobody else will, and we all miss the opportunity for the revolutionary advances that are unlikely to result from the current regime of funding evolutionary steps. By the same token, the existence of a healthy IT-security industry suggests that the private sector does make investments in short-term research; so there is a less-compelling reason for federal investments here.

There is a disconnect between research being funded and what is needed. Federal research funding has been too focused on a few established technical battlefronts (e.g., firewalls, anti-virus, intrusion detection, buffer overflows, etc.). In some cases, this focus reflects views held by researchers; in other cases, the focus comes from program management in the funding agencies. Whichever it is, this mindset is a decade or more out of step with the reality of our current adversaries. We need to re-imagine the scope of the cyber security problem itself and refocus our attention the same way our adversaries have refocused. We cannot afford simply to develop technologies that plug holes faster; we need to think of security research more holis-

---

[2] *Information Security Products & Services—Global Strategic Business Report,* Global Industry Analysts, Inc., July 2007.

[3] *The Networking and Information Technology Research and Development Program.* Report by the Subcommittee on Networking and Information Technology Research and Development, May 2009. Page 21. *http://www.nitrd.gov/Pubs/2010supplement/FY10Supp-FINAL-Preprint-Web.pdf*

[4] *Toward a Safer and More Secure Cyberspace.* S. Goodman and H. Lin (eds.), National Academies Press, Washington, DC, 2007. Appendix B.6. *http://books.nap.edu/catalog.php?record_id=11925*

[5] *Cyber Security: A Crisis of Prioritization.* President's Information Technology Advisory Committee, Feb. 2005. *http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf*

tically, determining how most efficiently to block, disrupt, or dis-incentivize opponents.

- We must establish a goal of developing a science base for trustworthiness, as discussed in detail above. Such a science base is crucial for understanding how to build systems that are trustworthy.
- We must investigate mechanisms—both operational and forensic—for better attributing cyber-attacks to the actors behind them, because this is essential for applying virtually all other instruments of policy, from law enforcement to diplomacy. This approach might well be a last resort, invoked only after defenses to prevent attacks have failed. So it needs to be an option, despite being technically quite challenging as well as raising non-technical questions ranging from privacy all the way to international law.
- We must consider not merely hypothetical opponents, but the real attackers we face today and those we expect to encounter tomorrow. The military does not train against a hypothetical adversary with hypothetical resources, strategies and interests, nor should cyber security researchers investigate defenses absent that information.
- We must prioritize developing better quantitative measures around cyber security risk, efficiency, and value. The government and the private sector cannot invest arbitrary amounts in securing our systems without better understanding the return on this investment.
- We must invest in research that bridges policy (regulation and economics) with technology. To do research in technology without knowledge of policy or vice versa risks irrelevance.
- We must better understand the human element in our systems. Too often system security is synonymous with inconveniencing users. And users are inclined to circumvent security controls they find inconvenient, defeating a system's defenses even before it is attacked.
- We must continue to invest in research concerned with building software systems: operating systems, networks, programming languages, formal methods, database systems, etc. Ultimately, the things that undermine a system's trustworthiness will be traced to errors in design, implementation, requirements, or assumptions—subjects that are studied by software researchers. And we must continue making research investments in the relevant theoretical areas, such as logics and cryptography.

While there is certainly both a role and need for undertaking classified research in trustworthy systems, there are significant limitations that come with the secrecy. Classified research does not engage many of the most capable cyber security researchers, is necessarily less likely to receive broad scrutiny by a diverse community of experts, and does not contribute to educating the next generation of cyber security researchers and practitioners. Classified research programs are also slow to impact the civilian cyber-infrastructure and its equipment, on which so much of our nation's critical infrastructure depends.

Having an Ecology of Federal Agencies is Valuable. There once was a diverse ecology of funding sources for the various styles and topics that trustworthiness research spans, but that ecosystem has been eroding as funding agencies have redefined their priorities. Some of these decisions are difficult to defend, given the central role that system trustworthiness plays in the missions these agencies are suppose to support.

Funding from a single agency (NSF) now dominates unclassified federal cyber security research. In the past, DARPA had been a significant source of funding for university researchers doing work in systems and security, but for the last eight years DARPA has not been making those investments. DHS has funded work in cyber security, but at significantly lower levels and focusing on problems with a short-term horizon. DOD, through AFOSR, ARO, and ONR, does fund some fundamental research in security, but the number of projects supported is relatively small and some of the funding is for special one-time initiatives (i.e., the MURI program). IARPA inherited from its predecessor organizations a small but strong trustworthiness research program. That, however, is being terminated, and new programs to take its place have been slow to get started. Also, the funding philosophy at IARPA appears to be oriented more toward production of quantifiable results than toward open-ended curiosity-driven explorations.

This ecology of different government agencies with their different needs, goals, and cultures, could yield a robust and diverse research climate. However, many of the potential benefits have not materialized, both because the interagency coordina-

tion has been voluntary and because tight budgets led some of the participants to reduce their cyber security research investments and/or to focus those expenditures on short-term work, which they saw as better suited for their missions.

Today, NSF is the only natural home for fundamental research in civilian cyber security. They not only fund single-investigators doing more-theoretical work, but they also fund larger-scale multi-investigator efforts that involve prototyping non-trivial systems. NSF's Trustworthy Computing (formerly Cyber Trust) program, the likely agent for funding investigations that will have high payoff, is woefully under-resourced. In the past, what had been DARPA's style complemented NSF"s style by supporting larger groups (three to five investigators) to work for relatively longer periods (five to ten years) in order to take a game-changing idea to a demonstrable embodiment. The NSF and former DARPA styles are complementary, and both ought to be supported. Another point of contrast between the different styles concerns the manner they review and select proposals for funding. External peer-review by the research community leads to funding work having a different character from internal review (where programmatic goals play a role in project selection).

There is a tension between maintaining a diverse ecology of federal agencies to fund trustworthiness research and allowing each individual funding agency the autonomy to alter its priorities. So we must be mindful: seemingly local decisions within an agency actually can have a broader impact by changing the federal portfolio of trustworthiness research (as well as changing the total amount of federal expenditures for trustworthiness research). This tension would be resolved if a coordinating body were to monitor such decisions and offset their impact on the federal portfolio by allocating additional resources and recreating the now-absent styles at agencies electing to continue funding trustworthiness research.

Finally, it is worth noting that new initiatives in energy (e.g., a "smart grid"), transportation, and electronic medical records will almost certainly require solving new trustworthiness research questions. A failure to engage the community early in such initiatives is a mistake. This kind of trustworthiness research is not done well in a vacuum from applications; there is no substitute for direct experience with the application area. Thus, part of these new initiatives should be to involve the trustworthiness research community, so they can help ensure that the internetworked systems required will be ones we can depend on.

Question: *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?*

The University Landscape. Cyber security professionals are today not being adequately trained to meet the needs of either the private sector or the public sector.

- **Part of the problem is resources.** University Computer Science (CS) departments lack the faculty to offer the relevant courses. Few faculty members have the necessary expertise to offer courses in this area. And even if a CS department has managed to hire a few cyber security specialists, they will likely also be involved in teaching the large complement of other classes that need to be covered by a department giving undergraduate and graduate CS degrees.
- **Part of the problem is content.** The field is relatively young and fast moving. There is not yet widespread agreement about what technical content must be covered, which makes this an exciting time to be teaching cyber security at the university level. But it also means that textbooks and other teaching materials have short lives unless they are frequently revised, which is a disincentive to some authors. So there are fewer good textbooks than would be found in a more mature subject. Yet, creating agreement on content by legislating a curriculum would be a serious mistake at this point, because it would retard the dissemination of new ideas to students and it would discourage faculty from writing texts that reflect improvements in our understanding of the field.

A Cyber Security Professional Degree. I believe that a well trained cyber security professional needs to have exposure to a broad variety of topics. One would expect to see courses that cover technical topics, such as computer security principles, distributed systems and networking, systems reliability, software engineering, cryptography, and user interfaces and human factors. But I also strongly advocate exposure to non-technical topics, including cyber-law (intellectual property law, communications law, privacy law), ethics, economics of computing and networking, business strategy, and human relations (i.e., management of people). This broad

education would enable a cyber security professional to use all conceivable technical and policy tools for achieving trustworthiness. It would also ensure that solutions could be evaluated in a broader societal context, so that risk-management and trade-offs between different social values (such as privacy versus accountability) can be contemplated.

There is likely more than one year's worth of content past today's CS BS degree, but there is probably less than three years of course material. This would argue for creating some sort of graduate, professional degree program. It would be designed so that its students would learn both the technical and the non-technical topics needed to define and develop trustworthy computing systems, manage them, and oversee their deployment, use, and evolution.

Undergraduate Education. Computer Science departments today educate students to pursue a rather diverse set of careers. And, in particular, not all undergraduate Computer Science majors are headed for system-building careers. Thus, it would be inappropriate to impose a cyber security requirement on all graduates from a Computer Science department. The more sensible model would be for universities to offer a *programme of study* for system trustworthiness, analogous to pre-law or pre-med. Such a program is typically not associated with a single university department but rather offered in conjunction with a various majors; it prescribes a set of courses for the electives available in that department's major. The courses would cover the subjects outlined above in connection with the cyber security professional degree. And it should be open to students in the various relevant majors.

Finally, it certainly seems reasonable that students destined to build systems—no matter what their major—should have exposure to the basic ideas needed for making those systems trustworthy. This means that they need exposure to basic cyber security, software engineering, and various systems topics (operating systems, networking, etc.). Such students will be found enrolled in various majors. So while the CS department is the obvious place to offer these courses, the courses will not be populated only by CS majors. And this has implications concerning what pre-requisites can be assumed.

BIOGRAPHY FOR FRED B. SCHNEIDER

Fred B. Schneider is Samuel B. Eckert Professor of Computer Science at Cornell University. He joined the Cornell faculty in Fall 1978, having completing a Ph.D. at Stony Brook University, preceded by a B.S. in Engineering from Cornell in 1975. Schneider currently also serves as the Chief Scientist for the NSF-funded TRUST Science and Technology Center, which brings together researchers at U.C.–Berkeley, Carnegie-Mellon University, Cornell University, Stanford University, and Vanderbilt University.

Schneider's research has focused on various aspects of trustworthy systems—systems that perform as expected, despite failures and attacks. His early work concerned formal methods to aid in the design and implementation of concurrent and distributed systems that satisfy their specifications; he is author of two texts on that subject: *On Concurrent Programming* and *A Logical Approach to Discrete Mathematics* (co-authored with D. Gries). He has also known for his research in theory and algorithms for building fault-tolerant distributed systems. For example, his paper on the "state machine approach" for managing replication brought an SOSP "Hall of Fame" award for seminal research. More recently, his interests have turned to system security. His work characterizing what policies can be enforced with various classes of defenses is widely cited, and it is seen as advancing the nascent science base for security. He is also engaged in research concerning legal and economic measures for improving system trustworthiness.

Schneider was elected Fellow of the American Association for the Advancement of Science in 1992, the Association of Computing Machinery in 1995, and the Institute of Electrical and Electronics Engineers in 2008. He was named Professor-at-Large at the University of Tromso (Norway) in 1996, and was awarded a Doctor of Science *honoris causa* by the University of NewCastle-upon-Tyne in 2003 for his work in computer dependability and security.

Schneider has served since Sept. 2006 as a member of the Information Security and Privacy Advisory Board (ISPAB), which advises NIST, the Secretary of Commerce, and the Director of OMB on information security and privacy issues pertaining to Federal Government Information Systems. He chaired the National Academies CSTB study on information systems trustworthiness that produced the 1999 volume Trust in Cyberspace. He also served as a member of CSTB from 2002–2008 and from 2004–2007 on the CSTB study committee for improving cyber security research. Schneider was a member of the NSF CISE advisory committee 2002–2006.

And in Fall 2001, he chaired the United Kingdom's pentennial external review of research funding for academic Computer Science.

In 2007, Schneider was elected to the Board of Directors of the Computing Research Association (CRA) and appointed to the steering committee of CRA's Computing Community Consortium. CRA is an association of more than 200 North American academic departments of computer science, computer engineering, and related fields; part of it's mission is to strength research and advanced education in the computing fields and to improve public and policy-maker understanding of the importance of computing and computing research in our society.

Schneider is a frequent consultant to industry, believing this to be an efficient means of implementing technology transfer as well as learning about the real problems. He is Co-Chair of Microsoft's Trustworthy Computing Academic Advisory Board, which comprises outside technology and policy experts who meet periodically to advise Microsoft about products and strategy. He also provides technical expertise in computer security as well as more broadly to a variety of firms, including: BAE Systems, Fortify Software, Lockheed Martin, and Microsoft.

Chairman LIPINSKI. Thank you, Dr. Schneider.

I now recognize Mr. Brown.

STATEMENT OF MR. TIMOTHY G. BROWN, VICE PRESIDENT AND CHIEF ARCHITECT, CA SECURITY MANAGEMENT

Mr. BROWN. Good morning, Chairman Lipinski, Ranking Member Ehlers and the Members of the Subcommittee. My name is Timothy Brown. I am the Vice President and Chief Architect for Security Management for CA Incorporated. I will testify today on behalf of CA, and I will draw in several instances upon the positions of the Business Software Alliance, of which CA is an active member. I appreciate the opportunity to testify today on cyber security and R&D. I commend you for your focus on these issues which are of great importance to CA and the cyber security of the Nation.

The threats to our security are real and ever changing. The days of the hobbyist hacker are long past. Today most threats are posed by organizations for profit, groups which run very much like businesses except their business plan is to steal data, identities, credit card numbers and other valuable information and convert them into profit. My job at CA is to help stop these bad actors. We develop tools that individuals and businesses can use to protect themselves, but the threats are ever changing. For example, we have an immense and recent growth in social networking sites like Twitter and Facebook. This is a good development, but the cyber criminals look at these developments as simply new business models.

So, what can we do about all this? We believe the solution requires a multi-prolonged and smart approach consisting of four elements. Industry and government need to work together, set comprehensive goals that meet the full range of threats and develop rapid and effective responses. As a country, we need to invest more in basic research. The science must advance for us to develop the tools we need to address the threat and we need to make sure that those advances in the laboratory are quickly turned into the products people and companies need to protect themselves and maintain their security. We need more and better educated security specialists. We have made some advances in this area but our universities must be encouraged to devote more resources to supplying the security professionals of tomorrow.

Finally, we must ensure the public is fully aware of the threats they face. Today, too many Internet users fail to take the needed steps to ensure their data and valuable information is safe and se-

cure. One of these elements stands out. We believe the indispensable element of addressing the security threats is ensuring our country continues to invest in basic research into the ever-changing information-sharing environment. In my written testimony, I set these points out in great detail. I would now like to highlight a few of the technology changes that will create new opportunities for cyber criminals.

First, increased bandwidth and connectivity to laptops and smartphones is very important to our economic recovery and key to our long-term growth, but this trend also poses new challenges to security by pushing our existing security technology to its limits. Second, demand for data storage and computing power are ever increasing. Over the coming years we expect these demands to increase sharply. More data means more cyber criminals have more opportunity to do harm. Third, as I have mentioned already, the emergence of social networking has happened very fast and is transforming the way the Internet is used both at home and work through increased collaboration and information sharing, but the security systems used by social networks need to get much better very quickly. Fourth, today businesses collaborate and share data. They no longer operate independently, and this is good. For example, hospitals collaborate with other hospitals, universities, health care providers, but more collaborations create more vulnerabilities. Finally, the source of risk is also changing. Too often today, the threats come from within an organization rather than from malicious outsiders trying to infiltrate systems. To date we have not given enough attention to these insider threats.

To address these problems, we recommend the following ways federal support for advanced research can help: developing test tools and products that can identify vulnerabilities, logical inconsistencies and inappropriate back doors; ways to ensure security measures can keep pace with data being used by hundreds, sometimes thousands of people simultaneously; new identity management technology and business models that are acceptable to consumers and industry, models enabling people to collaborate and interact securely; research into insider threat detection and advanced data leakage protection. But this is not enough. Colleges and universities have made great progress and security courses are now mandatory in many programs. However, the security knowledge tends to focus more on secure coding practices and less on implementation and design of secure systems. We need simply more security professionals well trained in areas such as identity and access management, threat detection and response, and cryptographic systems.

Finally, we believe we need to significantly increase our national effort to raise public awareness about cyber security. This would decrease the likelihood that consumers will become victimized as well as decrease the likelihood that the computers would be hijacked to serve as launching pads for larger attacks. We simply need to develop a national cyber security public awareness and education strategy.

I would be happy to answer any questions you may have for me. Thank you.

[The prepared statement of Mr. Brown follows:]

PREPARED STATEMENT OF TIMOTHY G. BROWN

Good morning Chairman Lipinski, Ranking Member Ehlers, and Members of the Subcommittee. My name is Timothy Brown. I am the Vice President and Chief Architect for Security Management for CA, Inc. I will testify today on behalf of CA. However, in several instances, I will also draw upon the cyber security policy positions of the Business Software Alliance (BSA), an association representing the world's commercial software industry and its hardware partners. CA is a member of BSA and we actively participated in the development of those positions.[1]

CA (*www.ca.com*) is one of the world's largest information technology management software providers, providing software and expertise support to more than 99 percent of Fortune 1000® companies, as well as United States Federal, State and local government entities, educational institutions and thousands of other companies and governmental organizations worldwide. Founded in 1976, CA is a global company with headquarters in the United States, 150 offices in more than 45 countries, and more than 5,300 developers worldwide. To strengthen relationships among research communities and our company, we established CA Labs in 2005. CA Labs works closely with universities, professional associations and government on various projects that relate to CA products, technologies and methodologies. The results of these projects include research publications, best practices, and new directions for products. We also work with many universities to enable and promote innovation—including funding university research projects in specific areas, working with faculty to enhance curriculum, and providing opportunities to interact with CA research and development experts.

I appreciate the opportunity to testify today on cyber security research and development (R&D), cyber security in higher education, and public education and awareness of cyber security. These three issues, which you raise in the questions you have asked that I answer, are of great importance to CA and to the cyber security of our nation, and I commend you, Mr. Chairman, and Ranking Member Ehlers, for focusing on them. They correspond to three key aspects of cyber security: R&D is central to our capacity to provide innovative and secure information technology products and services; university-level education directly impacts our workforce's ability to both develop and operate secure information technology products and services; and public awareness contributes to a sound foundation of technology and security savvy users.

INDUSTRY AND THE FEDERAL CYBER SECURITY RESEARCH AGENDA

I would like to start by addressing the issue of the role of the private sector in setting the federal cyber security research agenda. Specifically, you asked the following question:

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?

As a prelude, let me first say that the recently released Cyberspace Policy Review, announced by President Obama on May 29, reflects cyber security concerns understood by virtually all information security professionals. The state of cyber security today clearly shows that we need to deliver game-changing security innovations and practices. Cyber criminals, State and non-State actors, and other cyber adversaries move rapidly and adeptly to exploit weaknesses and vulnerabilities in systems, networks, applications and practices. They are successful at taking control of machines and stealing data. Their motivation may be monetary gain or broader, more sinister goals, but they all have the luxury of picking and choosing both targets and methods to take advantage of the weakest links available. They are increasingly sophisticated and technically adept. So today's reality is that we are in a very tactical arms race with our adversaries.

---

[1] The Business Software Alliance (*www.bsa.org*) is the foremost organization dedicated to promoting a safe and legal digital world. BSA is the voice of the world's commercial software industry and its hardware partners before governments and in the international marketplace. Its members represent one of the fastest growing industries in the world. BSA programs foster technology innovation through education and policy initiatives that promote copyright protection, cyber security, trade and e-commerce. BSA members include Adobe, Apple, Autodesk, Bentley Systems, CA, Cisco Systems, CNC Software/Mastercam, Corel, CyberLink, Dassault Systèmes SolidWorks Corporation, Dell, Embarcadero, HP, IBM, Intel, Intuit, McAfee, Microsoft, Minitab, Quark, Quest Software, Rosetta Stone, SAP, Siemens, Sybase, Symantec, and The MathWorks.

The software industry has raised the bar considerably in the past few years. We have implemented mature, responsible vulnerability disclosure practices, internal secure code training, penetration testing, and code inspection tools. Large software vendors now have security as one of the major architectural components of any software they build and have made important changes to their development processes based on the demand of their corporate customers. The industry has also worked to simplify security and make it more user-friendly.

However, we need to supplement these tactical successes with strategic ones. We face increasing cyber security risks emerging from factors such as the extension of the enterprise externally to partners and customers, the rapid pace of technology adoption, the integration of physical devices into a networked environment, and increasingly sophisticated threats. Industry's research efforts are typically directed to product feature development and relatively short-term objectives that have a high probability of success in the marketplace. Game changing, strategic research is a difficult investment because of financial risk and unclear return on investment. Because of this, federal research programs can and should look to longer-term research requirements that prepare us not for the past or present, but for the future, a research agenda that will focus on strategic, systemic and structural cyber security issues not addressable by short-term, tactical solutions.

The federal research agenda is laid down in the Federal Plan for Cyber Security and Information Assurance Research and Development (hereafter "the CSIA plan"). I will now address the shortcomings of this plan and of the process by which it was developed. I will also propose solutions to make this agenda more inclusive of the needs of industry. In doing so, I will draw upon the positions of the BSA.

First, while it identifies many worthy cyber security R&D priorities, **the CSIA plan does not propose national-level objectives.** Rather, it is an aggregation of the cyber security R&D objectives of the federal agencies that fund or conduct cyber security R&D. While it is appropriate for these agencies, in support of their individual missions, to have specific cyber security R&D objectives, their aggregation does not produce a cohesive picture of the Nation's overall R&D needs.

CA and BSA recommend that the objectives of the CSIA plan be established on the basis of a truly comprehensive and holistic view of the cyber security needs of the Nation. Once a set of comprehensive, national objectives has been identified with the input of government, industry and academia, then the plan can determine what entities—government, industry and academia, whether by themselves or in partnerships—are, or should be, pursuing each of them. The Office of Science and Technology Policy is responsible for coordinating the Federal Government's efforts surrounding cyber security R&D, and should ensure that federal R&D actually supports the Nation's strategic cyber security goals. President Obama announced on May 29, 2009 the future appointment of a Cyber Security Coordinator in the White House. CA and BSA recommend that the Cyber Security Coordinator provide joint oversight and direction to this effort, alongside OSTP. Once a national framework for R&D has been established, individual agencies should be assigned R&D projects within their areas of expertise.

Second, for the CSIA plan to reflect the cyber security R&D needs of the Nation, **a wide community of stakeholders needs to play an integral role in the creation of the plan and the identification of its objectives.** CA and BSA recommend that stakeholders, and in particular the owners and operators of critical cyber infrastructure and developers of critical cyber technology, be involved from the earliest stages of the process and throughout the creation of the plan, as well as when the plan's objectives and implementation activities are reviewed. The IT industry is a key stakeholder not only because it owns and operates the critical infrastructure of cyberspace and develops its underlying technology, but also because it invests tens of billions of dollars each year in R&D.

Another important avenue for identifying cyber security research gaps is via industry-government partnership initiatives organized jointly by the Department of Homeland Security and industry organizations such as the Information Technology–Information Sharing and Analysis Center (IT–ISAC) and the Information Technology Sector Coordinating Council (IT–SCC).

An extremely timely example of such an initiative is the IT Sector Baseline Risk Assessment, a major report that will be released soon, which results from a multi-year partnership between the IT–SCC, IT–ISAC, industry subject matter experts and DHS. The IT Sector's Baseline Risk Assessment is intended to provide a cyber and all-hazards risk profile that IT Sector partners can use in particular to inform resource allocation for security research and development in core IT functions. Those key functions include producing and providing IT products and services; incident management capabilities; domain name resolution services; identity management and associated trust support services; Internet-based content, information and

communications services; and Internet routing, access and connection services. With a powerful methodology for assessing risks and identifying necessary mitigation requirements, the Baseline Risk Assessment can serve as a foundation and industry-supported model for developing a strategic cyber security R&D agenda and plan of action.

I believe the inclusiveness is very much in line with the recently released conclusions of the White House Cyberspace Policy Review, which states that *"the Federal Government should greatly expand coordination of [NITRD and other R&D-related] strategies with industry and academic efforts."*[2]

Third, in addition to contributing to the identification of the overall objectives of the national cyber security R&D plan, companies can play a role downstream in the **definition of specific R&D projects** that will contribute to reaching those national objectives. CA and BSA believe that it would be appropriate to facilitate federal support for specific research topics or projects that were not conceived originally by a federal agency, but rather pro-actively suggested to an agency by a company. In such a situation, the company is awarded funding as a "sole source." We believe a mechanism should be found that would make it easier for agencies to act upon such suggestions. Today, such a process is insufficiently used, because of legitimate concerns regarding the fairness of the award process. CA and BSA's goal is to encourage more companies to suggest promising avenues for cyber security innovation to the Federal Government. Naturally, projects pro-actively suggested by private industry should be closely related to the national R&D plan, as well as to the particular part of that plan that was delegated to the agency to which the idea was suggested.

We would like to make it clear that we do not in any way oppose the mechanism by which companies receive federal funding because they submitted proposals in response to a competitive federal solicitation. In fact, CA and other companies actively review and respond to such proposals, and we believe it should continue to represent a large part of the federal R&D funding. We merely want to find a way to ensure that, in addition to this reactive role, companies can play a more pro-active role in the definition of R&D projects.

Fourth, I would like to address the issue of short-term vs. long-term R&D. We believe it is appropriate to include both. As a general rule, however, **CA and BSA recommend that the government focus on long-term and basic cyber security research.** We believe it is appropriate for the government to be involved in applied R&D if: the technological solution that is sought is not commercially available; and its absence creates a measurable security gap.

In most cases, when government agencies seek to develop specific technologies, we are concerned that they do not check beforehand whether commercially available solutions provide the same or an equivalent capability. We recommend requiring federal agencies to ascertain whether or not commercial solutions exist—or could be readily adapted—before they invest in an R&D project to develop equivalent capabilities. This would allow the government to better leverage its limited resources. Importantly for industry, it would also ensure that the federal effort focuses more on research that may bring breakthroughs of considerable importance to the cyber security of our nation's infrastructure in the long run, but lacks demonstrated short- or medium-term commercial viability. Commercial companies rarely undertake such research by themselves, but it is an ideal topic for federal research. This recommendation aligns with the White House Cyberspace Policy Review's emphasis on R&D in *"game-changing technologies that will help meet infrastructure objectives."*[3]

We note, however, that cyber security research is underfunded when compared to other research programs. For example:

> ". . . the President's fiscal year 2009 budget requests $29.3 billion for life science research, $4.4 billion for earth and space sciences, $3.2 billion for the Advanced Energy Initiative, $2.0 billion for the Climate Change Science Program, and $1.5 billion for nanotechnology. The National Information Technology R&D (NITRD) programs will receive $3.5 billion. Cyber security will receive about $300 million."[4]

In order to increase cyber security for the Nation, funding for fundamental and applied research in cyber security is required. Keeping current funding levels will

---

[2] Cyberspace Policy Review, pp. 32–33.

[3] Cyberspace Policy Review, p. 32.

[4] From "Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cyber security for the 44th Presidency," December 2008, page 74. This report is available at *http://www.csis.org/media/csis/pubs/081208_securingcyberspace_44.pdf*

result—at best—in maintaining the current level of progress and therefore the current inadequate level of cyber security.

Companies have an important role to play in fostering greater engagement with academic institutions and government. For example, CA today works with universities in a number of ways. Through the CA Academic Initiative, colleges and universities can get free access to select CA products, faculty education, professional courseware and technical support. CA also has a strong partnership with Universities for research. For example, CA is working with the University of California Davis and Pacific Northwest National Laboratory on insider threat research and with Dartmouth University on determining the benefits seen by organizations in the deployment of security software. CA is also working with Carleton University in Canada on data leak prevention research. This research is partially funded through the Canadian government's NSERC Strategic Network Grant.

Finally, for federal cyber security R&D to best address the needs of industry, it is important that we facilitate the migration path of technologies developed through federal R&D, so that they can more quickly and widely contribute to improving our nation's cyber security. This is another issue on which our recommendations are consistent with the direction advocated by the White House in its Cyberspace Policy Review.[5] CA and BSA propose two avenues to ease technology transition onto the marketplace. First, provide greater incentives for industry to participate in federally funded cyber security R&D by looking at the status of the intellectual property (IP) it generates. We recommend that Congress explore ways to make such industry participation more appealing through improved IP ownership or licensing, similar to what Congress did for small businesses, non-profits and universities through the *Bayh-Dole Act* in 1980. Second, the Federal Government should improve its sharing of the innovations generated by cyber security R&D conducted by federal agencies. Too often, those innovations are not shared with industry, where they could benefit the Nation as a whole through productization, even with licensing conditions that appropriately reward the agency in question.

SPECIFIC CYBER SECURITY R&D TOPICS

The second issue that you asked that I discuss in my testimony is that of specific topics and gaps in federal cyber security R&D:

Does the current range of federally supported research adequately address existing cyber security needs as well as new and emerging threats? If not, then what are the current research gaps and priorities?

As I discussed above, we need a long-term, strategically-focused, national research agenda developed in partnership between the Federal Government and industry. As we look to the future, we see a number of trends that will impact both the cyber infrastructure as well as specific cyber functionalities. An understanding of these trends can be useful in informing research planning and prioritization. What are some of these important trends?

- **Increased bandwidth and connectivity to a virtually unlimited number of devices.** The number of devices connecting to the cyber infrastructure continues to grow: desktops, laptops, smart phones, GPS devices, cars, houses and many more to come. The available bandwidth continues to grow both in the cellular environment, the wireless environment and the wired environment. Managing cyber security risks in this new world will push our existing security technology beyond its limits given the sheer scale of networked devices and speed of communications.
    - CA recommends federal support for advanced research in the area of threat detection, systems management and security management allowing security controls to scale to this emerging cyber generation.
- **Huge amounts of storage and computing power will be present in the home, in the enterprise and in the network.** More sensitive data in huge volumes will be stored and shared among businesses, government agencies and consumers. The technical disciplines of digital rights management, data leakage protection, and data classification are in their infancy from a technology perspective. Digital rights management is the process of embedding and managing access control within data. Data leakage protection refers to the identification and control of sensitive data. Data classification refers to

[5] Cyberspace Policy Review, p. 33: *"To enhance U.S. competitiveness, the Federal Government should work with industry to develop migration paths and incentives for the rapid adoption of research and technology development."*

the process of tagging data to indicate it is sensitive, owned by an individual or part of a larger system, and to associate it with controlling policies.

  - CA recommends federal support for advanced research to move these technologies into the mainstream where data can be tagged appropriately and managed in accordance with policy-driven rules, under the control of the entity or individual responsible for its care.

- **Greater expectations for managing identity risks.** The exponential growth of interconnected applications and systems will require advances in identity management technology. Today's user name and password model is inadequate. Stronger forms of authentication are available, but their acceptance and adoption have been slow. Similarly, the lack of a monetization model for strongly validated identities has limited their commercial success.

  - CA recommends federal support for advanced research to help with the development of new technology and new business models that are acceptable to consumers and industry.

- **Emergence of new, interactive social networking applications.** Social networking continues to go through many changes.

  - CA recommends federal support for advanced research to develop models enabling people to collaborate safely and securely, both to share the data they wish to share and to maintain anonymity as needed.

- **Universal business connectivity, collaboration and partnerships.** Businesses no longer operate independently; it is necessary for them to collaborate and share data as well as establish enforceable security policies. For example, a small hospital with 5,000 employees typically has 50,000 people in its user directories and collaborates with other hospitals, universities and health care providers. Today's technology can support these business and clinical relationships, but more advanced technology is necessary to truly enable a secure and auditable infrastructure as the collaborative environment expands almost exponentially.

  - CA recommends federal support for advanced research to enable a federated model where security and responsibility are technically manageable at the scales we expect to occur.

- **User manageability and interaction.** It is becoming more and more difficult for someone to live an unconnected life. Although technology has provided amazing capabilities, the device-human interfaces used to connect and interact with context and applications have not fundamentally changed.

  - Although browsers have greatly improved and are now being embedded in personal devices, as we look to the future CA recommends federal support for advanced research into flexible and manageable technical interfaces, displays and supporting instrumentality that incorporate seamless understanding, manageability and security functionality for users in many different environments and contexts.

- **Increasingly sophisticated cyber adversaries.** As I said at the beginning of this testimony, our cyber adversaries are sophisticated, they move rapidly and adeptly to exploit weaknesses and vulnerabilities.

  - CA recommends federal support for advanced research to create test tools and products that can identify vulnerabilities, logical inconsistencies and inappropriate "back doors." A new generation of tools would give application builders the ability to identify and fix vulnerabilities as well as meet industry security certifications more quickly and reliably.

- **The growing focus on insider threats.** As industry reacts to threats, cyber adversaries look for alternative business models. The insider is one of the most effective.

  - CA recommends federal support for advanced research into insider threat detection and advanced data leakage protection.

Let me now briefly turn to the final two questions you have raised.

CYBER SECURITY IN HIGHER EDUCATION

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?

My comments focus on the education of the technical workforce that will be responsible for the engineering of our applications, the implementation of our systems and the processes necessary to run these systems. Security is an important element to each one of these areas.

Cyber security education should consist of courses in secure coding practices, security architectures and security of complex systems. Colleges and universities have made great progress and security courses are mandatory in many programs. While still inconsistently deployed, there is also a movement within universities to incorporate secure coding practices into programming courses.

The level of security knowledge for graduates has greatly increased, but in many cases it lacks real world experience. The security knowledge tends to focus more on secure coding practices and less on implementation and system design. In order to fill the gap large software vendors have implemented programs to reinforce security design and secure software development practices to their existing and new employees.

Separate from the issue of developing *secure* systems is that of developing *security* systems and architectures. In this latter case students require more specialized knowledge of security, such as identity and access control, authentication, threat detection and response, cryptographic systems such as public-key cryptography, etc. Knowledge at this level tends to be obtained at the graduate level, and can be broadly categorized as operationally focused (typically the Master's level degrees) and research focused (doctoral degrees).

The National Security Agency has a history of supporting security education through their National Centers of Academic Excellence in Information Assurance Education program, where they certify programs that meet a minimum set of requirements. These programs produce students who have a broad understanding of security and who can perform operational roles ranging from being responsible for the information security of an organization to understanding functional requirements for security-related software.

At the doctoral level, the focus is on longer-term research in order to improve the cyber security field. This requires not only students who are interested in cyber security research, but also faculty who are active in this field. Government support at this level consists of providing support for students (e.g., through National Science Foundation grants and scholarship-for-service programs) and of supporting faculty research. Such programs should be strengthened.

PUBLIC AWARENESS AND EDUCATION

Allow me to turn to the last topic that you had asked me to address, that of cyber security awareness of the general public. Specifically, your question was:

What role can the Federal Government play in educating the general public about protecting themselves and their networks against cyber threats?

To address the need to increase public awareness of cyber security, I will draw upon the position of the BSA. CA and BSA believe we need to increase our national efforts to educate and raise awareness of the public about their cyber risks, and how they can protect themselves online, for two reasons. First, to decrease the likelihood that they will become victims of identity theft, and other harms that may befall them online. Second, to decrease the likelihood that consumers' computers will be hijacked to serve as launching pads for larger attacks against businesses, the infrastructure and our government—the botnet phenomenon.[6]

CA and BSA agree with the White House's Cyberspace Policy Review's recommendation that the Federal Government, in partnership with educators and industry, should develop a national cyber security public awareness and education strategy. Its objective should be to educate about the threat as well as about changing public attitudes online, towards greater cyber security as well as digital safety and ethics, to promote a responsible and ethical use of the Internet.[7] There are many such efforts: the National Cyber Security Alliance is a partnership between

[6] A bot is a computer that has been infected by a cyber criminal—known as a bot-master—so that the bot-master can control it remotely and use it, along with many other hijacked bot computers, to carry out various types of large cyber attacks, from sending out spam and phishing e-mails, to disseminating to malicious code, to performing distributed denial of service (DDOS) attacks against banks or government IT systems. The largest networks of botnets (networks of bots) can number in the hundreds of thousands, if not millions.

[7] Cyberspace Policy Review, pp. 13–14.

the Department of Homeland Security (DHS), the Multi-State Information Sharing and Analysis Center (MS–ISAC), corporate and non-profit partners to promote cyber security awareness for home users, small and medium size businesses, and in primary and secondary education. Information about their year-round campaigns, which culminate in National Cyber Security Awareness Month every October—and I note that Congress has for several years now recognized the October campaign in a resolution of support—can be found at *www.staysafeonline.org* I also want to mention the *www.onguardonline.gov* effort led by the Federal Trade Commission, as well as the *www.playitcybersafe.com* campaign of BSA, which offers tools and educational material for children, parents and educators about how to use the Internet safely and responsibly.

One final comment: educational programs will be most effective when targeted to specific age groups. For example online activities may be very different for five- to ten-year-olds, 10- to 13-year-olds, 13- to 17-year-olds and people over 18. Each age group has specific needs and should have appropriate messaging and education. The non technical community in all age groups is moving to cyber platforms at an unprecedented rate, and all need to understand the rules and the risks in the context of their work, social and academic life, and environment. This is another area where partnership initiatives are vitally important.

Mr. Chairman, Ranking Member Ehlers and Members of the Subcommittee, I appreciated the opportunity to appear before you to share some thoughts on cyber security R&D, cyber security education, and public education and awareness of cyber security. CA shares the Subcommittee's goal of helping to enhance cyber security, and we would be happy, together with the Business Software Alliance, to work with you towards this goal.

I would be happy to answer any questions you may have for me.

Thank you.

BIOGRAPHY FOR TIMOTHY G. BROWN

Timothy G. Brown is the Vice President and Chief Architect for Security Management for CA, Inc. He has overall technical direction and oversight responsibilities for the CA security products. This includes Identity Management, Server Security, Data Leakage Protection, Web Access Management and Single Sign On.

With over 20 years of information security expertise, Brown has been involved in many areas of security including compliance, threat research, vulnerability management, consumer and enterprise identity and access management, network security, encryption and managed security services. In his career, Brown has worked with many companies and government agencies to implement sound and practical security policies and solutions.

Prior to joining CA, Brown spent 12 years at Symantec's CTO office, where he was responsible for company-wide technical architecture, integration, gap analysis and technical strategy. Prior to joining the Symantec CTO office, Brown focused on Symantec's enterprise security architecture and the collection, correlation and prioritization of security data. Brown joined Symantec through the company's acquisition of Axent Technologies. At Axent he was responsible for the Identity Management, Single Sign On and multi-factor authentication products.

Brown is an avid inventor with 14 filed patents in the security field. He is active in promoting cross industry initiatives and has participated on a number of standards boards.

Brown earned a Bachelor of Science degree in computer science from MCLA and has participated in the Wharton School of Business Executive Education program.

DISCUSSION

Chairman LIPINSKI. Thank you, Mr. Brown. I thank all our witnesses for their testimony. At this point we are going to begin our first round of questions, which is the real fun point of these, so I am going to save my questions for the end and I am going to recognize Mr. Tonko for five minutes.

Mr. TONKO. Thank you, Chairman. It was made mention that we need to constantly update curriculum and make certain that we are creating state-of-the-art education for our cyber security professionals.

Dr. Schneider, you and I claim New York as our base of operations, and we have a wealth of community colleges. Is there potential to draw in the infrastructure of our community colleges and develop some earlier investment in cyber security professionals? And I would throw out, into the question I would make the statement of the unusual glut that seems to be emerging in terms of professionals from outside our borders that are addressing this field, this arena, and we are not growing and cultivating domestically the talent we require.

Dr. SCHNEIDER. Yes. Thank you for the question, and I completely agree with the premise that we need to employ a broad-spectrum educational approach to the problem. We are not going to solve this problem only with Ph.D.s or only with Bachelor's graduates. There are jobs that are suitable for somebody educated at the level of a community college, and there is life, which means people educated at the level of K through high school—and actually those of us who have graduated long ago and need to exist for some years to come—need to have a much more sophisticated view of what is going on. So I believe there is going to be a broad spectrum of jobs available, some of which we would do best to train people at the community college level for, and I believe the community college will become more and more sophisticated as we get a better understanding of some of the cyber security challenges.

Mr. TONKO. Are there others on the panel—and by the way, let me thank the panelists. Your information is very helpful. Is there anyone else that would like to respond to that? Dr. D'Amico.

Dr. D'AMICO. I think you raise a very interesting point about the role of community colleges, and I fully agree with you that there are not enough U.S. citizens who are being trained in this area. I think community colleges can participate in the training of security professionals because as we have learned, this is not all about academic education. There is a lot of learning by doing, and I think that we should incentivize the private sector to bring the community college students into internships. I sit on the Board of Directors of the Metro chapter of ISSA, which is the second-largest chapter of security professionals in the world right in New York City. We have people who want to bring in interns from places like community colleges to work with them, so I think this is part of structuring a mentorship program.

Mr. TONKO. Thank you.

Dr. Goodman.

Dr. GOODMAN. Let me return to the Scholarship for Service program for a moment and talk about one of the offshoots of that effort. Having these students, by the way, has enabled quite a number of departments—computer science departments or MIS departments around the country—to build their own capacity, and several of them use that greater capacity to seek roles in trying to develop curriculum and educate students regionally in other institutions, particularly community colleges and law enforcement schools in their areas. I mention in particular Mississippi State University and the University of Tulsa. And there is a very strong feeling among most people who are very seriously concerned about developing a workforce and an educated user community that this effort must be extended far more broadly than just the universities in

this country, and I would also again endorse the idea of programs that specifically are geared to do that.

Mr. TONKO. Thank you.

Ms. Franz.

Ms. FRANZ. Thank you. I would only like to add the notion that as we discuss a broad spectrum of the kinds of education and skills that can contribute to resolving the problem that we don't then funnel all of our students into very rigid, specific requirements for cyber security professionals. The multidisciplinary nature, the multi-faceted types of education that can contribute to resolving the problem is something we need to retain. Imagine that those that might be working in the cyber security field now did not get a college degree and yet they are doing—they are big contributors. If they were shut out of the ability to provide that, that would be a detriment.

Mr. TONKO. Thank you.

Thank you, Mr. Chair.

Chairman LIPINSKI. Thank you, Mr. Tonko, for your questions.

The Chair now recognizes Dr. Ehlers for five minutes.

Mr. EHLERS. Thank you, Mr. Chairman. It is a little hard to know where to start. It has been very rich testimony and very, very helpful. Several of you testified there needs to be better interaction between the government and the private sector with regard to cyber security, and by the way, these questions are going to be for everyone because I picked up ideas from all of you.

And Ms. Franz, I believe, testified a more formal mechanism needs to be put in place for private sector input and collaboration, and so one of the questions I am asking is, what has your involvement been with NITRD or any of the mission agencies to initiate such interactions or discussion? Have you been rebuffed or have you been accepted, and if you have been accepted, how have the conversations gone?

Dr. Goodman, you also note in your testimony that market forces have failed to provide the Nation with a level of cyber security adequate for its needs, and this seems to imply that government regulation or other significant intervention is required to achieve adequate cyber security, but it seems to me the government hasn't done that good a job itself in governing its own needs, and so the question is, can the government really provide the leadership you need or it is just the money you need, or how can we reach the point that you and I both seem to want to get to?

One other aspect as some of you mentioned, it is hard to recruit people for security jobs, and it wasn't clear to me whether it is because these jobs are not particularly appealing. Perhaps computer experts would rather be programming rather than playing cops-and-robbers. I don't know. Or maybe you have to appeal to cops-and-robbers people and provide them with appropriate cyber security training. But I am just wondering if the cyber security jobs are just not appealing enough to the people that you are trying to get. So it is a potpourri of questions but I think you are all sort of focusing in that same area.

So, Dr. Goodman, if you would kick it off, and we will just go down the line.

Dr. GOODMAN. Thank you, Mr. Ehlers. I think a fundamental problem out there that is largely behind the statement that I made is that for a variety of reasons, cyber security has frankly not been taken as seriously as it should be in putting all of these systems out there that are simply so vulnerable. Security has not been a major design consideration. It has not been a major driver for the businesses who are out there in cyberspace doing whatever they do in cyberspace. There has been no pressure on them, and when things go wrong, they usually are not the people who suffer the consequences. I am a believer that, as is the case with lots of other security and safety issues and other infrastructural domains, that some requirement, if you would like, needs to be made on those who are in the best position to mitigate risk to do so; and that may in fact require regulation, may require certain kinds of laws that for example heighten liability; it may benefit from coming up with the kind of technology that is so easy to use and so cheap to use and so easily integratable with what we have out there now that you just cannot not use it. Nevertheless, we have a situation where much of cyber defense is pushed on the end users, you and me and all the other citizens and organizations that are out there. This is partly built into the architecture of the Internet and other things, and we are increasingly incapable of defending ourselves against increasingly capable attacks and attackers. So an effort must be made to get those people who are in the best position to mitigate risk to do so, and I think what should be done and it has been done in other areas, industry and government need to get together and they need to get together under some perhaps formal form or other kind of institutional mechanism with the mandate that they come up with greater security in cyberspace. It is as simple as that. There are again other—most recently this seems to have produced some results in the electric power industry where there has been great concern about how vulnerable increasingly IT-controlled electric power generation and distribution may be to outside attacks or to other forms of failure, and FERC, the Federal Energy Regulatory Commission, got together with the industry associations and basically came up with mandated standards for the systems that they use to generate and distribute power, and I fear something like that will have to be necessary, particularly with regard to mobile telephony but elsewhere as well.

Mr. EHLERS. Thank you. Good comments.

Ms. Franz.

Ms. FRANZ. Thank you for your question on the partnership efforts. Most of the interaction that we have had with NITRD has been through our increasing dialogue with the Interagency Working Group on Cyber Security and Information Assurance, so we have had more and more discussions in the work of the Information Technology Sector Coordinating Council, or ITSCC, under the NIT framework that I mentioned, and that has been increasingly positive as well. However, I would like to say that we would like to see that discussion and dialogue start at the very beginning of a process rather than at the end, you know, where a document may be presented for review and input but at that point it is almost too late to do so, so the dialogue hasn't started in the beginning so you might see overlaps at a time that is too late. You might miss gaps

in things that needed to be done and weren't. And you might see areas where innovation might be stifled by the proposals that the government may make. So I would say that in order to avoid all of those landmines, we would want that partnership to start earlier. But our dialogue has been increasingly positive and rich and we are finding out a lot more about what industry is doing, what government is doing and where we can coalesce those efforts more productively.

Mr. EHLERS. So progress is being made but you would like it to be more formalized and proceed more rapidly?

Ms. FRANZ. Agreed. I mean, I think that a more formal process, a mechanism, as I mentioned, would enable that interaction at the earliest stage and get the expertise of both government and industry and other stakeholders in the room at the table, perhaps with a blank document, as some have mentioned, rather than a fully fledged product.

Mr. EHLERS. Okay. Dr. D'Amico, what can you add?

Dr. D'AMICO. Thank you. You have raised some interesting questions. I would like to address the one about how we increase the number of cyber security experts in the United States. The thing that is keeping this from happening is not the money. We know that they are well paid. In industry, the average salary for a security manager is $108,000, in the Federal Government, it is $98,000, and in the state and local, it is $79,000. So it is not the money. I think it has to do with three things. One is the availability of jobs, the second is the perceived status and the third is the lack of U.S. citizens. There are not that many jobs available in industry, and I think it is because they don't see the return on investment. The only reason that people are really investing in security is because of the compliance legislation, but from an economic perspective, they don't see the ROI. In the military, there is no real perceived status for being a techie in the military. If you are in the cyber defense force, you are not on the path to advancement and so you have to move out of that in order to advance in the military. And then with respect to U.S. citizens, more and more of the advanced degrees in information security and computer science are not granted at—not as many of them are granted to U.S. citizens as in prior years, and so a lot of Bachelor's degrees are given to U.S. citizens. Only, I think, eight percent of the degrees are to foreign nationals but by the time you get to Ph.D.s, there 38, 39 percent are given to foreign nationals, so we need to change that around as well.

Mr. EHLERS. Thank you. Dr. Schneider.

Dr. SCHNEIDER. If you want somebody to get to do something, there is this basic dichotomy of the carrot versus the stick. The only way industry that plays in cyberspace—not the cyber security industry but companies that benefit by doing business over it—are going to build more-secure systems, is if they are somehow incentivized to do that. Return on investment is the carrot. Legislation is the stick. I am not an expert on suggesting which way to go but I will point out that if there was an incentive structure, then two problems would be solved. One, there would be employment of experts and cyber security experts might be technical and they might be policy oriented, and second, companies would be very anx-

ious to facilitate tech transitions from researchers into companies. You have only to look back at the dot com era to notice that lots of good ideas were being discovered in research and were very quickly being monetized in the industry community. So there was an incentive structure. It was a carrot in this case, and it moved. It is the lack of incentive structure that in my opinion is what is holding things up.

Mr. EHLERS. Thank you. And finally, Mr. Brown.

Mr. BROWN. It is one of the things when we look at research gaps and try to resolve some of those between industry and government. You know, we look at these gaps, we identify these gaps. Industry today is focused, you know, primarily on satisfying their customers' needs today. We prioritize those needs. We staff for those needs. We make sure that we are creating products that can meet those needs today. One of the major challenges industry has is, how can we prepare for things that are going to happen five, six, seven years from now, how can we set up that infrastructure that is really going to prepare us for that, and, you know, there is a challenge there that says those investments are very high risk. You know, how many of those investments are going to really be fruitful, and as we looked at the list of the research areas, when we see those, we see that they are identified as areas but really plans are not put into place to say how we are going to address those areas. Some of those areas are better left to research of government. Some of those areas are better left to research for public and private partnerships. Some of those research areas are better for university research. It is important that we lay out plans to address each one of those areas and stay to those plans.

Mr. EHLERS. Okay. Thank you very much, very useful.

Chairman LIPINSKI. Thank you, Dr. Ehlers, for your questions, but now you know that you have used up your question time for the next two hearings also, so——

Mr. EHLERS. That is fine.

Chairman LIPINSKI. No, that was very interesting and very good questions and good answers, very interesting responses there. I will now recognize myself for five minutes.

Some of the things that I was going to ask about, some of the other Members have asked questions along those lines. I want to follow a little bit more—I am not sure if there is more we can learn or not but I just want to push a little bit more on one of those questions Dr. Ehlers just asked. It seems like one of the issues that we face with cyber security is that everyone thinks that it is not their problem, from individuals to companies, whether they have, you know, companies are producing software or operating systems or companies that just have data that is not protected. So I think that one of the issues—and I also think that there is not enough attention paid to this also. I am very happy that the Administration is paying attention to it because it is shining a light on this and what is going on and that is not just a political statement. I am very happy to see that because I think that is really needed in our country because a lot of people, they hear cyber security, they don't realize how much impact it is going to have on them. But just take an example. Yesterday Microsoft issued updates that patched 31 vulnerabilities in Windows and Office programs including 18 bugs

that they marked critical. You know, just focusing on Microsoft there, yes, I do use an Apple computer, a Macintosh operating system, always have, but not just to pick on Microsoft. But where—how do we better incentivize? Like I said, you have all kinds of different individual types of companies. How do we better incentivize trying to get these, whether it is on software programs, how do we keep data better protected? You touched a little bit on this, but does anyone have anything to add on that right now? Dr. Schneider.

Dr. SCHNEIDER. I think some sunlight would help. I think we don't do a good job of informing the population about the risk or about the consequences. You have a good notion of what the chances of being burglarized if you walk in any part of this city or probably the city you have come from. You don't have any notion of how often successful penetrations are occurring at banks or military installations or any of the attractive targets. There are good reasons why these institutions don't make this information public, yet if you look at the success of the California breach legislation that is now spreading throughout the Nation whereby when private information is disclosed, the institution that leaked it is obligated to inform the potential victims. That has had a very interesting effect and raised the consciousness both of the owners of this data and of people at large. So I see all this talk about raising public consciousness and public campaigns. I think if business were more obligated to be candid about what was happening, we would all understand and build a better model of the risks, and once people are more concerned about it, I think that is going to drive innovation and deployments.

Chairman LIPINSKI. Mr. Brown.

Mr. BROWN. Yeah, in the past few years, you have to remember that the software industry is, you know, ever changing. Our threats are ever changing. The adversaries we are up against are changing as well. So when we look at software vulnerabilities, you know, just four or five years no one had a plan in place to train their software professionals. Now I can't think of any large software vendor that doesn't put their coders through at least secure code training. So the level of awareness has raised to, you know, a very good extent. Now, we have to deal with a lot of things from the past so software that was written five years ago is still in place. Software slowly moves out of both industry and consumers, and, you know, the industry has done better at announcing vulnerabilities and, you know, they should be applauded for announcing vulnerabilities and working with—working in ways to patch those vulnerabilities as quickly as possible. So overall, I think the industry is getting better. Now, can we do more? Absolutely. Should we have more trained people coming into our organizations? Yes. Should we have better, more trained professionals? Absolutely. But things are taking time but they are getting better. So we have to remember where we were three years ago versus today.

Chairman LIPINSKI. Ms. Franz.

Ms. FRANZ. I would like to build on a couple of things that my other distinguished panelists have mentioned. First, I think there is still a great need for awareness or sunlight, as Dr. Schneider said, on what the issue is, and particularly there is only a small

community that knows what the threats are to them or what the activity is in cyberspace and so we have often asked for a mechanism that allows more information sharing between the government and industry on just what the problem is and what are the problems we are trying to solve. That certainly needs to be done in as trusted environment as possible, so that goes back to the partnership mechanism, but that information sharing and exchange is important.

I would like to touch upon the incentive piece from a positive side of the equation, more of a carrot and stick, I suppose. Dr. Schneider mentioned the data breach notification laws and certainly that is something TechAmerica has been actively engaged in, particularly looking at the requirement for notification when there is a breach and providing for a safe harbor for industry and companies or other organizations, government or academic institutions if they have taken protective steps to protect that data before it could even be breached, to render that data unreadable, unusable, and so there is a presumption of a lack of harm in that instance. And so on the one hand, it incentivizes companies and other organizations to take protective mitigative steps before hand and then makes the data unreadable, unusable if it is accessed. So that is a positive incentive to look at sort of the carrot-and-stick approach. I also might suggest that we consider ways that the tax structure could benefit efforts in R&D or other investments in cyber security efforts.

Chairman LIPINSKI. Thank you. I am over time, but I want to throw one other part in here. Dr. D'Amico talked about how we need a cultural shift here so that people understand that what they are doing and the damage that can be caused, and I will give the credit where it is due. John Veysey, who works for me, sitting behind me, said if I wanted to cause trouble, what I would do would be to take some thumb drives and throw them out in the parking lot with a Trojan horse on there because almost everyone is going to pick it up, take it in the office and plug it into their machine just to even see who this might belong to, just things as simple as that. How do we change people's habits and just automatic reactions that they have that can be very dangerous and cause these vulnerabilities? How do we reach out to the general public to do that? Dr. D'Amico.

Dr. D'AMICO. We need a marketing campaign, and Americans are very good at marketing and there is a lot of research on how to market effectively to Americans. People want to be good U.S. citizens and we really need some kind of marketing campaign for individuals and for companies that you too can make a difference, engaging good computer hygiene so that before—they wouldn't touch a dirty object on the ground because of health considerations. They shouldn't touch a potentially dirty thumb drive on the ground because of computer hygiene considerations, and I think it is well within our capability to engage in a public awareness campaign using everything we know about good marketing. I think the second thing, and this is much harder, is that we really need to understand what the impact is of any single failure. So if somebody picks up that thumb drive and sticks it into the computer and they get some kind of infection, what are the cascading effects of that? We

really don't know, and this really is a ripe area for research. We don't know enough about the interdependencies within an enterprise and across enterprise to be able to say you pick up that thumb drive, you put it into your computer, well, guess what? Somebody in a bank account two states away from you is going to have some money taken out of their account. We just don't know that and we need to study that.

Chairman LIPINSKI. Dr. Goodman.

Dr. GOODMAN. The problem of educating the public or making the public really fear what might happen to them out there is very, very difficult in this domain. We have a situation—I mean, in other domains usually there is some immediate physical threat that gets public interest and arouses them to protect themselves and to get help from others to protect them. This kind of threat for most users, not only in this country but especially around the world, it is so remote, it is so abstract, they are connected to these systems. They see all the good stuff that is going on out there. That is why they are spending so many hours at terminals, on their cell phones and what have you, and any kind of threat is out in oblivion someplace, okay, and physically it may well be out on the other side of the world. They don't see the immediacy. They don't see—and it is very difficult to educate them to this, given so many other things they have to think about. And we have again a situation where even when the public has seen immediacy, for example, in the world of automobile safety, those industries that are in the best position to do something about it have had to have a great deal of government push to do something to protect the public, and I don't think the public—each individual out there can do things to help them as they do with their homes, with locks on their doors and what have you. That is not going to be enough, and the public doesn't fully appreciate it and I am not sure what kind of educational program will bring it home what kinds of risk they have out there.

Chairman LIPINSKI. Thank you. I have gone way over time here so I am going to conclude at that and recognize Mr. Neugebauer.

Mr. NEUGEBAUER. Thank you, Mr. Chairman, and thank you for calling this hearing. I think the first question, in most of your testimony you indicate that a lot of the infrastructure for cyberspace is in the private sector, and a lot of ideas have kicked around of how to enhance the cyber security, and one of those is to establish a rigorous regulatory regime to impose on these private companies and I think the second one is to somehow give those companies some kind of liability protection for maybe mandates that the government would impose on those companies to do certain activities. So those are two ideas. One of them sounds like more big government. You know, what are your thoughts on the current things that are being talked about. And third is, are there better ideas that we need to be thinking about? I will throw that open to whoever wants to jump in.

Ms. FRANZ. I will take the first cut at that. I think that certainly right now we see a lot of proposals for the kinds of things that either regulatory or—the regulatory nature or with regard to practice requirements. The problem is, while the bulk of the information technology or cyber security or critical infrastructure is owned and

operated by the private sector, the issue is, it moves so quickly. We see transitions and evolutions in the technology at a very rapid pace and legislation is not always the best way to address that, at least not in very specific ways. It usually is a blunt hammer for a very specific problem. So if there is a way to identify the problem, and again, I would suggest doing that in a collaborative sense, and then finding the best way to approach it, either through a standard or a best practice in many of the collaborative bodies that we have, either standards bodies nationally and internationally. Again, it is also a global issue. We don't want to put into place a regime that is restrictive, would be irrelevant in a very short period of time and then is either conflicting or provides—causes extra burden on companies or other organizations that have national and multinational operations. So it requires a really good robust dialogue on the best way for legislation to address the issue as well as other mechanisms.

Mr. BROWN. Ms. Franz also brought up the point of standards, and standards are extremely important when we look at adhering to—as software is developed, adhering to standards will help us have more consistent and more secure infrastructure across the board. So that is also an extremely important component of this. You know, the infrastructure players in the private sector are—you know, they are driven to do the best that they can. You know, you see who is out there and who hasn't survived, and, you know, the bottom line is, if they don't do their job, they don't do things securely, they don't do things in high-bandwidth methods, then, you know, they won't survive as a company. So there are a lot of incentives for the private sector to do the right thing here.

Mr. NEUGEBAUER. I agree with you, and I think that is one of the things that kind of concerns me about, you know, the government stepping in. Sometimes when the government does that, it leaves a false impression that oh, the government is watching out for me now and so I don't have to be careful, I can pick up that thumb drive, you know, and so I think we ought to—because most companies are very competitive business.

Mr. BROWN. Absolutely.

Mr. NEUGEBAUER. And, you know, they encourage you to buy firewalls and virus software because they know that if you have a disruption in your service, something that came over their network, whether they could have, you know, prevented it or not, there is problems to do that.

I want to move to another area, and that is with the huge amount of growth in the use of PDAs and cell phones and texting, you know, that has become a huge piece of our world. Dr. Goodman, you kind of mentioned that in your testimony. What is going on as far as threats to my PDA and to my cell phone and what—I don't know. There may be virus software and firewalls for PDAs but, you know, I am not aware of it. So can you kind of update us on that?

Dr. GOODMAN. There is nothing in this world, I mean world, expanding faster than cellular telephony and mobile devices more generally, and to perhaps restate some of what I said earlier, I think before you came, the devices are becoming increasingly powerful computers. Many are not yet around the world but the trend

is very much there, and as such, they have all of the vulnerabilities, particularly as they become the principal devices for most of the world to connect to the Internet, that you have such things as laptops and desktop computers. So everything that is seen as a vulnerability that can be exploited with desktops and laptops will be coming with those cellular devices. I can guarantee that. Plus, and I rattled off a number of other features that are associated with mobile devices, that are uniquely vulnerable to them such that they use airwaves. They have very limited battery power and there is a disinclination on the part of everybody, the providers, the cell phone manufacturers and what have you to use up some of that battery power for security kinds of functions. I could go on and on. The list is really very substantial. I believe, and I used the word "tsunami" in my oral statement, that there is a tsunami of insecurity far greater than what we are seeing now coming with those devices, okay, and it will be worldwide, and to make another point with regard to worldwide on a comment that you raised, Mr. Representative, there are limitations. You used the term "rigorous regulatory regime" and I advocated more regulation or at least thinking about regulation. There are limitations to that and everything else that everybody has raised here with regard to educating the American public and what have you and that is, we are dealing with infrastructure to an extent like no other on this planet that is connected to the rest of the world and you can regulate U.S. businesses, you can regulate U.S. users. Universities have been dropping. Our universities are not the best protected places on earth, I hate to say, but what sort of leverage does that regulation or law enforcement have on the other 200 countries or semi-sovereign entities where the Internet and cellular telephony all come to ground and some real thought has to be given to that and I am afraid close to no thought has been given to that except from a law enforcement standpoint around the world. And I will also say that as a crime and punishment approach, you know, people who are doing things out there are almost safe from being caught and prosecuted. Real attention needs to be given to prevention and recovery, and the world as a whole, much even worse than the United States, is giving very little thought to that.

Mr. NEUGEBAUER. Just a quick follow-up, Mr. Chairman?

Chairman LIPINSKI. Thank you. We are going to have to—if we have time, we can come back. We have a couple more members that have questions to get in here. The Chair will now recognize Mr. Carnahan for five minutes.

Mr. CARNAHAN. Thank you, Mr. Chairman, and welcome to the panel. I had a few questions I wanted to jump through, so I will try to move this along.

First, I wanted to ask, what is in the panel's opinion the most effective route for small innovative companies that have new cutting-edge technologies to get visibility and consideration within the Federal Government cyber security area? Yes?

Dr. D'AMICO. Well, I am from a small business in New York and we do cyber security research, so I could say from experience that the Small Business Innovation Research Program is one of the best vehicles for small businesses to become involved in cyber security. It is an excellent program and it requires that the small businesses

not just work in cyber security and R&D but also transition the technology. So I think that that is very important. One of the things that hurts small businesses and innovations is the common criteria certification that is required on security products. In order to get a new security product used in the Federal Government, one has to go through a very expensive common criteria certification. Entry-level price is about a quarter of a million dollars and very few small businesses can afford that, so as a result you have some of the most innovative ideas that really never get into the Federal Government because of this certification requirement.

Mr. CARNAHAN. Thank you. Anybody else on that? Ms. Franz.

Ms. FRANZ. I would like to touch upon two aspects. One is I think building upon the awareness aspect. There are several mechanisms for making small business and other users more aware of the steps they can take to protect themselves, so looking at it from that perspective, what does a small business need to do vis-à-vis what a large company or individuals need to do, and one great resource for that is the National Cyber Security Alliance, which is involved in a lot of awareness efforts and a partnership with the Department of Homeland Security. Those kinds of efforts certainly could be bolstered to have more of a marketing campaign-like effect that Dr. D'Amico alluded to earlier and I think would be positive.

With regard to how they can take advantage of cyber security efforts in the government, I just think it is a great awareness need, outreach need, a look at how procurement efforts can be undertaken to take those into consideration and make it easier for them to participate.

Mr. CARNAHAN. Thank you. In the defense reauthorization bill, section 254, entitled "Trusted Defense Systems," it calls for an assessment of various methods of verifying the trust of semiconductors procured by the Department of Defense from commercial sources for use on mission-critical components potentially vulnerable defense systems. How can the Federal Government better prepare and provide for these critical needs in a more comprehensive manner and a more timely schedule to meet those critical semiconductor requirements today? Yes?

Dr. SCHNEIDER. So I think you are alluding to what is known as the supply chain problem wherein we are now purchasing semiconductors, boards and software from abroad, either through U.S. companies or not, and using them in defense systems, and we are using them also in private sector systems which are used in defense and which are controlling critical infrastructures that are not used in defense. This is a big problem, and it does not have a short-term solution. It is a very difficult problem involving probably five to ten years' worth of research before we will have some basic engineering approaches to solve it, and we should appreciate the severity of the threat and hope that the sophistication of our attackers is not at the level it could be.

Mr. CARNAHAN. Anyone else on that? Ms. Franz.

Ms. FRANZ. I would just like to highlight the notion that suppliers, whether they be U.S. companies or otherwise, are very aware of the vulnerabilities they have if something goes wrong. So they have taken steps in a number of ways to address their supply chain cycles and efforts in order to shore that up along the way.

Of course, there are always situations in which that doesn't happen. Those measures aren't undertaken and not only the company but others could possibly see the ramifications of that, but before we do anything that disrupts the economic model that many companies and governments are benefiting from, we need to have a discussion about how best to construct that in a positive way. So again, that partnership is really important to figure out exactly what is happening, what is industry doing, perhaps what it is and what the parts that need to be addressed before we disrupt the system, and thereby restrict the kinds of innovations that government can get in a timely manner. Certainly the spectrum of sensitivity or classification or criticality of a mission needs to be taken into consideration as well, where do they need the most critical, the most secure solutions and where might they be able to leverage a global marketplace better. So that discussion and consultation is necessary for that.

Mr. CARNAHAN. Let me just wrap up with the last question. There was a recent article in the *New York Times* entitled *"Contractors Vie for Plum Work Hacking for the U.S."* that focused in part on the growing demand for cyber warriors. How can the government and our educational system ensure that we meet the demands for these, not only meet the demand but also win the cyber security race and stay ahead of the curve here?

Dr. D'AMICO. I recall that article, and there are a few things about it. One is that they mentioned that there are very few people who have the security clearances that are needed to engage in some of that work. We need to have more U.S. citizens who get advanced degrees in computer science, engineering and the interdisciplinary areas that are related to computer security. The second thing is that a lot of those people came out of the military. One of the reasons they came out of the military is because of something that I alluded to before, that if you are a techie in the military, you don't get an advancement. We really need to have in the military a way of rewarding those people who are cyber defenders, cyber warriors, and then you will grow them in the military, and then when they retire they will be there to help in those areas that were mentioned in the *New York Times* article.

Mr. CARNAHAN. Mr. Brown.

Mr. BROWN. Yeah, I think one of the other things—so education is definitely important. Educating people—you know, a lot of our workforce is coming out of universities with education on secure coding capabilities but not really secure systems. Understanding how to design systems in a secure fashion is actually a lot more difficult than understanding how to code securely. A lot of the threats that we see are really more systems threats. You know, you are using fine software throughout your system but, you know, it has got a weak password rule or those types of things are in place. So making sure that we have people that understand those and are coming up through the ranks of our universities that understand how to design secure systems. Now, we do have—you know, we have been producing more of those professionals in the last few years but it is still just a growing field so we need to do more. It is also important that we institute strong internship programs, strong programs that link them with industry, link them with gov-

ernment because the university environment only gives so much focus to the real world essentially. So a lot of our work with universities today, we fund university research, but when we see the researchers come in, a lot of those researchers, we are teaching them about the real world and trying to give them enough knowledge to have impact in other places.

Mr. CARNAHAN. Thank you all very much.

Chairman LIPINSKI. Thank you, Mr. Carnahan. Mr. Neugebauer had a follow-up question so the Chair recognizes Mr. Neugebauer.

Mr. NEUGEBAUER. Well, thank you. I was just going to go back to our conversation that Dr. Goodman was talking about in the cell phone area, and we talked about the devices necessarily may not be equipped to process some of the threats, but I guess the question is, what is the industry doing I guess out there to make sure that, you know, their systems have integrity because obviously a lot of people, it is big business so other panel members, if you have some knowledge on that, I think it would be helpful for us as well.

Dr. GOODMAN. I will let Fred also respond, but from where I sit, I don't see—and it is big business. I mean, it is big business worldwide, not just the providers of the service but the makers of the devices and so on and so forth. So far I don't see much. I would also like to say something hopefully encouraging in that we are at the beginning of what I perceive to be a very rapidly rising curve in this domain. We have a certain amount of history with mistakes and not getting ahead of the game with regard to the Internet and all sorts of other security areas. Right now most of the users of cell phones, most of that 3.5, probably four billion people in the world now are using fairly weak devices that limit the kind of risk they are taking. That is going to be changing rapidly. Can we all of us, industry, government, governments around the world actually for once get ahead of the curve on this and do something to mitigate these risks before it becomes the kind of tsunami that I am afraid is going to become?

Mr. NEUGEBAUER. Mr. Brown? I thought you——

Mr. BROWN. Yes. Thank you. So when we look at—you know, I agree. In some cases we are in infancy in the cell phone/PDA world. We have opportunity to do a lot better in this world than we have in the laptop/desktop world. The threats are going to be different here though as we open up new interfaces and new capabilities to these phones. You know, Apple first put out their iPhone and they said a browser will be your only interface. That was easy to secure. But guess what? Consumers demanded that I have an application for everything, as the Apple commercial says, and each one of those applications now has increasing functionality. Each one of those applications has potential vulnerabilities. You know, we have—they have done a better job at securing things but there are more vulnerabilities, more opportunities to either socially engineer threats, which is actually probably more of a threat than software engineering of a threat. So we are at the point where we can do more and not have the same problems that we had sort of in the desktop/laptop world.

Mr. NEUGEBAUER. Dr. Schneider.

Dr. SCHNEIDER. Let me point out a few technical differences between the cell phone world and the desktop world and the way

they are evolving that might give you some reason to sleep at night. First, there is no dominant producer of the operating system for cell phones. There are a fair number of producers. That means there is not a monoculture so it is difficult for a single attack to attack all the processors. Second, early in the evolution of cell phones, the phone companies established a model that they owned the software and that they would periodically change your software without telling you when they decided to make a change in feature or fix a bug. So the model that we have for desktop software where Microsoft announces a bunch of patches for some vulnerabilities, notice they didn't announce that they were successfully attacked. They were preempting that. But the model where it is the user's responsibility to configure the system and it is the user's responsibility to keep it up to date has been abandoned and at least for the basic operating system of the cell phone, this is under the control of the manufacturer. There is a possibility now that everyone is going to be able to download their own applications and they will be responsible for that piece of the picture. That will be a problem. But if the cell phone manufacturers retain the view that they manage your security, then we might be better off.

Mr. NEUGEBAUER. Thank you, Mr. Chairman.

Chairman LIPINSKI. Thank you. We keep pushing back. I am looking at the TV screen here to see about when we are going to vote. I don't want to get into—we don't have much time so I just want to very briefly get into—throw out one more question. I was looking through my notes that I had made so I will recognize myself for five minutes but hopefully we can keep it to shorter than that. Dr. D'Amico talked about need to incentivize technology transfer and Dr. Schneider also talked about needing to bridge the gap between the research and policy. How do we do this? And this is always an issue that is facing so many different areas in technology transfer. It is something I am very interested in because I think it is very critical, getting that research, especially from our universities and getting them together with industry. How do we do that in this instance? So Dr. D'Amico?

Dr. D'AMICO. We really need to make the government program managers who are monitoring this federally funded research accountable for the technology transition and make the researchers incentivized to do it. First of all, the programs that are funded should include a technology transition phase and not stop at well, you have built a prototype, you have demonstrated in a laboratory and now we are done and we write the paper. It really has to go through usability testing and operational environment, and the money has to be there to do it. The second thing, and this is something I raised in my oral testimony, is that I think that the researchers need to go out to the security professionals who are ultimately going to be using the results of their work. So much of research is really—so many researchers brief themselves or their community. They publish papers within their community and they never really go out and talk to the security practitioners, and we need to have the results of the research brought out to those security practitioners, write an article for information security, see if you can turn your research into something that makes sense to the

practitioners, and it may change the way you do your research. So those are two of the ideas that I have.

Chairman LIPINSKI. Thank you.

Dr. Schneider.

Dr. SCHNEIDER. Let me comment on two things. First, so I am one of those researchers and I do get government grants. I run a fairly big operation. Today if you want to get a grant, you are much better off being able to assert in the grant application what your successful technology transitions were than to list publications. At least in many of the funding agencies, there is a culture that people who succeed in having a real impact are the ones they want to fund and publications don't matter so much. The other question has to do with teaching policy and technology. I think academia may be a bit ahead of the curve here but when I read places asserting we need to teach all our students the list of common security holes and secure coding practices and the next step is to teach them how to do secure designs, I think we need to teach them ethics, I think we need to teach them law, because if they don't understand these things, they are not going to know when they can trade off between a technological solution and a policy solution. If they don't have a good sense of ethics and sociology, then they won't understand how when they change the Internet so it is more secure, the fact that it became less usable makes it a less attractive place for all of its users and it gets ruined in another way, and so I think it is the responsibility of universities and any educator to have a much broader view than this kind of technology, and we shouldn't get railroaded into believing that we should produce technologists to solve this problem because they will come up with solutions but they are not going to be good solutions in the big picture.

Chairman LIPINSKI. Thank you.

Mr. Brown.

Mr. BROWN. Just one quick comment. When you talk about moving from research into products and applications, we have to understand that some of that takes a long time. You know, even if I come up with the greatest idea today within my company, within my position, I am a year and a half out before that idea gets into a product because we are mid-cycle in products, we are going to take that time. So patience and diligence, diligence and follow-through is critical to get anything done. So we have great ideas, we have great research. They take time to get implemented in products and they take time for people to implement them in the commercial sector or in the government sector. So we need to have processes in place that are going to attract those that research that we are doing through its life cycle and not give up on it after a year or two years.

Chairman LIPINSKI. Thank you.

You have to be very brief, Dr. Goodman.

Dr. GOODMAN. Very brief, I guess. There is another side to this. The implication in a lot of what has just been said is that somehow the innovators, the people who do the research need to push what they have done into the real world, and perhaps by offering things get policy changed or what have you. There is the other side of things, and that is that people who are going to be the primary consumers of better security, whether they are trying to manifest

this through policy or through what they think will really help their products, their commercial activities be more secure, they have got to send serious signals that there is a demand for certain kinds of research to solve certain kinds of problems, and that demand I think will filter into the research community and with funding they will get results. It is a two-way street to get things from ideas into useful practice.

Chairman LIPINSKI. Thank you, and I want to thank all of our witnesses for your testimony today. I certainly have learned a tremendous amount, and as we move forward right now, we have, as I said, two more hearings on cyber security. As we move forward with legislation in this area, we are certainly going to take a lot of what you have said and any more follow-up that you may have for us, we would appreciate. The record will remain open for two weeks for additional statements from Members and for answers to any follow-up questions the committee may ask of the witnesses.

So again, I thank the witnesses for their testimony. I thank the Members for their participation, and the witnesses are excused and the hearing is now adjourned.

[Whereupon, at 11:42 a.m., the Subcommittee was adjourned.]

Appendix:

Answers to Post-Hearing Questions

ANSWERS TO POST-HEARING QUESTIONS

Responses by Seymour E. Goodman, Professor of International Affairs and Computing; Co-Director, Georgia Tech Information Security Center, Georgia Institute of Technology

Questions submitted by Chairman Daniel Lipinski

Q1. The Administration's Cyberspace Policy Review calls for the development of an R&D framework that focuses on game-changing technologies, but at the same time new threats that need immediate attention are constantly emerging. What is the appropriate balance between long-term, game changing research and research targeted toward incremental improvement?

A1. It is easy to wish for R&D leading to "game changing technologies." But it is much harder to identify promising ways to go, and to see them through to widespread and effective adoption, a necessary condition if any game is really going to change. Identifying good candidate possibilities must be done by exercising bold expert assessments of the possibilities, with an appreciation of what successful pursuit of those R&D possibilities might mean for effective and comprehensive cyber security. There will not be many such proposals, but funding should be available to pursue the most promising to stages where they may prove their viability as serious game changing candidates.

To that end, what might "game changing" technologies actually do? The National Research Council committee and report that I recently chaired (*Toward a Safer and More Secure Cyberspace,* National Academies Press, 2007) proposed a Cybersecurity Bill of Rights that consisted of "10 basic provisions that the committee believes users should have as reasonable expectations for their online safety and security." I suggest that new technologies, and policies for their implementation, leading to demonstrable progress towards making a significant part of this vision a reality would constitute game changers.

There is also a pressing need for effective and timely work on extremely important emerging problems. A prime example that I raised in my oral testimony is comprehensive security for mobile devices, especially cellular phones, with an eye toward getting ahead of the problem and "getting security right," or at least much better than is now the case, as they become more powerful computing devices that will be truly ubiquitous, including the likelihood that they will become the primary vehicle everywhere in the world for access to the Internet. Another may be "cloud computing." Both have the promise for creating massive new waves of cyber insecurity unless we can get ahead of the technology and diffusion curves. Some people might consider successful work on these problems as "game changing" since they are so important, rapidly emerging, and would affect very large user communities. Certainly this would amount to much more than "incremental improvement."

I believe an appropriate balance should be weighted towards problems like these, with no more than about 20 percent devoted to finding grander and more comprehensive "game changing" solutions, and no more than about 20 percent devoted to incremental improvement. I believe most of the latter should be done by industry, including funding third party research and development people. If promising directions towards "game changers" are clearly demonstrated, the funding agencies should have the flexibility to redirect resources toward their aggressive pursuit.

As stated in my oral testimony, I believe a fundamental issue for both the near and long terms is effectively assigning responsibility for exploiting the results of R&D and implementing security in the real world of cyberspace. Right now this doesn't exist to anywhere near the extent it should. People and organizations who are most at risk of being victims are among the least capable of defending themselves and doing what needs to be done to protect what might be called the "cyber commons." Analogies can be made with the histories of safety and security in other infrastructures, e.g., with seat belts, shatter proof windshields, air bags, traffic laws and police and courts (but we must be careful of trying to make such analogies too close). One might argue that responsibility needs to be with those who are in the best position to make cyberspace significantly more secure. I would argue that resolving this problem is both researchable—although not in the narrow computer science sense, and will require thinking about incentives, regulation and law, economics, the makeup of the IT industry, and technical feasibility—and a necessary precursor for any effective "game changer."

Q2. Beyond the Scholarship for Service program, discussed in your testimony, do you have any specific recommendations for existing federal agency programs that should be expanded or new programs that might be created to address cyber se-

curity education needs? Is there a specific level of education that is in need of increased attention?

A2. Two opposite ends of the education spectrum need much increased attention: the general user community and graduate level education. The first addresses people who are most vulnerable, and most defenseless against increasingly sophisticated threats. They need to understand more about the risks they are subject to in cyberspace and what they can do to decrease their vulnerabilities. My response to Rep. Hall's fourth question below addresses two important age brackets of the general user community. My comments here are mostly concerned with the second, the post-graduate degree granting institutions.

People with graduate education are needed to professionally protect organizations, the "cyber commons," and parts of the relatively defenseless general user community. People with graduate education will be necessary to do most of the research, development, and the deployment of better technology and policies, and become the teachers of others. Presently, there are far too few to meet these needs.

Currently I would estimate that there are fewer than 50 universities each capable of graduating even a small, steady stream of graduate level professionals in information security. For example, Georgia Tech has one of the largest and most substantial programs, sustained by an unusual number of faculty members seriously concerned with cyber security, but we graduate only about 30–40 new MS and Ph.D. people a year in this area. And, again, we are one of the largest.

It is not easy to create more, as partially evidenced by the fact that the capacity building track of the SFS program has not worked out particularly well. And it is not easy to build up those schools that exist, e.g., because of internal competition from other areas for faculty hiring and coverage, and enrollment problems in computer science departments where most of this capacity resides. There is much less in information systems departments that are typically part of business or public policy schools, and efforts must be made to get cyber security into their programs. A necessary condition for doing better is to build up the number of Ph.D. level faculty members, and this takes time. One possible way of trying to deal with this might be to expand the SFS program to include more Ph.D. students, and to permit them to satisfy their immediate service obligations through teaching and program development in a range of K–12 and post-secondary educational institutions, including universities and community colleges.

Questions submitted by Representative Ralph M. Hall

Q1. Some experts have suggested that we should consider taking critical infrastructure networks such as those that control electricity transmission and distribution "off the grid"—into a network physically not connected to the public Internet, just as we do with our classified military networks. Please comment on whether you think such an approach warrants further consideration, and if so what potential benefits as well as challenges would accompany it.

A1. If much of the risk to these networks arises through connectivity to the public Internet, then that risk must be mitigated. Until this is effectively done in ways that permit safe forms of connectivity, it might be best to keep at least some of them disconnected, although connectivity has become such that this may be harder to do than it sounds. In the discussions about balancing the risks of insecurity against other factors, e.g., profitability, efficiency, or convenience, security usually seems to come up short.

But at least for the electric power distribution industry and infrastructure, the regulator (the Federal Energy Regulatory Commission) seems to be trying to step up to the problem. For a discussion of this effort, and much more, I refer you to a recent paper by one of my colleagues at Georgia Tech: Stephen J. Lukasik, "Reducing Threats to Users of the Global Cyber Commons," Center for Strategy, Technology, and Policy, Georgia Institute of Technology, Atlanta, GA 2009. A copy of this paper has been left with the Committee staff.

The positions that Dr. Lukasik has held over the years include Deputy Director and then Director of ARPA (now DARPA) when the ARPANET was being conceived and first implemented, and the first Chief Scientist of the Federal Communications Commission. In the spirit of this question, and given the precarious state of cyber security more generally, Dr. Lukasik suggests, "users should seriously revisit the premise that any two things are better connected than left unconnected." I would endorse that cautionary statement.

Q2. The comprehensive cyber security initiative that was created by President Bush and is continuing under President Obama focused on improving cyber security

coordination across government and on funding, game-changing "leap-ahead" technologies. Do you agree with these priorities? If you had an additional $100 million to spend on cyber security R&D, to what agencies and research areas would you devote it? Is there general agreement within the scientific community regarding security research priorities?

A2. Our 2007 NRC report, referenced in my response to Rep. Lipinski's first question, advocated a broad, defense in depth approach covering a number of important and complementary technologies. As also discussed in my response to that question, some effort to identify and develop game changing, "leap-ahead" technologies should be pursued, but the problems of cyber security are so extensive and complex that such silver bullets may be hard to come by at best, and are unlikely to come quickly.

Some areas, like improving methodologies for designing and engineering or re-engineering of more fundamentally secure systems and applications, would underlie almost anything else that would be done. So would research into architectures that would be fundamentally more secure than what we now have. I believe there is fairly general agreement within the scientific community on these points, but less so on many others. Again, I would place a large fraction on any new funding on dealing with the security problems associated with very large and rapidly emerging new technologies, notably mobile phones and other devices, and cloud computing, and also on research that looks into the problems of the timely, effective, and widespread implementation of new security policies and technologies. Many of the latter problems are at least as much matters of management, organization, and incentives as they are matters of technology. The problem of effective, widespread adoption is so enormous and complex that it might well negate good new technology if it is not given serious attention.

There are many agencies under the NITRD umbrella. I would hope that some of them would see these problems as particularly relevant to their mission statements and eagerly step up to producing solutions.

Q3. The strategy of both the past and current administration has focused most of our cyber security investment several billion dollars annually—on procuring and deploying intrusion detection systems. Due to the cat-and-mouse nature of cyber warfare and defense that several of you noted in your testimony, it seems that these systems are only effective against threats that we already know about and understand. Given this reality, can this type of approach produce effective results over the medium- or even short-term? If not, is research on a new and fundamentally secure Internet architecture the only long-term answer?

A3. Given the attention and investment over a long period in R&D for intrusion detection systems (IDS), I would suggest that it is time for a serious assessment of its impact. This would provide a far better and more constructive answer than what I might offer in this short response. I believe that most R&D in cyber security should be done as if application matters. In keeping with that, we must learn to do serious evaluations of progress towards a safer and more secure cyberspace, and IDS is a good place to start.

Are we able to detect almost all intrusions into almost all of our computers? Are we doing anything that is effective against emerging threats? If so, what combination of technical R&D and deployment incentives and strategies made this possible? What has this gotten us in terms of safer and more secure computers? Have we been able to thwart the intents and limit the damage done by these intrusions? Are we really limited to those threats that we failed to anticipate and prevent and ultimately learned about the hard way?

If not, then we need to understand why not before we pour billions of dollars and other resources more into IDS or something else. With most of the well-educated professionals among the good guys, why can we not pre-empt new forms of intrusions as they are happening or before they happen? Do we have good technical solutions that are not being implemented? Is the technology just not up to it, or are our systems so fundamentally insecure and there are so many threat possibilities that we should not have unrealistic expectations here, or is part of the problem apathy or resistance on the parts of the people and organizations in the best positions to implement and sustain these solutions? If the latter is the case, what can change this?

Note that intrusion detection is largely a matter of computer security. A "new and fundamentally secure Internet architecture" is more about network security and some different kinds of forensics, although it might have some positive effect on computer security. It may well be the necessary and best long term answer. There is no doubt that we could do better producing a more secure architecture today than was originally the case, but "fundamentally secure" is a very tall order, especially

if it also is to be effective in protecting us from insecure applications that could be put on the net. And ultimately there is the massive and very difficult problem of the huge legacy Internet to be abandoned or moved to the new architecture. In this regard, we have not always been very successful on much smaller scales.

Q4. When this committee discusses a STEM education issue, we don't just focus on higher education: We start at the pre-K levels and extend beyond post-graduate work. Most of the education-related testimony has focused on our adult population either from an academic and workforce perspective, a behavioral perspective, or a public awareness perspective. What are your education recommendations for our children when it comes to cyber security in all of these areas?

A4. Children and young people in the age range usually associated with primary and high schools, roughly ages 5–18, are a particularly vulnerable and important category of general user. In the United States, beyond the first few grades as a group they are probably coming increasingly close to being almost 100 percent users of the Internet or mobile phones and other devices. And the Internet has become part of many programs in K–12 educational institutions in this country, even if just as an augmentation to or substitute for traditional hard copy libraries.

It is important to include the concept of "safety" in addition to the common usages of "security" in discussing this age group. Some undesirable Internet enabled activities specifically involving children and teenagers range from the unauthorized use of credit cards (to paraphrase a classic New Yorker cartoon: "on the Internet, nobody knows if you are a child"), to massive violations of the intellectual property of others, to risking their own privacy on an unprecedented scale, to hacking for sport, bragging rights, and profit, to enabling a huge worldwide child pornography underworld, to providing unprecedented entries for people who physically or mentally prey on children. Furthermore, the naive or undereducated or malicious use of the Internet by children and teenagers may put others at risk.

But this is an age group that is almost totally accessible through their schools. Education covering the safe, secure, and ethical use of cyberspace is thus arguably a necessary and desirable addition to the curriculum in the primary and secondary schools. More generally, I would reflect a view expressed in the Association for Computing Machinery (ACM), the oldest and one of the largest professional associations devoted to computing, that we should look for ways to integrate grade-appropriate cyber security curriculum into existing courses, but we also need to expand the teaching of core computing concepts at the K–12 level. Computer science education is too often missing from the K–12 education landscape. As computing becomes ubiquitous through platforms such as hand-held or cellular devices and its role grows in society, it is imperative that students have a better grasp of the fundamentals of computing. We can do this by making a rigorous and engaging computing education part of the core that students must know and by making safe, secure, and ethical use a central part of this education.

If a narrower focus is desired, many precedents exist for helping K–12 students to cope with some of the problems in the real world, for example, for hygiene, nutrition, driver and sex education. But it will be more difficult to deal with this subject since the risks are more abstract and usually not physically proximate. And the problems are much more dynamic and rapidly changing.

We also have much to do with regard to educating the educators, i.e., developing capable teachers and the materials for them to use. This is not likely to be done well on a purely voluntary or local basis. In some ways and locales it is likely to be controversial, and care must be taken to get together material that is sensible, interesting, well presented, and does not needlessly scare the wits out of children (or senior citizens, see below). As stated above, the subject might be treated as a separate course, or distributed throughout the computer-using curriculum. It would also need to be reinforced in other public domains such as libraries and Internet cafes. This is a difficult assignment that must be given to the Department of Education, with start-up help from the NSF. Other professional organizations could also be constructively involved. These might include the ACM, the IEEE Computer Society, the Computer Science Teachers Association, the International Society for Technology in Education, and some industry associations.

I have one final concern at the opposite end of the spectrum, with an adult age group that usually does not figure into the academic or workforce discussions noted in the statement of this question. A sizable and growing fraction of senior citizens are users of the Internet, having been coerced and cajoled into doing so for what are often good reasons. But many do not take to computing as easily and "naturally" as young people. I believe that seniors are particularly vulnerable to exploitation and accident, and to fraud in particular. Some thought and effort should be given to help them. The institutional means of broadly educating this group is much less

obvious and more diversified than is the case for children and teenagers. But there are a large number of vehicles for "lifelong learning" in the United States, and safe computing and computing more generally should be made a much larger part of their curricula than is now the case. Again the professional associations, and the AARP in this case, might be constructively engaged in dealing with this problem.

ANSWERS TO POST-HEARING QUESTIONS

Responses by Liesyl I. Franz, Vice President, Information Security and Global Public Policy, TechAmerica

Questions submitted by Representative Ralph M. Hall

Q1. Some experts have suggested that we should consider taking critical infrastructure networks such as those that control electricity transmission and distribution "off the grid"—onto a network physically not connected to the public Internet, just as we do with our classified military networks. Please comment on whether you think such an approach warrants further consideration, and if so what potential benefits as well as challenges would accompany it.

A1. There would be considerable impacts on the usability and innovation derived from critical infrastructure networks should they be "taken off the grid" and put onto a classified-like proprietary network. In fact, in many cases such separation would be incompatible with the vision for improved, data-driven efficiencies that motivates "smart grids." With regard to electricity transmission specifically, TechAmerica member companies cite such examples of pooling and analysis of real-time, end-devise power-consumption data that enables more efficient electricity generation and transmission. In addition, we caution against policies that would adversely impact innovation in home networks or consumer products, either in inhibiting the very innovation that helps drive our economic growth or in establishing one-size-fits-all cyber security requirements that stifle functionality and, in many cases, may not deliver greater security.

With regard to this question, specifically, I highlight two key principles: (1) Cyber security is not a one-size-fits-all endeavor, and no one solution will meet all the needs of any given client. Therefore it is imperative that government, industry, and even individual network owners and operators undertake a risk management approach to the security of their operations. (2) As manufacturers and users of innovative technological solutions consider ways to ensure inter-operability and security measures, they should engage in appropriate, and global, standards development organizations in order to meet the specific needs of each product or service and involve all stakeholders.

Q2. The comprehensive cyber security initiative that was created by President Bush and is continuing under President Obama focused on improving cyber security coordination across government and on funding game-changing "leap-ahead" technologies. Do you agree with these priorities? If you had an additional $100 million to spend on cyber security R&D, to what agencies and research areas would you devote it? Is there general agreement within the scientific community regarding security research priorities?

A2. The IT industry does support efforts to improve cyber security coordination across government and on funding for the development of "leap ahead" technologies. As such we support the intent of the R&D efforts that are part of the Comprehensive National Cyber Security Initiative (CNCI). However, we believe those efforts can only be successful if they incorporate consultation and coordination with industry and the science community on identifying priorities. The IT sector is undertaking efforts now to engage the U.S. Government and provide suggestions and exchange information on R&D programs. The primary goal of these efforts is to ensure support for allocation of funds for projects that do not duplicate existing or ongoing work and help the government identify areas for research funding that lack a viable commercial market opportunity or incentives.

Implicit behind the premise of "leap ahead" research is the idea that there may be problems too intractable to be addressed in a timely fashion through incremental research. At times, useful discoveries may occur from unanticipated multi- or cross-disciplinary investigations. The creation of public/private partnership models to support revolutionary (as opposed to evolutionary) research is an important part of a balanced national strategy for cyber security research and development.

Another important part of balanced approach to R&D is ensuring that the benefits of that research are made available to others. Such technology transfer is the ultimate goal of industrial research programs that bring the effect of research successes to the market and to product users. To the extent that government can streamline the environment for technology transfer the greater the benefit.

With regard to research areas where additional funding could be applied, we highlight two that have been part of recent discussions, including the recent Nation Cyber Leap Year Summit. First, given new challenges to IT management as systems

become more automatically adaptable or self-modifying in order to resist attacks, we may benefit from research into the management of adaptive systems. Second, research into cyber security metrics is another area where there is significant opportunity for progress.

Lastly, whichever agency or agencies receive funding for such research and development efforts, we strongly urge requirements for coordination and collaboration with other agencies and with the private sector and the academic community.

Q3. The strategy of both the past and current administration has focused most of our cyber security investment—several billion dollars annually—on procuring and deploying intrusion detection system. Due to the cat-and-mouse nature of cyber warfare and defense that several of you noted in your testimony, it seems that these systems are only effective against threats that we already know about and understand. Given this reality, can this type of approaches produce effective results over the medium- or even short-term? If not, is research on a new and fundamentally secure Internet architecture the only long-term answer?

A3. It is precisely the dynamic and evolving threat environment that calls for taking a risk management and all-hazards approach to protecting ourselves from cyber attacks, to include not only technology, but people and processes as well. Certain technologies will address specific kinds of attacks, while a more sophisticated enterprise architecture will help defend against various kinds of intrusions. Each enterprise—or individual—needs to assess their specific usage, system, and security needs and make their investments accordingly. While R&D on a new Internet architecture may be something to consider, such an approach must be evaluated with all the stakeholders at the table to ensure a thorough vetting of the objectives, potential solutions, and intended and possibly unintended consequences. In the meantime, however, we must continue to invest in key cyber security R&D for both short and medium term innovative solutions to today's challenges.

Q4. When this committee discusses a STEM education issue, we don't just focus on higher education. We start at the pre-K levels and extend beyond post-graduate work. Most of the education-related testimony has focused on our adult population either from an academic and workforce perspective, a behavioral perspective, or a public awareness perspective. What are your education recommendations for our children when it comes to cyber security in all of these areas?

A4. At the most rudimentary level, we should be including ways to sensitize our children to cyber security considerations when they are learning how to use a computer and the Internet, something which is occurring at very young ages today. We can take advantage of that early learning to infuse good user practices that address safety (what information you put on the Internet about yourself), security (if you are learning how to download any number of "fun" applications, you can also download anti-virus software and encrypt your wireless connection), and ethics (consequences of cyber bullying or cyber fraud). Building such elements into the K–12 curriculum must recognize the dynamic nature of the cyber medium and the threats it faces and, therefore, be set up in a way that is flexible to be updated as necessary, and to provide resources for educators and students about where they can go to get the most up-to-date information. One good source for such information is *www.staysafeonline.org,* which is run by the National Cyber Security Alliance (NCSA), a non-profit public-private partnership to build cyber security awareness with all user groups.

At a more strategic level, we can be developing curriculum that lays the foundation for a workforce that is capable of designing secure systems. Congress could call for a short-term task force that engages industry, academia, the Department of Education, the Department of Homeland Security, and the Department of Commerce's National Institute for Science and Technology (NIST) to make recommendations for establishing such a foundation, evaluating and building upon any existing efforts and/or developing new ones.

Q5. Ms. Franz, in your testimony you call for a "true government-industry collaboration on research projects." Please elaborate on this recommendation. How would it be structured, and how would research priorities be identified? What agency or agencies do you think should fund such an effort?

A5. In my testimony, I wanted to emphasize the need for collaboration among government-industry partners on equal footing. Such equal footing could be achieved a number of ways, including through a structure that ensures engagement with government and industry representatives at the very beginning of any evaluation and prioritization process. In addition, a governance structure could ensure that each partner has equally weighted "votes" in the deliberation process. Too often one part-

ner works on a process alone for so long that once the other partner is brought into the process, it is too late for a fully deliberated discussion and prioritization. Finally, true collaboration would include commensurate stakes and investment by each partner. For example, should the government fund an effort, industry could provide expertise that meets the need—and the stated level of partnership. Such "true" collaboration would require a change in how government and industry each approach the R&D discussion today and bring them together at the beginning of the partnership process—even in how that process is conceived.

For funding a cyber security R&D collaborative effort, I believe any number of agencies could—and should be involved to maximize not only the funding sources but also the expertise from various constituencies and bring them—and their industry stakeholders—together for such a project.

ANSWERS TO POST-HEARING QUESTIONS

Responses by Anita D'Amico, Director, Secure Decisions Division, Applied Visions, Inc.

Questions submitted by Chairman Daniel Lipinski

Q1. In your written testimony you indicate that good security decisions are based on an understanding of risk. How is cyber security risk assessed and are the current methods or tools adequate? If current measures of cyber security are not adequate, what research is needed to improve cyber security risk assessment?

A1. The methods and tools for measuring cyber security risk are not adequate. There is an excellent May 2009 publication entitled "Measuring Cyber Security and Information Assurance" by the Information Assurance Technology Analysis Center (IATAC) which is available through the Defense Technical Information Center. It summarizes the state-of-the-art of measuring cyber security, which is a prerequisite to understanding and measuring the actual risk associated with the security state, and describes several measurement approaches. It concludes: "there are no universally recognized, reliable, and scalable methods to measure the security of [IT] assets."

Even if the risk measurement tools and methods were scalable and reliable, their value for enhancing security state would be minimized without commitment by the decision-makers to consistently use the tools and methods. However, business managers have not yet committed to regular measurement and mitigation of the discovered risks. What will it take for risk measures to be embraced by corporate and military officers?

- **Answer the "Risk to what?" question—**The broad usage of security risk measurement is more likely to occur if the industry managers and military commanders understand the impact of these risks to their specific mission, whether that mission is to build a greater revenue stream or protect Afghani citizens from terrorists. Risks must be put into the context of the goals of the organization and the individual investing in the risk measurement. *A ripe research area is to identify methods for automatically linking the availability, confidentiality and integrity of IT assets to the specific business processes or mission tasks that the organization or individual must perform.*
- **Establish the credibility of the risk measures—**As with any metric, it must be grounded in systematic observation of lots of data. The data on which the metric is based must be recognized as meaningful to the ultimate users of the metrics.
- **Make it easy to collect—**Automated tools for collecting relevant data from the network enterprise and calculating the risk measures would decrease resources needed to perform risk measurement. *Research and technology development is needed to determine the best methods for collecting and calculating risk measures in real-time.*
- **Make it easy to mitigate—**The IATAC report cites a need for research in *"self-healing" measures in which an automated response would be triggered when a threshold of risk metric is reached.* In addition to the automated mitigation approaches, *we need methods of presenting the outcome of risk measurement in intuitive and actionable form.*

Finally, most cyber security risk measurement is focused on wired networks, ignoring the ubiquity of wireless devices. Wireless access points, wireless cards within laptops, and smart phones can be exploited by attackers to penetrate critical wired networks. Even though wireless networks may be excluded by policy from many military and industry organizations, the mobile devices carried by the personnel hold high-value information which can be exploited by cyber criminals or foreign agents. *Future research in risk measurement must factor the wireless landscape into the calculation of risk.*

Questions submitted by Representative Ralph M. Hall

Q1. Some experts have suggested that we should consider taking critical infrastructure networks such as those that control electricity transmission and distribution "off the grid"—onto a network physically not connected to the public Internet, such as we do with our classified military networks. Please comment on whether

you think such an approach warrants further consideration, and if so what potential benefits as well as challenges would accompany it.

A1. I don't feel I have the background to respond to this question.

Q2. The comprehensive cyber security initiative that was created by President Bush and is continuing under President Obama focuses on improving cyber security coordination across government and on funding game-changing "leap-ahead" technologies. Do you agree with these priorities? If you had an additional $100 million to spend on cyber security R&D, to what agencies and research areas would you devote it? Is there general agreement within the scientific community regarding security research priorities?

A2. I thought the NITRD Cyber Leap Year call for leap-ahead technologies was an innovative approach to exciting the cyber security research community. They reviewed 238 responses, and produced five categories of technology that NITRD cited as critical areas for funding:

- Digital Provenance—basing trust decisions on verified assertions
- Moving-Target Defense—attacks only work once if at all
- Hardware-Enabled Trust—knowing when we've been had
- Health-Inspired Network Defense—move from forensics to real-time diagnosis
- Cyber Economics—crime doesn't pay

I concur that all of these are important areas for future funding. However, there are a few areas that I believe warrant government investment such as the $100 million to which you referred:

- **Cascading effects of an attack—**More work is needed in understanding the interdependencies within the cyber infrastructure, and between the cyber infrastructure and other critical infrastructures. Other work is needed to understand the dependencies of critical business operations on the IT infrastructure and how a cyber attack can cascade to affect several business operations within and across organizations.
- **Resiliency and recovery—**Attackers will get into our systems. The cascading effects of an attack will occur. How do we continue to work through and fight through the attack?
- **Information value—**The cascading effects of an attack, and recovery decisions, are based in part on the value of the information needed to maintain critical operations. However, we have little understanding of what makes information valuable to people and critical operations. If we knew how to measure the value of information, we would be able to apply security measures to follow the high-value information, even as it moves throughout a network.
- **Attack attribution and legal response—**Proving the source of an attack remains difficult. Research is needed on how to identify the attack source. Additional work on the legal aspects of cyber crime must determine the appropriate level of evidence needed for attack attribution, and the laws and policies that will permit the collection of that evidence.
- **Security of socially connected wireless devices—**The steady rise of social networking, much of it performed with mobile devices, poses threats to our cyber infrastructure as well as potential opportunities for remediation. Research in this area is still in its early stages, and should be continued with greater investment.

A few minor criticisms of the Cyber Leap Year format for solicitation:

- There would have been more responses, particularly from some of the large industrial R&D organizations, if NITRD had made a provision for protecting proprietary approaches and proposing classified ideas. The companies with the biggest Internal R&D funding were unlikely to toss out their best ideas for anyone on the Internet to review.
- It is surprising that *none* of the 238 responses were deemed of sufficient merit to warrant a topic-specific workshop. The fact that no one got an invitation to a workshop based on the merit of their response is likely to negate future enthusiasm for such a program.

Regarding which agencies should receive the funding, I think the decision should be guided in large part by which agencies are most likely to transition the resulting technology into widespread operations, and are most likely to manage research that combines researchers from various communities, i.e., academia, industry, govern-

ment, classified and unclassified. I believe that the service laboratories (e.g., Army Research Laboratory, Air Force Research Laboratory, Naval Research Laboratory) and DHS Cyber Security R&D are in an excellent position to bring together academic, industry and government researchers. NSF is largely biased toward academic researchers. NSA requires clearances that many academicians don't have. The service laboratories and DHS–CSRD also have the mindset and contractual experience to handle classified and unclassified work and address contract terms relevant to both academia and industry.

Perhaps most important, the service laboratories are in a position to help transition the technology into military and homeland security programs.

Q3. The strategy of both the past and current administration has focused most of our cyber security investment—several billion dollars annually—on producing and deploying intrusion detection systems. Due to the cat-and-mouse nature of cyber warfare and defense that several of you noted in your testimony, it seems that these systems are only effective against threats that we already know about and understand. Given this reality, can this type of approach produce effective results over the medium, or even short, term? If not, is research on a new and fundamentally secure Internet architecture the only long-term answer?

A3. Intrusion detection systems, while not the ultimate solution, can be useful in the short term because they add a layer (albeit weak) of defense that thwarts script kiddies and other amateurs. They also creates a nuisance for more-sophisticated attackers, thereby increasing the amount of time and effort they must expend in order to penetrate our systems. However, intrusion detection systems do not warrant significant government research funding, as the commercial companies deploying them are incentivized by their sales to continue this work.

Government research does need to focus on the larger, game-changing issues in order to achieve real security. A new and fundamentally secure Internet architecture is an excellent long-term goal. However we must accept the fact that no system or architecture can achieve complete security without completely sacrificing openness. Therefore research needs to continue to focus on defensive techniques, but from the new perspectives discussed earlier—not from the perspective of just making better intrusion detection systems.

Q4. When this committee discusses a STEM education issue, we don't just focus on higher education. We start at the pre-K levels and extend beyond post-graduate work. Most of the education-related testimony has focused on our adult population either from an academic and workforce perspective, a behavior perspective, or a public awareness perspective. What are your education recommendations for our children when it comes to cyber security in all of these areas?

A4. Students need to acquire an understanding about computers and the Internet as basic elements of life in the digital age. Safe computing should be a basic element of our K–12 curriculum, like math and reading, not an elective. Organizations such as the National Cyber Security Alliance are already working to support safe computing education for K–12, but additional assistance and attention is needed.

Education of children is also the first step in a cultural shift towards a more secure digital world and away from the current view of digital information as a free-for-all. The ease with which information can be shared, copied, pirated, and distributed has created a sense in the current generation that the information itself has no real value. Teaching adults to fear the Internet and to be careful about downloading may achieve behavioral change to some degree, but does not affect cultural change.

The younger generation is the driving force in this cultural shift: they are the ones stealing music and movies, posting personal information on social networking sites, installing peer-to-peer software on their computers without concern for the security risks, and in general treating their digital lives with the same carelessness with which they clutter their rooms. They do this because they can, and because they have not been taught that this is all wrong. This fundamental lesson of respect for information—its financial value, its privacy implications, its intrinsic importance to their lives—must be ingrained in them from the earliest days. From this will flow a cultural shift away from the information-wants-to-be-free attitude of the early Internet days towards a more mature, and secure, digital world.

The building of a culture of safety, respect and ethics in the digital world should begin in early *elementary school* education. This should start with awareness training in elementary school for cyber safety and cyber security basics such as *safe browsing and e-mail, identity theft, and issues around social networking—think of it as hygiene lessons for the digital world—and should also instill the ethics of information.* Children need to learn that information has real value, and must be pro-

tected and respected just as much as physical treasure. Most well-raised American children wouldn't even consider walking into a Wal-Mart store and stealing a Nintendo game, yet millions of them think nothing of downloading music illegally from Lime Wire every day.

Cyber education should progress during the *middle school years to more advanced issues of cyber security and ethics such as data protection, data sensitivity, privacy, and digital copyright. Digital privacy issues should be emphasized in grades five through nine.* Current middle-schoolers, though conscious of their privacy needs at home, really have no sense of digital privacy—something that some adults unfortunately exploit. The kids cry "invasion of privacy" when Mom cleans their room and finds some sort of contraband under the bed, yet they think nothing of installing bitTorrent on their iMac and opening their files for the entire world to see. They cringe if you put their class photo on the refrigerator, yet they gleefully post photos of their latest binge on Facebook.

By the time students reach *high school,* they should be prepared to drive themselves in the digital world. The goals should be similar to those of driver education: *know how to operate the equipment, be knowledgeable of the laws and the repercussions of breaking them, and be able to travel without injury to yourself or others.* Those with even greater interest can learn how to build, take apart and speed up the information technology—always with safety in the forefront.

ANSWERS TO POST-HEARING QUESTIONS

Responses by Fred B. Schneider, Samuel B. Eckert Professor of Computer Science, Department of Computer Science, Cornell University

Questions submitted by Chairman Daniel Lipinski

Q1. In your written testimony you indicate that good security decisions are based on an understanding of risk. How is cyber security risk assessed and are the current methods and tools inadequate. If current measures of cyber security are not adequate, what research is needed to improve cyber security risk assessment?

A1. Risk is usually defined as an "expected value" (in the statistical sense) and, therefore, requires identifying all possible hazards and then estimating the cost and probability of each. Applying this definition to a computing system would require calculating or estimating these costs and probabilities (as well as identifying all hazards), and that is far beyond the state of the art. Moreover, historical data, which works so well for writing life, health, and property insurance policies does not help for doing a cyber security risk assessment: a system's internals (hence the system's vulnerabilities), where systems are being deployed (hence the consequences and cost of a successful attack), and attacker sophistication (hence the likelihood of an attacker's success) change too rapidly for the past to be a good predictor of the future.

Given these inherent difficulties in measuring the constituents of the "expected value" that defines cyber security risk, I believe we would be better off focusing our research investments on science and engineering that helps ascertain a system's compliance with given behavioral specification or properties. This is, in a sense, the flip side of cyber security risk, since risk involves the probability of a system's exhibiting behavior that departs from those specifications.

Examples of the kinds of research I am advocating can be found in (among others) the area of programming language design and the area of automated tools for analyzing program execution—for instance, research into rich type systems for programming languages and model checking for program verification. These technologies can help establish that a program's execution will exhibit certain properties and, as a side effect, enable tools to detect large classes of code vulnerabilities. We should also invest in research that aspires (i) to developing a principled way for extracting "trust assumptions" in systems and (ii) to understanding how various security technology relocates "trust assumptions" from one component to another, since this is a way to surface the risks in a system design.

Although this proposed research ignores the probabilities and costs of attacks, its fruit doesn't prevent individuals from using insights about threats, system internals, or the circumstances of a system's deployment when deciding how best to manage the risk of cyber attacks. Here, broadly disseminating information about attackers, successful attacks, and cost or consequences of attacks would be in everyone's best interest, because system operators and their users all could then evolve a better understanding of the risks they face and have a basis to make more intelligent decisions. Therefore, I advocate putting in place incentives for public reporting of successful attacks, attacker capabilities, and their consequences as another key step toward being able to assess cyber security risk.

Q2. One of the near-term action items of the Administration's Cyberspace Policy Review is to provide the research community with event data. What is the quality event data currently utilized by the research community and is it a realistic representation of network activity.

A2. Event data is today not broadly available to the research community. This means researchers do not have good data against which to evaluate solutions they develop nor do they have a way to gain the kind of first-hand experience that is often crucial for understanding the real problem and inventing solutions.

Today we find that to avoid undermining public trust, information about successful attacks is generally kept confidential. Information about vulnerabilities is generally not made public until after a defense has been widely deployed. And information about network traffic is not generally available from ISPs or from other network operators because it can reveal information about their cost and pricing models; it also can reveal users' private information.

Network traffic data sometimes is made available today to selected researchers if they agree not to further disclose that data nor disclose its attribution in publications that analyze the data. Such data cannot be shared with other researchers, making comparative analysis of work done in different labs impossible.

Various test-beds allow researchers to experiment "at scale" and sometimes it is possible to use those as a source of data. However, load (including attacks) in these testbeds is either generated artificially or (in the case of PlanetLab[1]) would depend on concurrently executing experiments (hence is difficult to reproduce). In short, today's testbeds are a poor substitute for experiments that use real, operational, datasets.

Recently, the Office if Science and Technology Policy invited the National Science Foundation to organize a group of NSF-supported computing researchers and provide a white paper detailing specific kinds networking and cyber security data that would be useful for the academic research community. Professor Nick Feamster (Georgia Tech) coordinated that effort, and a short white paper is now available.[2]

Q3. Do you have any specific recommendations for existing federal agency programs that should be expanded or new programs that might be created to address cyber security education needs? Is there a specific level of education that is in need of increased attention?

A3. I am aware of two federal programs in support of cyber security education:

- The Federal Cyber Service Scholarship for Service (SFS)
- National Centers of Academic Excellence in IA Education (CAEIAE)

I have no direct experience with SFS.

I have some experience with CAEIAE. This program certifies whether a college or university offers an educational program deemed by the National Security Agency (NSA) to provide a suitable background for working in information assurance. The criteria for CAEIAE designation include requirements about what is taught and about the qualifications of who does the teaching.

I decided not to pursue CAEIAE for Cornell because I did not find current thinking about cyber security well represented in the curriculum requirements for CAEIAE certification. And while the number of schools with CAEIAE certification is rather substantial, Cornell is hardly the only outsider. Only Carnegie Mellon University (CMU) of the five universities in the NSF funded TRUST Science and Technology Center pursued a CAEIAE certification, yet these five universities are among the very top cyber security programs in the country; also only two (CMU and University of Illinois) of the top five ranked Computer Science departments are listed on the CAEIAE web site as having CAEIAE certification. Recently, Purdue, which hosts the nationally known Center for Education and Research in Information Assurance (CERIAS), decided against renewing its CAEIAE certification. Professor Eugene Spafford, Director of CERIAS, contributed to creating the CAEIAE program in 1997; he details his reasons to now forgo CAEIAE certification in his on-line blog.[3]

The field is moving rapidly, and what we teach needs to keep pace with what is known and with the needs of all the stakeholder communities; CAEIAE doesn't. Moreover, the dividing line between what constitutes training and education is shifting, with various software producers now taking an active role in training their workforces about (for example) secure coding and avoiding common vulnerabilities. What gets taught in the university should reflect those realities and not waste time duplicating current industry-training efforts. Needless to say, one way that I believe the Federal Government can help move cyber security education forward is by not imposing constraints on content.

Second, our very best faculty, who typically are exploring new approaches to organizing and teaching cyber security, need incentives to spend that extra time and effort necessary for disseminating this work (just as the academic culture today provides incentives that prompts the dissemination of research results). So, for example, programs for funding cyber security education should endeavor to attract research-focused faculty at our Tier 1 institutions. And although funding is an important part of the picture, it is not the only part—it is crucially important that opportunities for peer recognition be present and that some means exist to surface evidence of national impact from a faculty member's efforts to further cyber security education.

I believe the greatest opportunities for having impact in cyber security education—and ultimately on the workforce—hence the place to focus increased atten-

---

[1] *http://www.planet-lab.org/*

[2] Jean Camp, Lorrie Cranor, Nick Feamster, Joan Feigenbaum, Stephanie Forrest, Dave Kotz, Wenke Lee, Patrick Lincoln, Vern Paxson, Mike Reiter, Ron Rivest, William Sanders, Stefan Savage, Sean Smith, Eugene Spafford, Sal Stolfo. Data for Cybersecurity Research: Process and "Wish List." June 10, 2009. Available at *http://www.cc.gatech.edu/~feamster/papers/data-wishlist.pdf*

[3] *http://www.cerias.purdue.edu/site/blog/post/centers_of_academic_adequacy/*

tion, is in creating a new cyber security professional degree, analogous to what we have today in law and medicine. The undergraduate major serves a broad set of needs and, as a result, offers few opportunities for adding new content. Moreover, there is simply not enough time for an undergraduate to get a broad education in Computer Science and also be exposed to all the material that a cyber security expert (or even an apprentice) should see. Graduate education, by contrast, allows the flexibility to require substantial course work in specialized areas.

Universities and students will not invest in a new degree unless there is some clear benefit. Requiring some sort of credential for cyber security professionals is often suggested, just as lawyers and doctors have their respective credentials. But if we are going to pursue this, then we should first understand the options (since, looking across the other professions, there are many possibilities) and be clear about the consequences. Therefore, I would argue that before mandating a credential, we first commission one or more objective bodies, such as the National Research Council's Computer Science and Telecommunications Board (CSTB) and/or the Government Accountability Office (GAO), to do a study that lays out the options. Inputs should be solicited from researchers, educators, systems builders, and systems operators (private sector and the government). And the study should:

1. Assess what (if any) benefits would come from imposing liability-based and/or regulation-based incentives for credentialing cyber security professionals. What would the costs be?
2. Identify practical structures for defining and evolving the content that a cyber security credential covers, and consider the various candidate examination instruments.

In parallel, we should make investments in community workshops, planning grants, and curriculum development, as a way both to understand whether a new cyber security professional degree is workable and to facilitate building a community consensus for such a new degree program. Yes, there is a crucial and immediate need for better-educated cyber security experts and what I am proposing will take some time. But a poorly thought-out credential and mandating the wrong content for our students is not going to improve matters (and might well set things back).

Questions submitted by Representative Ralph M. Hall

Q1. Some experts have suggested that we should consider taking critical infrastructure networks such as those that control electricity transmission and distribution "off the grid"—onto a network physically not connected to the public Internet, just as we do with our classified networks. Please comment on whether you think such an approach warrants further consideration, and if so what potential benefits as well as challenges would accompany it.

A1. Separating the networks used by critical infrastructures from the Internet could entail a significant opportunity cost, and it would be virtually impossible to enforce. I therefore think it would be unwise to pursue this approach.

The opportunity cost of separating the networks comes from the potential loss of services. First, certain Internet services could provide important benefits to critical infrastructures; isolating the networks would make those services unavailable to those critical infrastructures. Access to on-line weather predictions, for example, could be useful in automatically controlling electric-generation capacity, allowing new generators to spin-up in time to serve peak air-conditioning loads on a summer day. So-called network-guard technology could be deployed here and connect the networks, but this sacrifices the bullet-proof appeal of complete isolation. And the critical infrastructure's network could not be designed under the assumption that this network is completely isolated from the Internet, since attacks have been known to pass through guards.

Second, the Internet provides pervasive connectivity that would be quite costly to replicate. And there will be strong temptations to use that connectivity in making our critical infrastructures more convenient, more efficient, and more effective. For example, an engineer in charge of controlling a critical infrastructure might well prefer to make after-work unexpected adjustments from his home rather than trekking into the office at odd hours, and an Internet connection to that critical infrastructure could be used for that—quite securely, if VPN (virtual private network) technology is employed. And a smart grid might serve us better if homeowners could remotely control appliances, thermostats, or even the class of electric service being purchased to run the household at any time. But implementing this kind of

functionality would mean sacrificing isolation because there would be devices connected both to the Internet and to the network controlling a critical infrastructure.

Regarding the enforceability of a network-isolation mandate, it takes but one person connecting a single computer to both networks for the isolation to be destroyed. Likely this connection would be done as a matter of convenience and, judging from past experience reported for the public telephone network, the connection would be made by a low-level technician and without the consent or knowledge of management. Desktop machines running commercial operating systems are not known for their strong security guarantees, so we would be unwise to depend on the desktop's security to provide isolation between the networks when both are connected to the same machine.

Q2. The comprehensive cyber security initiative was created by President Bush and is continuing under President Obama focused on improving cyber security coordination across government and on funding game-changing "leap-ahead" technologies. Do you agree with these priorities? If you had an additional $100 million to spend on cyber security R&D, to what agencies and research areas would you devote it? Is there general agreement within the scientific community regarding security research priorities?

A2. I am not knowledgeable about the details of CNCI, because the initiative has been classified and, therefore, information about it has not been generally available to the academic research community. I nevertheless can offer high-level comments about what seem to be the key elements.

Better coordination of cyber-defense across government should be a national priority. A cyber-defense is only as good as its weakest link. So a coordinated defense, if overseen by a technically strong organization that has the power to compel federal agencies to deploy specific cyber-defensive measures, is likely to decrease the chances that any agency's computing system becomes such a "weak link." The existence of a central clearinghouse for information about attacks—on-going and past—also would be valuable for cyber-defense.

To deploy new cyber-defenses will require replacing and reconfiguring systems. I presume funding for these activities is a large part of the CNCI budget. We will want to be sure this money is spent wisely, and the absence of opportunities here for advice from the research community or from the private sector concerns me. Some government agencies are well served being advised by the intelligence community, with its strong track record of securing our nation's classified systems. But other agencies are more like the commercial organizations found in the private sector, with different needs and a different tolerance for risk. Such agencies might benefit more from advisors outside the intelligence community. Finally, I should report that the utility of various CNCI-proposed defenses has been questioned by cyber security experts in the private sector and in the research community (albeit, people who did not receive classified briefings and therefore have an incomplete understanding of the problem and solution). This questioning suggests that any kind of central coordination should be in conjunction with some sort of advisory board that is populated by cyber security experts (technical and policy) from the private sector and academia.

The CNCI emphasis on "game-changing 'leap-ahead' technologies" seems well intentioned, but we should be careful about exactly how this is interpreted. For sure, if we continue with business as usual then we will never get to the point of running networked information systems that are trustworthy. But, as noted in my testimony, the way to be proactive and have the greatest chances of revolutionary advances—what I presume is meant by "game-changing leap-ahead technology"—is to build a science base for trustworthiness. The science base must come first; an initiative that focuses on only the technologies would likely fail without a science base.

Second, the advances CNCI seeks are not going to come if we just concentrate on developing new technologies and educating the workforce. Economics and law play a significant role in determining what (if any) investments system builders and operators actually do make in support for system trustworthiness. If we as a nation are not prepared to make game-changing alterations to our values and policies, then business as usual will continue despite any game-changing technologies we might develop, because it is virtually certain that trustworthiness will be far from free.

Finally, I note that we might "leap-ahead" but our attackers will surely follow. Cyber security is not a game that can be won once and for all. We must win it each day anew. Let nobody believe that we only need one set of "game-changing 'leap-ahead' technologies."

How to spend an additional $100M on cyber security research? Page 6 of my testimony gave a list of research areas. This list was based on (i) a consensus view of academic cyber security researchers NSF brought together earlier this year to pro-

vide input[4] for Melissa Hathaway's White House 60-day Cyber-Policy review as well as (ii) a recent National Research Council study[5] on a cyber security research agenda; I was directly involved in both efforts.

NSF is the obvious agency to distribute additional cyber security research funding. Up to 200 additional researchers in cyber security could be funded at $500K per year, and I would argue that an individual researcher's funding needs to be at (or preferably above) that level if we can have hopes of supporting enough graduate students to make in-roads into the demand for additional faculty and private sector experts. But should all the money be sent to NSF? I have no basis for justifying a scheme to divide the funds among various funding agencies. For example, there is now a new DARPA director, with indications that she will return DARPA to its past role in funding cyber security research at universities. This would be a wonderful development, because DARPA-funded research has a very different character from the efforts that NSF supports; I have no idea whether this redirection of effort within DARPA would require additional funding. The Air Force, Army, and Navy also have (modest) cyber security research programs that fund faculty; these have yet a different character from the DARPA and NSF programs, and they likely would make good use of additional funds.

Q3. The strategy of both the past and current administration has focused most of our cyber security investment—several billion dollars annually—on procuring and deploying intrusion detection systems. Due to the cat-and-mouse nature of cyber warfare and defense that several of you noted in your testimony, it seems that these systems are only effective against threats that we already know about and understand. Given this reality, can this type of approach produce effective results over the medium- or even short-term? If not, is research on a new and fundamentally secure Internet architecture the only long-term answer.

A3. Despite the difficulty with intrusion detection that is noted in the question statement, this approach does have defensive value if relatively little time elapses between isolating the signature of a new attack and distributing that signature to intrusion detection subsystems on hosts that have not yet been attacked. Some recent research results will help put this into context. Simulations of the Internet done by cyber security researchers at U.C.–San Diego (and elsewhere) have shown that a worm could spread though the Internet so quickly that having a human involved anywhere in the path from signature-isolation to signature-distribution would introduce too much delay for intrusion detection to be effective. That suggests intrusion detection has limited value against attacks that propagate rapidly. But investigators at Microsoft Research designed and prototyped an automated system that can detect a successful worm attack, automatically generate filters and/or patches for that attack, and disseminate those defenses to other systems ahead of the worm. Thus, there are deployments that avoid direct human involvement on the critical path for defense.

Virus scanners can be seen as a special case of intrusion detection. And they have been quite effective at defending desktop systems against malware, which to date has tended to propagate through the Internet slowly. Even for malware that is not slowly propagating, downloading a new signature file for a virus detector is usually faster and less likely to destabilize a production system than patching the vulnerability being exploited by that malware. So updating a virus detector's signature file is often the fastest way to securely reconnect a system that had been vulnerable to Internet malware. However, new attacker technology, which obfuscates different copies of a given virus differently, can make it impossible to create the malware-signatures needed by today's virus scanners. Thus, virus scanners are likely to become less and less effective.

The design and deployment of a "fundamentally secure Internet architecture" would be important step towards improving the trustworthiness of our networked information systems. However, we should be clear about what it involves and what would be its consequences. It involves new research—various proposals for improved Internet architectures have been made, but there is much investigation and prototyping to be done before we might attempt to use these proposals as a basis for replacing the Internet. These investigations might take a decade or more.

And having a "fundamentally secure Internet architecture" would not mean the problem is solved. Today's networked information systems comprise end-systems

---

[4] Notes for White House 60-day Cyber-Policy Review. Available on WWW at *http://www.cs.cornell.edu/fbs/publications/SciPolicyNSFnotes.pdf*

[5] *Toward a Safer and More Secure Cyberspace.* S. Goodman and H. Lin (eds.), National Academies Press, Washington, DC, 2007. Available on WWW at *http://books.nap.edu/catalog.php?record_id=11925*

(desktops and servers) interconnected using the Internet. For example, the DNS service is part of the Internet architecture but services (like Google and Amazon) and desktops (running Windows and Linux) are end-systems. Virtually all attacks originate at the end-systems and most attacks are directed at the end-systems today because the compromise of end-systems offers value to attackers and these end-systems are low-hanging fruit. Thus, having an Internet that is "fundamentally secure" only solves part of the problem—to solve the entire problem, we must also have end-systems that are "fundamentally secure."

It does seem clear that designing a new, secure, Internet architecture is a crucial step towards supporting trustworthy networked information systems, and it seems equally clear that a new Internet architecture (notably, one that supports stronger notions of provenance and accountability) would be a key enabler for building "fundamentally secure" end-systems. Yet, leveraging accountability would also depend on making progress on policy matters. New privacy questions would be raised and need to be resolved; and international agreements about jurisdiction and extradition would need to be negotiated, since the premise of accountability is that attackers can be found and punished.

Q4. When this committee discusses a STEM education issue, we don't just focus on higher education. We start at the pre-K levels and extend beyond post-graduate work. Most of the education related testimony has focused on our adult population either from an academic and workforce perspective, a behavioral perspective, or a public awareness perspective. What are your education recommendations for our children when it comes to cyber security in all of these areas?

A4. Our children use computers, so it is sensible to suggest that they ought to be told something about actions they might take that could be risky. And some risky behaviors are indeed simple enough to teach a child about (e.g., don't play with matches and don't accept candy from strangers). But other behaviors are not (e.g., don't attend movies with adult themes)—we as a society prevent such behaviors, not by educating the child but instead with other safeguards. So the real issue is whether we can devise guidance even a child can understand and that, if followed, would serve that child well when venturing in cyberspace.

I'm afraid the flexibility and universal nature of computers that is their strength is also the reason simple guidance is unlikely to be useful in describing to children (or even to many adults) a large space of potentially unsafe behaviors. Unlike Smokey the Bear's exhortation about the prevention of forest fires ("Only you can . . ."), vague exhortations about risky cyber security behaviors are hard to apply when defenses and attacks co-evolve, since what is risky periodically changes.

For example, consider what we might tell a child concerning web sites he/she might visit or what actions might be "safe" when visiting a web site. The browser interface changes every few years, and attacks seem to keep pace with the creation of defenses these interfaces embody. In fact, "human-computer interaction" research studies have now demonstrated that people taught about a browser security icon (e.g., the "key icon" signifying an https connection) are still fooled by attackers who—knowing what these users have been told—create a facsimile of the icon or fashion some message that convinces users all is safe even with the icon absent. In general, as each defense fails, we as defenders create a new symbol or structure; attackers then find a way to spoof that, causing people who practice what we have previously preached to fall prey.

In light of this co-evolution of attacker and defender, we must disseminate a message for each defense we deploy. And we have a choice about that message:

- If we disseminate messages that are general enough so they don't have to be changed for each defense, then our messages are likely to require sophistication to interpret and act on. Children (and many adults) will not be well served by such messages.
- If we disseminate very specific messages that are easy to interpret and act on, then the message must change for each new generation of defense. Moreover, the different messages might have to be inconsistent with each other. Again, children (and many adults) will not be well served by such messages.

What we really need first is good tools (i) for informing users what they can trust and (ii) for users to authenticate what is at the other end of an Internet connection. Until we have such tools, our "public education" campaigns will have to be vague, hence have limited effectiveness because they cannot be converted into advice that a child can act on.

Q5. You testify that cyber security professionals are not being adequately trained to meet our needs citing lack of faculty resources and technical curriculum content

as the major problems. Which of these do you consider to be the biggest challenge and what recommendations do you have to address both of these issues.

A5. The number of cyber security faculty is the bottleneck for getting research done as well as for the development of the much needed curriculum and the delivery of that content to undergraduates, masters students, and doctoral students. Moreover, the rate at which we can graduate additional cyber security faculty will accelerate only if we can increase the number cyber security faculty members who are teaching and actively engaged in research at Ph.D.-granting institutions.

How many cyber security faculty does the Nation need? Here is one, conservative, analysis. Approximately 250 faculty are today doing research in cyber security, judging from attendance levels at research conferences and numbers of grants made by agencies that fund this kind of work. Since there are approximately 125 Ph.D.-granting institutions, that works out to approximately two researchers per institution. In reality, the distribution is skewed—the top-raked departments have more (maybe three or four) because cyber security is today a hot research area.

The list of cyber security research topics is long enough to easily justify a community of 500 researchers, since that size would allow approximately five researchers per topic area (and anything smaller does not constitute a critical mass to form a community or make significant progress). So that would mean an average of four faculty per institution, which is also a reasonable number given the number and variety of courses that should be covered.

ANSWERS TO POST-HEARING QUESTIONS

Responses by Timothy G. Brown, Vice President and Chief Architect, CA Security Management

Questions submitted by Representative Ralph M. Hall

Q1. Some experts have suggested that we should consider taking critical infrastructure networks such as those that control electricity transmission and distribution "off the grid"—onto a network physically not connected to the public Internet, just as we do with our classified military networks. Please comment on whether you think such an approach warrants further consideration, and if so what potential benefits as well as challenges would accompany it.

A1. Although there are instances where it may be desirable to segment networks completely, with no interconnection (for example, this approach is considered valuable for separating commercial aircraft flight control systems from passenger Internet access and entertainment systems), as a practical matter effective management of networked information systems, including such critical infrastructure assets as electrical generation and transmission systems facilities, require interconnection to ensure effective management, administration, maintenance and reliability. Internet connectivity is becoming increasingly necessary, as we can see from new proposals for the "smart grid," which may require Internet communications from business premises and customer homes to help monitor electricity demand and other factors important to support national energy policy.

Even in the existing environment, companies have implemented Supervisory Control and Data Acquisition systems using the Internet to enable logins to remote sites to check systems and fix problems. Without Internet access, the cost of taking these systems off-line and putting them on a private network would be enormous.

Related to this are the fact that for all practical purposes even separate networks will rely on Internet Protocol (IP) technologies, standards and products to operate and will require the assessment and management of cyber security risks. In today's environment, even very sensitive government networks require some connectivity to the public Internet, but have in place very strong controls to mitigate known risks.

The bottom line is that proposals to completely separate control systems from the public Internet are typically not feasible. We do have a responsibility, however, to treat our critical infrastructure networks differently. We should understand the risks and design systems and procedures that appropriately address these risks. In some rare cases this may require a dedicated network, but in most cases a mature well designed system of processes and technology will suffice. Our focus must be on effective cyber security risk management.

Q2. The comprehensive cyber security initiative that was created by President Bush and is continuing under President Obama focused on improving cyber security coordination across government and on funding game-changing "leap-ahead" technologies. Do you agree with these priorities? If you had an additional $100 million to spend on cyber security R&D, to what agencies and research areas would you devote it? Is there general agreement within the scientific community regarding security research priorities?

A2. Many details related to CNCI are classified, and so it remains difficult for private sector subject matter experts to assess the 12 CNCI components and their relative priorities in sufficient detail to understand how "leap-ahead" technologies development—technology is only one of the CNCI focus areas—ranks in terms of dollars and importance. To many external experts, the broad bias in the CNCI's publicly-available descriptions appears to be on the defense and response aspects of cyber security, such as reducing the number of Internet connections, intrusion detection, intrusion prevention systems and situational awareness.

The absence of designated components in the critical areas of identity management, authentication, authorization, data leak detection and prevention, insider threats, and governance areas such as records management and e-discovery does not mean they are not being addressed or given priority in the research and development initiative, but they are not given emphasis in public information. This reinforces the points I made in my testimony about the need for much more trusted collaboration between the government and industry in developing an effective national cyber security research and development agenda.

In terms of what to do with $100 million in cyber security R&D funding, my response would be that a reasoned way to answer that question is to put into place the model which I advocated in my testimony: a collaborative research agenda, re-

flecting tactical, mid-term and strategic research investments, and an accountability system for achieving results. Again, it is very important that our limited research dollars are not allocated using the current contracts and grants model. That model must be improved.

Q3. The strategy of both past and current administration has focused most of our cyber security investment—several billion dollars annually—on procuring and deploying intrusion detection systems. Due to the cat-and-mouse nature of cyber warfare and defense that several of you noted in your testimony, it seems that these systems are only effective against threats that we already know about and understand. Given this reality, can this type of approach produce effective results over the medium- or even short-term? If not, is research on a new and fundamentally secure Internet architecture the only long-term answer?

A3. As suggested in my previous response, an unbalanced focus on intrusion detection systems (IDS) overlooks the complexity of the cyber security infrastructure and the multiple, interrelated areas of risk that must be managed as part of a balanced cyber security risk management program.

With respect to IDS specifically, in the academic arena IDS research has focused largely on anomaly detection, certainly an area of promise for detecting new attacks (unlike signature-based approaches). However the false positive rate is still far too high, and it is possible that funding of research might help over the medium-term. However, IDS, while important, can never be the complete solution. IDS is a known entity in cyber warfare and as a known entity, it can be subverted. Therefore, we must address other critical areas of cyber security risk, and I would focus long-term research in the areas which I listed in my testimony.

For the long-term, I am not convinced that a "new and fundamentally security Internet architecture" is possible. For example, even in terms of advanced Internet protocols (which also have security implications), we have not seen the widespread deployment of Internet Protocol Version 6 (IPv6), despite many operational benefits. And so the adoption of a completely new architecture would be more challenging by an order of magnitude.

Perhaps a better approach is to fund research into how you can build accountability into systems, and what changes would be required to the current Internet to do that. Accountability may not be possible at the packet level, but it may be possible with changes in deployed software and applications, which may contribute to some measure of improvement to cyber security risk management.

Q4. When this committee discusses a STEM education issue, we don't just focus on higher education. We start at the pre-K levels and extend beyond post-graduate work. Most of the education-related testimony has focused on our adult population either from an academic and workforce perspective, a behavioral perspective, or a public awareness perspective. What are your recommendations for our children when it comes to cyber security in all of these areas?

A4. It cannot be repeated too often: cyber security risk management represents an unprecedented challenge for government, business and individuals and the global society, and one of its many components is the need to educate Internet users at all ages. As I noted in my testimony, education must play its appropriate role and do its part to provide cyber security awareness, knowledge, skills for our youngest students, and also contribute to the widespread adoption of ethical behaviors and practices by our youngest technology users.

I believe educational programs should be developed to ensure that teachers and schools have the skills and resources they need to make this possible and can tailor their programs to specific age groups, which have specific characteristics and needs, and must have age-appropriate content, messaging and approaches. Like cyber security itself, the programs need to address complicated subjects and issues, and an effective program will require a strong partnership and broad-based partnership among many stakeholders: school boards, educators and administrators, parents, and other communities. This is an area where well-understood approaches to educating the very young can and must be applied in support of a national cyber security educational agenda. Again, this is an area where collaboration and partnering among key stakeholders is critical.

Q5. You suggest in your testimony that it would be appropriate for a company to be awarded "sole source" federal funding for bringing a specific new research idea or project to the attention of government. I applaud your proactive approach and agree that there are many research ideas out there that will be conceived by the private sector and not by one of our federal agencies. However, I also agree with you awarding the company with the idea raises "legitimate concerns

about the fairness of the award process." How would you suggest we make this work and encourage companies to participate, while at the same time ensuring the integrity of competitive federal solicitations? Wouldn't the government and the American taxpayer gain more by an open solicitation process that would perhaps even stimulate better ideas?

A5. As I indicated in my testimony, a sole source approach would not supplant open solicitations, but would serve an important role in augmenting the current process. If my proposal for a jointly-developed, partnership-based cyber security research and development agenda were implemented, it would make possible the identification of clear categories and specific areas of research, a prioritized ranking based on risk imperatives, and a new process for funding contracts and grants using existing research funding agencies and programs. This national cyber security R&D strategy could also incorporate a category for novel, unanticipated, breakthrough ideas that could be submitted via unsolicited proposals or that could be awarded by research funding agencies directly outside the competitive solicitation process.

Whether agency-identified or proposed by external research entities, the awards process would require that the sole source grant or contract be awarded transparently, be viewed within the frame of the overall national research strategy, and be subject to accountability and performance controls.

In effect, I am proposing an approach that injects greater speed and flexibility into the research grants and contracts process for proposals that align with national objectives, but are out of cycle with the regular solicitation process or are extremely novel. I do not see sole source awards as a major tranche of awards, but as a way to augment the current process.

Finally, I believe that this option, as part of a broader national R&D strategy and plan, would serve as a clear incentive for research funding agencies to be more receptive to unsolicited proposals and see them as valuable—and supportable.

○