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

HEARING CHARTER

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 vulnerability 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 1 to 5 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 multi-faceted 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.

[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."

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 cybersecurity expertise in the Federal government.

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**	**Change over FY 2009**	
			Amount	**% 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 cybersecurity R&D and education. NSF's request is an 8.6 percent increase above FY09 levels.

NSF's cybersecurity research activities are primarily funded through the Directorate for Computer & Information Science & Engineering (CISE). CISE supports cybersecurity R&D through a targeted program, Trustworthy Computing, as well as through a number of its core activities in Computer Systems Research, Computing Research Infrastructure, and Network and Science Engineering. The cybersecurity 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 Cybersecurity 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 2-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 cybersecurity 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 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?