U.S. HOUSE OF REPRESENTATIVES

SUBCOMMITTEE ON TECHNOLOGY AND INNOVATION
SUBCOMMITTEE ON RESEARCH AND SCIENCE EDUCATION
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HEARING CHARTER

Protecting Information in the Digital Age:
Federal Cybersecurity Research and Development Efforts

Wednesday, May 25, 2011
10:00 a.m. – 12:00 p.m.
2318 Rayburn House Office Building

I. Purpose

On Wednesday, May 25, 2011, the Subcommittee on Technology and Innovation and the Subcommittee on Research and Science Education will convene a joint hearing to examine Federal agency efforts to improve our national cybersecurity and prepare the future cybersecurity talent needed for national security. An overview of cybersecurity research and development activities will be provided by the Networking and Information Technology Research and Development program (NITRD), the National Science Foundation (NSF), the National Institute of Standards and Technology (NIST), and the Department of Homeland Security (DHS). In reviewing the activities of the agencies' cybersecurity programs, the hearing will address: how each agency has responded to and continues to address objectives of the 2009 *Cyberspace Policy Review*; efforts to educate and develop the necessary cybersecurity personnel; and how standards development is coordinated with other relevant agencies.

II. Witnesses

Dr. George O. Strawn is the Director of the National Coordination Office for the Networking and Information Technology Research and Development Program.

Dr. Farnam Jahanian is the Assistant Director of the Directorate for Computer and Information Science and Engineering at the National Science Foundation.

Ms. Cita Furlani is the Director of the Information Technology Laboratory at the National Institute of Standards and Technology.

Rear Admiral Michael Brown is the Director of Cybersecurity Coordination in the National Protection and Programs Directorate for the U.S. Department of Homeland Security.

III. Overview

In January 2008, the Bush Administration established, through a series of classified executive directives, the *Comprehensive National Cybersecurity Initiative* (CNCI). The Obama Administration has continued this initiative, with the goal of securing Federal systems and fostering public-private cooperation. In February 2009, the Obama Administration called for a 60-day review of the national cybersecurity strategy. The President's review required the development of a framework that would ensure that the CNCI was adequately funded, integrated, and coordinated among Federal agencies, the private sector, and state and local authorities.

On May 29, 2009, the Administration released its *Cyberspace Policy Review*. The Review recommended an increased level of interagency cooperation among all departments and agencies, highlighted the need for information sharing concerning attacks and vulnerabilities, and highlighted the need for an exchange of research and security strategies essential to the efficient and effective defense of Federal computer systems. Furthermore, it stressed the importance of advancing cybersecurity research and development, and the need for the Federal Government to partner with the private sector to guarantee a secure and reliable infrastructure. The Review also called for increased public awareness, improved education and expansion of the number of information technology professionals.

The House Committee on Science, Space, and Technology held three subcommittee hearings in the 111th Congress to explore the state of federal cybersecurity research and development, to review the findings and recommendations included in the Administration's *Cyberspace Policy Review*, and to review the findings and recommendations of a report from the Government Accountability Office (GAO)[1]. Both the review and the report called for an increase in effective public/private partnerships, and for clarification of roles and responsibilities.

Since the release of the *Cyberspace Policy Review* and the hearings held in the 111th Congress, NITRD has continued to provide leadership in coordinating the Federal unclassified research and development. DHS has been tasked with monitoring Federal civilian networks for cyber attacks and coordinating the gathering and dissemination of information on cyber attacks to Federal agencies and private industry. NIST currently develops cybersecurity standards for non-national security Federal information technology systems, and NSF acts as the principal agency supporting unclassified cybersecurity research and development, education, and the development of cybersecurity professionals.

IV. Legislation

In June 2009, GAO found that the Federal agencies responsible for protecting the U.S. Information Technology (IT) infrastructure were not satisfying their responsibilities, leaving

[1] *National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture*, Government Accountability Office, http://www.gao.gov/new.items/d09432t.pdf

the Nation's IT infrastructure vulnerable to attack. In an effort to strengthen the work of those Federal agencies, the U.S. House of Representatives passed the Cybersecurity Enhancement Act of 2010 (H.R. 4061) in the 111th Congress. H.R. 4061 required increased coordination and prioritization of Federal cybersecurity research and development activities, and the development of cybersecurity technical standards. It also strengthened cybersecurity education and talent development and industry partnership initiatives. The Senate did not act on the legislation.

The Obama Administration released a cybersecurity legislative proposal[2] on May 12, 2011. The proposed legislation is focused on simplifying and standardizing data breach reporting and it sets penalties for computer crimes. The Administration's proposal requires that DHS work with industry to identify the core critical-infrastructure operators, and that the agency prioritize the most important cyber threats and vulnerabilities for those operators. In addition, specific cybersecurity risks must be addressed by standardized frameworks, to be developed by private sector representatives and evaluated by DHS. If DHS determines that the standardized frameworks developed by industry are insufficient, DHS will develop alternative frameworks with advice and guidance from the Director of NIST. The Administration proposal would also update the Federal Information Security Management Act (FISMA) and would formalize DHS's current role in managing cybersecurity for the Federal Government's civilian computers and networks in order to provide departments and agencies with a shared source of expertise.

V. Issues and Concerns

Research and Development

Cybersecurity research and development efforts include working on the prevention of cyber attacks, detecting attacks as they are occurring, responding to attacks effectively, mitigating severity, recovering quickly, and identifying responsible parties. In December 2010, the President's Council of Advisors on Science and Technology (PCAST) reported on Federally funded research and development in networking and information technology. The report made several recommendations, including investing in long-term, multi-agency research initiatives in security and cyber infrastructure and enhancing the effectiveness of government coordination of networking and information research and development.

Research and development provides a greater understanding of weaknesses in systems and networks and of how to protect those systems and networks. The Subcommittees will examine the integration of research and development activities within the Federal Government's cybersecurity efforts given its importance in increasing security over the long term. The hearing will explore current government research and development investments to ensure they are properly focused to provide effective and lasting cybersecurity, and will assess the challenges to establishing a prioritized national research and development agenda that strategically includes near-term, mid-term, and long-term goals.

[2] http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/Law-Enforcement-Provisions-Related-to-Computer-Security-Full-Bill.pdf

Education and the Development of Cybersecurity Professionals
Well trained professionals are essential to the implementation of security techniques in critical computer and network systems. Institutions of higher education are working to create and improve cyber education and training programs focused on ensuring an adequate number of relevant cyber professionals. Furthermore, public awareness about protecting personal information is another area of identified need within cybersecurity education. Federal agencies engaged in cybersecurity activities currently support a number of cybersecurity education, training, and development programs. The Subcommittees will consider the coordination and implementation of these activities across Federal agencies.

Standards Development
The Subcommittees will examine NIST's current and future role in the development of benchmarks, guidelines, and standards for cybersecurity, in conjunction with other government agencies and the private sector. The Subcommittees will also examine the appropriate role for NIST in facilitating the voluntary critical infrastructure cybersecurity standards as envisioned in the Administration's legislative package.

Agency Coordination
Since 1991, Federal agencies have been required to set goals, prioritize investments, and coordinate activities in networking and information technology research and development. The Subcommittees will explore what measures have been taken to improve the coordination of Federal cybersecurity research and development efforts and the best approach to improve the coordination of private sector critical infrastructure and network cybersecurity. This hearing will also examine how agencies are coordinating cybersecurity standards development.

VI. Background

In the current system, Federal Government responsibilities for cybersecurity research and development, coordination, and education fall on many different agencies. The National Security Agency (NSA) is responsible for all classified network systems. The Department of Defense (DOD) is responsible for military network systems, and DHS is the lead agency for all Federal civilian network systems. Additionally, DHS is responsible for communicating information on cyber attacks to other Federal agencies. The NITRD program coordinates unclassified cybersecurity research and development across 14 Federal agencies and is currently chaired by the Director of National Coordinating Office and the NSF Assistant Director of the Directorate for Computer and Information Science and Engineering. NSF funds a majority of Federal basic cybersecurity research and development and education efforts. Three other key agencies, NIST, DHS and DOD also fund significant cybersecurity research and development. NIST develops and promulgates standards to help secure Federal civilian network systems and the Office of Management and Budget (OMB) implements and enforces the standards set by NIST.

Networking and Information Technology Research and Development Program
The Networking and Information Technology Research and Development (NITRD)

program coordinates unclassified cybersecurity research and development across 14 Federal agencies (additional agencies informally participate in NITRD).
The High-Performance Computing Act of 1991 (PL 102-194) established NITRD. The Act has since been amended through the Next Generation Internet Research Act of 1998 and the America COMPETES Act of 2007. In the 111th Congress, the U.S. House of Representatives passed the National Information and Technology Research and Development Reauthorization Act (H.R. 2020). The bill sought to prioritize and strengthen Federal information technology activities across the Federal government. The Senate did not act on this legislation.

In December 2010, the President's Council of Advisors on Science and Technology (PCAST) completed a legislatively required report on NITRD. The report, entitled *Designing a Digital Future: Federally Funded Research and Development in Networking and Information Technology*, found that "NITRD is well coordinated and that the U.S. computing research community, coupled with a vibrant Networking and Information Technology (NIT) industry, has made seminal discoveries and advanced new technologies that are helping meet many societal challenges."[3] The PCAST report included several recommendations, including increasing investments in long-term, multi-agency research initiatives in security and cyberinfrastructure, and enhancing the effectiveness of government coordination of NIT research and development.

In February 2011, NITRD released its Supplement to the President's Budget request. The Supplement is a summary of the NITRD research activities planned and coordinated for Fiscal Year (FY) 2012. The NITRD request totals $3.9 billion for FY 2012, a 1.9 percent increase from FY 2010 expenditures. The NITRD Supplement also breaks down budget requests for the fourteen Federal agencies involved in NITRD according to Program Component Areas, including Cyber Security and Information Assurance and Social, Economic, and Workforce Implications of IT[4]:

Agency	Cyber Security and Information Assurance		Social, Economic, and Workforce Implications of IT	
	FY10 Budget Actuals (in millions)	FY12 Budget Request (in millions)	FY10 Budget Actuals (in millions)	FY12 Budget Request (in millions)
NSF	$72.7	$94.7	$99.2	$98.0
NIST	$29.6	$54.7	$0.3	$4.3
DARPA	$144.7	$222.4		
DHS	$38.0	$41.0		

National Science Foundation

NSF is the principal agency supporting unclassified cybersecurity research and development and education. NSF provides the largest Federal investment in cyber-related research and development activities. The February 2011 NITRD Supplement to the President's FY 2012

[3] President's Council of Advisors on Science and Technology, Report to the President and Congress December 2010, *Designing a Digital Future: Federally Funded Research and Development in Networking and Information Technology*, p. v

[4] Subcommittee on Networking and Information Technology Research and Development, *Supplement to the President's Budget for Fiscal Year 2010*, p. 28

Budget totals NSF's budget request for advanced technologies (which combines eight Program Component Areas) at nearly $1.3 billion, with $94.7 million dedicated for cybersecurity and information assurance and $98 million dedicated to the social, economic, and workforce implications of IT.

At NSF, the Directorate for Computer and Information Science and Engineering (CISE) is the principal directorate promoting the progress of computer and information science. CISE works across its three Divisions and across a number of NSF Directorates, focusing on theory, people and systems. Programs like Trustworthy Computing and Cybsersecurity Research, Computing Education for the 21st Century, Science and Engineering Beyond Moore's Law, and Cyber Infrastructure Framework for the 21st Century are only a handful of CISE cross-cutting programs. CISE's FY 2012 budget request includes a 17.7 percent increase over FY 2010 funding, totaling $728.4 million.

NSF has also made significant investments in cybersecurity education and workforce through the Directorate on Education and Human Resources (EHR). EHR's Scholarship for Service program provides awards to increase the number of students entering the computer security and information assurance fields, and to increase the capacity of institutions of higher education to produce professionals in these fields. EHR also offers Advanced Technological Education grants educating technicians for high-technology fields with a focus on two-year colleges.

National Institute of Standards and Technology

The NIST Information Technology Laboratory (ITL) promotes innovation and competitiveness through research and development in information technology, mathematics, and statistics. ITL, which is made up of six divisions, manages the majority of NIST cybersecurity activities, primarily through the Computer Security Division (CSD). CSD provides standards and technology to protect information systems against threats to the confidentiality, integrity, and availability of information and services.

NIST has extensive experience in developing cybersecurity standards and guidelines. NIST's core cybersecurity focus areas include: research, development, and specification; secure system and component configuration; and assessment and assurance of security properties of products and systems.

NIST develops and issues cybersecurity standards through Federal Information Processing Standards (FIPS). NIST also develops standards in conjunction with national and international consensus standards bodies. NIST publishes cybersecurity guidelines through Special Publications (NIST SP) and Interagency Reports (NISTIR).

The Computer Security Act of 1987 (PL 100-235), later replaced by the Information Technology Management Reform Act of 1996 (P.L. 104-106), gave NIST the authority to develop standards and guidelines to secure non-classified Federal information systems. Title III of the E-Government Act (PL 107-347), entitled the Federal Information Security Management Act of 2002 (FISMA), tasked NIST with developing cybersecurity standards, guidelines, and associated methods and techniques for use by the Federal Government.

The Administration's 2009 *Cyberspace Policy Review* listed trusted identities as a key issue in improving cybersecurity. On April 15, 2011, the Administration released its *National Strategy for Trusted Identities in Cyberspace* (NSTIC), with a focus on establishing identity solutions and privacy-enhancing technologies to improve the security and convenience of sensitive online transactions. As part of the strategy, the Administration plans to establish a National Program Office (NPO), which will be led by NIST within the Department of Commerce, to manage the Federal Government's role in implementing NSTIC. NIST included $24.5 million in its FY 2012 budget request to fund the NPO and to provide grants and other funding programs to conduct pilot projects of trusted authentication systems.

Department of Homeland Security

DHS is responsible for coordinating the overall national effort to enhance the protection of the critical infrastructure and key resources of the United States[5]. DHS works to prevent or minimize disruptions to our critical information infrastructure in order to protect the public, economy, government services, and the overall security of the United States by supporting a series of continuous efforts designed to further safeguard Federal Government systems by reducing potential vulnerabilities, protecting against cyber intrusions, and anticipating future threats.

The DHS Science and Technology Directorate (S&T) conducts and supports research, development, testing, evaluation, and transition for advanced cybersecurity and information assurance technologies to secure the Nation's current and future cyber and critical infrastructures. *The President's National Strategy to Secure Cyberspace*[6] and the *Comprehensive National Cybersecurity Initiative*[7] detail DHS S&T's research and development roles and responsibilities. Cybersecurity research within DHS S&T is planned, managed, and coordinated through the Cyber Security Research and Development Center. This center supports the research efforts of the Homeland Security Advanced Research Projects Agency (HSARPA), coordinates the testing and evaluation of technologies, and manages technology transfer efforts. The FY 2012 budget request for the DHS S&T Cybersecurity Division is $64.1 million.

Housed within the National Protection and Programs Directorate (NPPD) the National Cyber Security Division (NCSD) is the operational arm of DHS's Office of Cybersecurity and Communications (CS&C). NCSD works collaboratively with public, private, and international entities to secure cyberspace and America's cyber assets, and protect cyber infrastructure through two overarching objectives: building and maintaining an effective national cyberspace response system, and implementing a cyber-risk management program for the protection of critical infrastructure. Numerous programs housed within NPPD work

[5] *Homeland Security Presidential Directive-7: Critical Infrastructure Identification, Prioritization, and Protection*. December 17, 2003. http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm#1

[6] *The National Strategy to Secure Cyberspace*, February 2003. http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf

[7] *Comprehensive National Cybersecurity Initiative*. May 2009. http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf

on cybersecurity related issues. The total FY 2012 budget request, as related to cyber programs, totals more than $500 million.
NCSD programs include the United States Computer Emergency Readiness Team (US-CERT), which is responsible for analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information through the National Cyber Alert System, and coordinating incident response activities. The National Cyber Response Coordination Group (NCRCG) is the principle Federal agency mechanism for cyber incident response. In the event of a nationally significant cyber-related incident, the NCRCG, which is made up of 13 Federal agencies, helps to coordinate the Federal response, including that of US-CERT, and the cybersecurity groups of DOD, the Federal Bureau of Investigation, the NSA, and the intelligence community.

The coordinated efforts of DHS to reduce risk and improve the resilience of the nation's critical infrastructure are facilitated with many departments and agencies. DHS works with OMB to reduce and consolidate the number of external connections that Federal agencies have to the internet through the Trusted Internet Connection initiative. This initiative allows DHS to focus monitoring efforts, and block against cyber attacks on government computers. The EINSTEIN system, which is designed to provide intrusion protection and early warning of intrusions, shares information with DOD for enhanced situational awareness. DHS, OMB, and NIST coordinate the protection of agency information systems through compliance with FISMA, and DHS also coordinates with the Department of Justice to enable real-time assessments of baseline security postures across individual agencies and the Federal enterprise as a whole.