

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

HEARING CHARTER

Assessing Cybersecurity Activities at NIST and DHS

Thursday, June 25, 2009
2:00 p.m. – 4:00 p.m.
2318 Rayburn House Office Building

I. Purpose

On Thursday, June 25, 2009, the Subcommittee on Technology and Innovation will convene a hearing to assess the cybersecurity efforts of the Department of Homeland Security (DHS) and the National Institute of Standards and Technology (NIST). In reviewing the activities of the agencies' cybersecurity programs, the hearing will solicit the input of private-sector experts on how federal cybersecurity activities can enhance privately-owned critical infrastructure, better monitor federal networks, and more clearly define cybersecurity performance with metrics and success criteria.

II. Witnesses

Mr. Greg Wilshusen is the Director of Information Security Issues at the Government Accountability Office.

Mr. Mark Bregman is the Executive Vice President and Chief Technology Officer of Symantec Corporation.

Mr. Scott Charney is the Corporate Vice President of Microsoft's Trustworthy Computing Group.

Mr. Jim Harper is the Director of Information Policy Studies at the Cato Institute.

III. Overview

In January 2008, the Bush Administration established, through a series of classified executive directives, the Comprehensive National Cybersecurity Initiative (CNCI). While the goal of the initiative was to secure federal systems, a number of security experts have expressed concern that the 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 of CNCI. 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 Cyber Space Policy Review. The review recommended an increased level of interagency cooperation amongst all departments and agencies. The active exchange of information concerning attacks, vulnerabilities, research, and security strategies is essential to the efficient and effective defense of federal computer systems. 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.

The hearing will address recommendations made in the Cyber Space Policy Review and a recent report from the GAO¹. DHS currently monitors the federal civilian networks for cyber attacks and coordinates the gathering and dissemination of information on cyber attacks to federal agencies and private industry. The policy review and GAO report highlight deficiencies in both the operations and coordination roles. The policy review also calls on a more proactive plan for collaboration with international standards bodies and an end to the cybersecurity distinctions between national security and other federal networks. NIST currently develops and promulgates standards to help secure the federal civilian network systems. Finally, both reports call for an increase in effective public/private partnerships, despite a current high number of coordination councils and advisory boards. The policy review states that the high number of coordinating groups has left some participants frustrated with unclear roles and responsibilities and an excess of plans and recommendations.

IV. Issues and Concerns

Operations

The Cyber Space Policy Review called for the review of some of the DHS cybersecurity programs. It recommends a review of the "operational concept and the implementation of the National Cyber Security Center (NCSC) to determine whether its proposed responsibilities, resource strategy, and governance are adequate to enable it to provide the shared situational awareness necessary to support cyber incident response efforts." This center was also specifically discussed in the report from GAO in its recommendation that DHS needed to ensure that there are distinct and transparent lines of authority and responsibility assigned to DHS organizations with cybersecurity roles and responsibilities. The same report also mentioned DHS difficulties in hiring and retaining adequately trained staff that has been hindering the function of the NCSC.

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 Cyber Space Policy Review also recommended that DHS continue to pursue the goal of the Trusted Internet Connection program to reduce the number of government network connections to the Internet but to reconsider goals and timelines based on a realistic assessment of the challenges. DHS uses the trusted connections and monitoring devices to protect the federal civilian networks. The review calls for the evaluation and continuation of these pilot deployments of intrusion detection and prevention systems in consultation with the civil liberties and privacy community. The lessons learned from these deployments could be used with other networks, such as those operated by the State governments.

Standards

A major recommendation from industry experts indicates the need to end the bifurcation of minimum cybersecurity standards amongst military, national security, and federal civilian networks. A recent draft report from NIST proposes a unified set of standards that meet this recommendation². The use of a single set of basic standards and minimum security requirements will simplify acquisition of network components and ease the assessment of cybersecurity performance.

The review team also recommends that the federal government determine a strategy to work with international partners to develop cybersecurity standards and legal framework with which to deal with cybercrime. Internationally-consistent policies will provide a simpler set of cybersecurity guidelines for international companies and for prosecution of cybercriminals. Additionally, the review recommends that the federal government coordinate with international partners and standards bodies to support next-generation global communications capabilities.

Critical Infrastructure

Critical infrastructure represents a challenge because much of it is privately-owned, yet could represent a major vulnerability to the security of the nation. The Cyber Space Policy Review called for increased coordination and integration of current efforts among all federal departments and agencies, and with private industry to assist in securing critical infrastructure. Currently, an assortment of public-private partnerships, advisory boards, and information sharing mechanisms exists across the federal government, such as the Critical Infrastructure Partnership Advisory Council (CIPAC), IT-Sector Coordinating Council (IT-SCC), National Infrastructure Advisory Council, and Information Security and Privacy Advisory Board (ISPAB).

Metrics

Throughout its recommendations, the review team highlights the need for the increased use of performance metrics to guide strategies and to make key planning decisions. Cybersecurity efforts are traditionally assessed by detailing the number of initiatives and funding spent on these initiatives. A set of metrics based on actual outcomes of efforts, instead of output of initiatives and funds would better assess the current activities and

² *Recommended Security Controls for Federal Information Systems and Organizations*, National Institute of Standards and Technology Special Publication 800-53 DRAFT, <http://csrc.nist.gov/publications/drafts/800-53/800-53-rev3-FPD-clean.pdf>

identify areas for improvement. 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.

V. Background

In the current system, responsibilities for the security of federal network systems fall to 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 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, National Science Foundation (NSF), DHS and DOD (specifically the Defense Advanced Research Projects Agency (DARPA)) fund the majority of cybersecurity research and development (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 (NCSA), 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 NCSC to meet this need.

National Cyber Security Division

The NCSA is the operational arm of DHS's cybersecurity group and handles a host of tasks: they detect and analyze cyber attacks, disseminate cyber attack warnings to other federal government agencies, conduct cybersecurity exercises, and help reduce software vulnerabilities. The budget request for the NCSA is \$400 million, an increase of \$87 million above FY 2009.

- **United States Computer Emergency Readiness Team**

Within NCSA, 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 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 Computer Security Information Assurance (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 foci ensure that access to information is only granted to the appropriate users and done so 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.

Information Security and Privacy Advisory Board) – 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.