U.S. HOUSE OF REPRESENTATIVES

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

HEARING CHARTER

Agency Response to Cyberspace Policy Review

Tuesday, June 16, 2009
2:00 p.m. – 4:00 p.m.
2318 Rayburn House Office Building

I. Purpose

On Tuesday, June 16, 2009, the Subcommittee on Technology and Innovation and the Subcommittee on Research and Science Education will convene a joint hearing to review the response of the Department of Homeland Security (DHS), the National Institute of Standards and Technology (NIST), the National Science Foundation (NSF), and the Defense Advanced Research Projects Agency (DARPA) to the findings and recommendations in the Administration's 60-day Cyberspace Policy Review.

II. Witnesses

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

Dr. Jeannette Wing is the Assistant Director of the Directorate for Computer & Information Science & Engineering at the National Science Foundation.

Dr. Robert Leheny is the Acting Director of the Defense Advanced Research Projects Agency at the Department of Defense.

Dr. Peter Fonash is the Acting Deputy Assistant Secretary for the Office of Cyber Security Communications at the 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). 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

[1] CNCI objectives have been assembled from various media reports. *Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations,* http://apps.crs.gov/products/r/pdf/R40427.pdf

classified nature of the CNCI has inhibited 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. 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 60-day review of cyberspace policy. The review team acknowledged the difficult task of addressing cybersecurity concerns in a comprehensive fashion due to the large number of federal departments and agencies with cybersecurity responsibilities and overlapping authorities. According to the review, cybersecurity 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 cybersecurity. The appointee will report to both the National Security Council and the National Economic Council. The report suggests that the appointee should also 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 team also emphasized the need for the federal government to partner with the private sector to guarantee a secure and reliable infrastructure. Furthermore, it highlighted the need for increased public awareness, the education and expansion of the Information Technology (IT) workforce, and the importance of advancing cybersecurity research and development.

IV. Issues and Concerns

The Cyberspace Policy Review includes a number of near-term and mid-term action plans that are relevant to the Committee's work on the issue. (Please see the appendix for a complete list.) The review uniformly calls for increased coordination and integration of current efforts among all federal departments and agencies. The Committee is interested in how information is shared across the diverse array of coordinating bodies, which models of coordination are the most effective, and why the current mechanisms have been inadequate.

Research and Development

In the near-term, the review team recommends the development of a framework for research and development (R&D) strategies that focus on game-changing technologies that have the potential to enhance the security, reliability, resilience, and trustworthiness of the digital infrastructure.

In the mid-term, the review team recommends that the agencies expand support for R&D to ensure the Nation's continued ability to compete in the information age economy.

Unclassified federal cyber security R&D is inventoried under the interagency Networking and Information Technology R&D (NITRD) Program. The NITRD agencies have requested a total of $343 million for the Cyber Security and Information Assurance (CSIA) R&D in FY 2010. A report[2] by the Center for Strategic and International Studies (CSIS) on cybersecurity stated that "a $300 million R&D investment is inadequate." Additionally, a 2007 National Research Council (NRC) report[3] on cyberspace indicated that cybersecurity research funding was too low for researchers to pursue their promising ideas and sustained funding was necessary to increase the number of researchers examining cybersecurity topics, however, neither report offers guidance on the appropriate level of funding.

The task of coordinating unclassified cybersecurity R&D falls to CSIA interagency working group under NITRD, and to date, there have been no suggestions that another group should assume this responsibility. However, the federal plan for cybersecurity R&D developed by the working group in 2006 has been heavily criticized. The various reports[2,3] and groups indicate that the plan is just an aggregate of agency R&D activities, and they have called for the development of a set of national research objectives and funding priorities as well as a roadmap to achieve those objectives. Experts have also expressed concern that the CSIA R&D portfolio is inappropriately weighted toward short-term projects rather than long-term, potentially transformative research. Additionally, private sector stakeholders, including witnesses at the June 10th hearing, have suggested that NITRD is requesting input on the R&D agenda too late in the process for the input to be properly considered. The Committee is interested in the development of a national cybersecurity strategy with clear R&D objectives that is fully informed by academic and industry stakeholders.

The review team also recommended that the agencies provide the research community access to event data to facilitate developing tools, testing theories, and identifying workable solutions. Some in the research community have expressed concern that much of the realistic data necessary for the modeling and evaluation of cybersecurity technologies is classified or proprietary and therefore unavailable to them. DARPA is in the process of developing a large-scale testbed, the National Cyber Range (NCR), which will provide "an environment for realistic, qualitative and quantitative assessment of potentially revolutionary cyber research and development technologies." According to DARPA officials, the intent is to have the NCR available for both classified and unclassified research, but it remains to be determined if adequate firewalls can be built into the system to make this a viable goal. Related to that, the Committee is interested in exploring to what extent the academic research community will be involved in the design of NCR and whether NCR will meet their needs assuming they are granted access.

Education

There is general agreement that there are significant unmet needs for both public education and formal education and training for information technology students and professionals. The Administration's review team called for the evaluation and possible expansion of

[2] *Securing Cyberspace for the 44th Presidency*, Center for Strategic and International Studies, http://www.csis.org/component/option,com_csis_pubs/task,view/id,5157/type,0/

[3] *Toward a Safer and More Secure Cyberspace*, National Research Council, http://www.nap.edu/catalog.php?record_id=11925

existing education programs, and specifically mentioned three programs: Pathways to Revitalized Undergraduate Education in Computing (CPATH), Scholarship for Service, and the National Centers for Academic Excellence in Information Assurance Education and Research.

CPATH is an NSF sponsored program that seeks to increase the number of students with computational thinking skills by providing those types of learning opportunities in core computing classes and in other fields of study. The CPATH program receives $10 million annually.

The Scholarship for Service program is sponsored by NSF and DHS and it provides 2-year scholarships to students who are interested in pursuing a degree in information assurance and computer security. Scholarship recipients are required to work for two years in the federal government upon completion of their degree. The Scholarship for Service program is funded at $10.3 million for FY 2009, and to date, 970 scholars have been placed in federal agencies.

The National Centers for Academic Excellence in Information Assurance Education and Research, which have been in place since 1998, are sponsored by the National Security Agency (NSA) and DHS. Institutions must meet specific requirements prior to designation as a center for excellence and they must go through re-certification every five years. There are currently 94 institutions across 38 states and the District of Columbia. A number of institutions have expressed concern that the certification requirements do not accurately reflect the rigorousness of the information assurance or computer security degree offered by the institution, and therefore have chosen to let their certification lapse.

Standards and Metrics

Throughout its recommendations, the review team highlights the need for the increased use of metrics to guide strategies and to make key planning decisions. They recommend the development of a formal program assessment framework that would guide departments and agencies in defining the purpose, goal, and success criteria for each program. This framework could then be used as a basis for implementing a performance-based budgeting process, setting priorities for research and development initiatives, and assisting in development of the next-generation networks.

The review team also stresses the importance of developing standards for incident reporting, for both the federal government and private industry. Current reporting policies vary by federal department and agency based on their statutory authorities, privacy concerns, and historical practices. The consolidation of reporting policies in the federal government and expansion into the private sector would allow for more reliable and timely responses to cyber attacks.

When developing cybersecurity standards and guidelines, NIST monitors standards from international bodies such as the International Organization for Standardization (ISO). The review team, along with a report[4] from the Government Accountability Office (GAO), recommends that the federal government not only adopt appropriate standards developed by international bodies, but actively work with them to develop standards that will provide solidarity across international borders.

Cybersecurity Operations and Information Coordination

The review team calls for assessments of many of the cybersecurity programs in DHS and for an increased level of coordination among the federal departments and agencies, as well as the private sector. Although the report highlights coordination and partnership as a key element in cybersecurity strategy, it concedes that private industry may be reluctant to give information on cyber attacks due to concerns about reputational harm and liability. The federal government limits shared information based on the need to protect sensitive intelligence sources and the privacy rights of individuals. For programs like DHS's National Cyber Alert System to function as intended, guidelines must be established to enable all parties to effectively distribute cyber attack information and respond appropriately.

V. Background

In the current system, responsibilities for the security of federal network systems fall to many different agencies. NSA is responsible for all classified network systems. The Department of Defense (DOD) is responsible for military network systems and DHS is responsible for all federal civilian network systems. Additionally, DHS is responsible for communicating information on cyber attacks to other federal agencies. NIST develops and promulgates standards to help secure the federal civilian network systems, along with their other roles that will be discussed below. The Office of Management and Budget (OMB) implements and enforces the standards set by NIST. Three key agencies, NSF, DHS and DOD (specifically DARPA) fund the majority of cybersecurity R&D.

Department of Homeland Security

As tasked in Homeland Security Presidential Directive (HSPD) 7, DHS, "…shall be responsible for coordinating the overall national effort to enhance the protection of the critical infrastructure and key resources of the United States. The Secretary shall serve as the principal federal official to lead, integrate, and coordinate implementation of efforts among federal departments and agencies, State and local governments, and the private sector to protect critical infrastructure and key resources." As a response to HSPD-7, DHS created the National Cyber Security Division, detailed below. In 2008, HSPD-23, which was mostly classified, called for a central location to gather all of the cybersecurity information on attacks and vulnerabilities. DHS created the National Cyber Security Center to meet this need.

National Cyber Security Division

The National Cyber Security Division (NCSD) is the operational arm of DHS's cybersecurity group and handles a host of tasks: they detect and analyze cyber attacks,

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

disseminate cyber attack warnings to other federal government agencies, conduct cybersecurity exercises, and help reduce software vulnerabilities. The budget request for the NCSD is $400 million, an increase of $87 million above FY 2009.

- **United States Computer Emergency Readiness Team**
  Within NCSD, the US Computer Emergency Readiness Team (US-CERT) monitors the federal civilian network systems on a 24/7 basis and issues warnings to both federal agencies and the public through the National Cyber Alert System when cyber attacks occur.

  ***EINSTEIN* -** The EINSTEIN program is an intrusion detection system which US-CERT uses to monitor the federal civilian network connections for unauthorized traffic.

- **National Cyber Response Coordination Group**
  The National Cyber Response Coordination Group (NCRCG), composed of US-CERT and the cybersecurity groups of DOD, Federal Bureau of Investigation (FBI), NSA, and the intelligence community, coordinates the federal response to a cyber attack. Once an attack is detected, a warning is issued through the NCRCG to all federal agencies and the public.

- **Cyber Storm**
  Cyber Storm is a biennial cyber security exercise that allows participants to assess their ability to prepare for, protect from, and respond to cyber attacks that are occurring on a large-scale and in real-time. Cyber Storm exercises have taken place in 2006 and 2008, with 5 countries, 18 federal agencies, 9 US states, and over 40 private sector companies.

- **Software Assurance Program**
  The Software Assurance Program maintains a clearinghouse of information gathered from federal and private industry cybersecurity efforts, as well as university research, for public use. The Program has established Working Groups focused on specific software areas and holds regular forums to help encourage collaboration.

National Cyber Security Center
The National Cyber Security Center (NCSC) was created in 2008 to act as a coordinating group for consolidating, assessing and disseminating information on cyber attacks and vulnerabilities gathered from the cybersecurity efforts of DOD, DHS, NSA, FBI, and the intelligence community. By collecting information from all of these departments, the NCSC was established to provide a single source of critical cybersecurity information for all public and private stakeholders. Funding for NCSC in FY 2010 is $4 million.

Cyber Security Research and Development Center
Cybersecurity research within DHS is planned, managed, and coordinated through the Science and Technology Directorate's 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 2010 budget includes $37.2 million for cybersecurity R&D at DHS; this is an increase of $6.6 million over FY 2009.

National Institute of Standards and Technology

NIST is tasked with protecting the federal information technology network by developing and promulgating cyber security standards for federal civilian network systems (Federal Information Processing Standard [FIPS]), identifying methods for assessing effectiveness of security requirements, conducting tests to validate security in information systems, and conducting outreach exercises. These tasks were appointed to NIST in the Computer Security Act of 1987. In the Federal Information Security Management Act of 2002, OMB was tasked to develop implementation plans and enforce the use of the FIPS developed by NIST. Cybersecurity 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.

Computer Security Division

The Computer Security Division (CSD) within the Information Technology Laboratory houses the cybersecurity activities of NIST and is divided into four groups.

- **Security Technology**
  The Security Technology group focuses on cryptography and online identity authentication. These areas enable federal civilian network system users to access information both in the office and remotely in a secure manner using technologies such as: cryptographic protocols and interfaces, public key certificate management, biometrics, and smart tokens.

- **Systems and Network Security**
  The Systems and Network Security group maintains a number of databases and checklists that are designed to assist public and private network users in configuration of more secure systems. The group also conducts research in all areas of network security technology to develop new standards and transfer technologies to the public.

  ***National Checklist Program* –** This program helps develop and maintain checklists to guide network users to configure network systems with basic security settings.

  ***National Vulnerability Database* –** This database contains information on known vulnerabilities in software and fixes for these vulnerabilities.

  ***Federal Desktop Core Configuration* –** This program supplies security configurations for all federal civilian network systems using either Microsoft Windows XP or Vista. By supplying a standard configuration, this program enables security professionals to default to a known secure configuration for all new desktop computers and when experiencing a cyber attack.

Security Management and Assistance

This group extends information security training, awareness and education programs to both public and private parties.

***Federal Agency Security Practices (FASP)* –** This website provides information on cybersecurity best practices for public, private, and academia use. It contains implementation guides for education programs and a contact list of FASP staff for consultation.

***Information Security and Privacy Advisory Board (ISPAB)* –** This board advises NIST, the Secretary of Commerce, and OMB on information security and privacy issues pertaining to federal civilian network systems. They also review proposed standards and guidelines developed by NIST.

***Small Business Corner* –** This program provides workshops for small business owners to learn how to secure business information on small networks in a practical and cost-effective manner.

- **Security Testing and Metrics**
  The Security Testing and Metrics group develops methods and baselines to test security products and validate products for government use.

National Science Foundation

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 cyber security portfolio supports both theoretical and experimental research. NSF cybersecurity research and education activities are funded at $127 million for FY 2010.

- **Trustworthy Computing Program**
  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.

- **Scholarship for Service**
  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.

Defense Advanced Research Projects Agency

DARPA is the principal R&D agency of DOD; its mission is to identify and develop high-risk, high-reward technologies of interest to the military. DARPA's cybersecurity 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.

- **Intrinsically Assured Mobile Ad-Hoc Network**
  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.

- **Trustworthy Systems & TrUST**
  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.

- **National Cyber Range**
  The goal of the NCR is to provide a revolutionary environment for research organizations to test the security of information systems. The budget request for the NCR is $50 million for FY 2010.

VI. Action Plans

The review team recommends the near-term and mid-term actions listed in Tables 2 and 3.

TABLE 2: NEAR-TERM ACTION PLAN

1. Appoint a cybersecurity policy official responsible for coordinating the Nation's cybersecurity policies and activities; establish a strong NSC directorate, under the direction of the cybersecurity policy official dual-hatted to the NSC and the NEC, to coordinate interagency development of cybersecurity-related strategy and policy.
2. Prepare for the President's approval an updated national strategy to secure the information and communications infrastructure. This strategy should include continued evaluation of CNCI activities and, where appropriate, build on its successes.
3. Designate cybersecurity as one of the President's key management priorities and establish performance metrics.
4. Designate a privacy and civil liberties official to the NSC cybersecurity directorate.
5. Convene appropriate interagency mechanisms to conduct interagency-cleared legal analyses of priority cybersecurity-related issues identified during the policy-development process and formulate coherent unified policy guidance that clarifies roles, responsibilities, and the application of agency authorities for cybersecurity-related activities across the Federal government.
6. Initiate a national public awareness and education campaign to promote cybersecurity.
7. Develop U.S. Government positions for an international cybersecurity policy framework and strengthen our international partnerships to create initiatives that address the full range of activities, policies, and opportunities associated with cybersecurity.
8. Prepare a cybersecurity incident response plan; initiate a dialog to enhance public-private partnerships with an eye toward streamlining, aligning, and providing resources to optimize their contribution and engagement
9. In collaboration with other EOP entities, develop 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 access to event data to facilitate developing tools, testing theories, and identifying workable solutions.
10. Build a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties interests, leveraging privacy-enhancing technologies for the Nation.

TABLE 3: MID-TERM ACTION PLAN

1. Improve the process for resolution of interagency disagreements regarding interpretations of law and application of policy and authorities for cyber operations.
2. Use the OMB program assessment framework to ensure departments and agencies use performance-based budgeting in pursuing cybersecurity goals.
3. Expand support for key education programs and research and development to ensure the Nation's continued ability to compete in the information age economy.
4. Develop a strategy to expand and train the workforce, including attracting and retaining cybersecurity expertise in the Federal government.
5. Determine the most efficient and effective mechanism to obtain strategic warning, maintain situational awareness, and inform incident response capabilities.
6. Develop a set of threat scenarios and metrics that can be used for risk management decisions, recovery planning, and prioritization of R&D.
7. Develop a process between the government and the private sector to assist in preventing, detecting, and responding to cyber incidents.
8. Develop mechanisms for cybersecurity-related information sharing that address concerns about privacy and proprietary information and make information sharing mutually beneficial.
9. Develop solutions for emergency communications capabilities during a time of natural disaster, crisis, or conflict while ensuring network neutrality.
10. Expand sharing of information about network incidents and vulnerabilities with key allies and seek bilateral and multilateral arrangements that will improve economic and security interests while protecting civil liberties and privacy rights.
11. Encourage collaboration between academic and industrial laboratories to develop migration paths and incentives for the rapid adoption of research and technology development innovations.
12. Use the infrastructure objectives and the research and development framework to define goals for national and international standards bodies.
13. Implement, for high-value activities (e.g., the Smart Grid), an opt-in array of interoperable identity management systems to build trust for online transactions and to enhance privacy.
14. Refine government procurement strategies and improve the market incentives for secure and resilient hardware and software products, new security innovation, and secure managed services.