AGENCY RESPONSE TO CYBERSPACE POLICY REVIEW

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY AND INNOVATION

AND THE

SUBCOMMITTEE ON RESEARCH AND SCIENCE EDUCATION

COMMITTEE ON SCIENCE AND TECHNOLOGY

HOUSE OF REPRESENTATIVES

ONE HUNDRED ELEVENTH CONGRESS

FIRST SESSION

JUNE 16, 2009

Serial No. 111–34

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

50–171PDF WASHINGTON : 2010

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. LUJAN, 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 TECHNOLOGY AND INNOVATION

HON. DAVID WU, Oregon, *Chair*

DONNA F. EDWARDS, Maryland
BEN R. LUJAN, New Mexico
PAUL D. TONKO, New York
DANIEL LIPINSKI, Illinois
HARRY E. MITCHELL, Arizona
GARY C. PETERS, Michigan
BART GORDON, Tennessee

ADRIAN SMITH, Nebraska
JUDY BIGGERT, Illinois
W. TODD AKIN, Missouri
PAUL C. BROUN, Georgia

RALPH M. HALL, Texas

MIKE QUEAR *Subcommittee Staff Director*
MEGHAN HOUSEWRIGHT *Democratic Professional Staff Member*
TRAVIS HITE *Democratic Professional Staff Member*
HOLLY LOGUE PRUTZ *Democratic Professional Staff Member*
DAN BYERS *Republican Professional Staff Member*
VICTORIA JOHNSTON *Research Assistant*

VerDate 11-MAY-2000 11:39 Jan 29, 2010 Jkt 050171 PO 00000 Frm 00002 Fmt 5904 Sfmt 5904 C:\DWORK\T&I09\061609\50171 SCIENCE1 PsN: SCIENCE1

SUBCOMMITTEE ON RESEARCH AND SCIENCE EDUCATION

HON. DANIEL LIPINSKI, Illinois, *Chair*

EDDIE BERNICE JOHNSON, Texas	VERNON J. EHLERS, Michigan
BRIAN BAIRD, Washington	RANDY NEUGEBAUER, Texas
MARCIA L. FUDGE, Ohio	BOB INGLIS, South Carolina
PAUL D. TONKO, New York	BRIAN P. BILBRAY, California
PARKER GRIFFITH, Alabama	
RUSS CARNAHAN, Missouri	
BART GORDON, Tennessee	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 16, 2009

Page

Appendix: Answers to Post-Hearing Questions

AGENCY RESPONSE TO CYBERSPACE POLICY REVIEW

TUESDAY, JUNE 16, 2009

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON TECHNOLOGY AND INNOVATION,
JOINTLY WITH THE
SUBCOMMITTEE ON RESEARCH AND SCIENCE EDUCATION,
COMMITTEE ON SCIENCE AND TECHNOLOGY,
Washington, DC.

The Subcommittees met, pursuant to call, at 2:47 p.m., in Room 2318 of the Rayburn House Office Building, Hon. David Wu [Chairman of the Subcommittee on Technology and Innovation] presiding.

VerDate 11-MAY-2000 11:39 Jan 29, 2010 Jkt 050171 PO 00000 Frm 00007 Fmt 6633 Sfmt 6633 C:\DWORK\T&I09\061609\50171 SCIENCE1 PsN: SCIENCE1

BART GORDON, TENNESSEE
CHAIRMAN

RALPH M. HALL, TEXAS
RANKING MEMBER

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE AND TECHNOLOGY
SUITE 2321 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6301
(202) 225–6375
http://science.house.gov

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

Hearing on:

Agency Response to Cyberspace Policy Review

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

Witness List

Ms. Cita Furlani
Director, Information Technology Laboratory, National Institute of Standards and Technology

Dr. Jeannette Wing
Assistant Director, Directorate for Computer & Information Science & Engineering, National Science Foundation

Dr. Robert Leheny
Acting Director, Defense Advanced Research Projects Agency, Department of Defense

Dr. Peter Fonash
Acting Deputy Assistant Secretary, Office of Cyber Security Communications, Department of Homeland Security

HEARING CHARTER

SUBCOMMITTEE ON TECHNOLOGY AND INNOVATION
JOINTLY WITH THE
SUBCOMMITTEE ON RESEARCH AND SCIENCE EDUCATION
COMMITTEE ON SCIENCE AND TECHNOLOGY
U.S. HOUSE OF REPRESENTATIVES

Agency Response to Cyberspace Policy Review

TUESDAY, JUNE 16, 2009
2:00 P.M.–4:00 P.M.
2318 RAYBURN HOUSE OFFICE BUILDING

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 multifaceted initiative was to secure federal systems.[1] 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. 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. Accord-

[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*

ing 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 cybersecurity 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

---

[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*

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 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 two-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 recertification 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

[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*

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, 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 U.S. 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 cybersecurity 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 five countries, 18 federal agencies, nine U.S. 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 cybersecurity 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 web site 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 cybersecurity 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 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 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.

Chairman WU. This hearing will now come to order. Welcome everyone to this afternoon's hearing on the Administration's Cyberspace Policy Review. This is the second of three hearings the Science and Technology Committee is holding on cybersecurity. Last week the Research and Science Education Subcommittee held a hearing on the research needs for improved cybersecurity, and next week my Technology and Innovation Subcommittee will hold a hearing on the cybersecurity activities of the National Institute of Standards and Technology (NIST) and the Department of Homeland Security (DHS).

I have been long concerned by the lack of attention given to cybersecurity by the Federal Government and by the private sector. Previously, federal efforts were output oriented-focused on things like the number of programs, funds spent, or numbers of interagency working groups—rather than outcome driven. I am pleased that the new Administration has made cybersecurity a top priority and is focusing efforts on achieving outcomes such as fewer breaches of federal systems, fewer cases of identity theft, and the security of smart grid systems and health IT systems.

In order to achieve these very, very important results, it is essential to first conduct a review of our federal cybersecurity structure and efforts. The Administration's cyberspace review does not make any brand new recommendations. However, it is valuable as a frank assessment of current federal activities and a roadmap for what needs to be fixed. In general, the recommendations suggest improving interagency coordination and coordination with the private sector, modernizing the research agenda, and enhancing public education on cybersecurity.

By addressing each of these recommendations we are laying the building blocks for our new, outcomes-based approach to federal cybersecurity. The four agencies appearing before the Committee today have a significant role to play in creating that foundation. During today's hearing, I hope to learn how each agency intends to improve its current cybersecurity efforts in response to the Administration's review. This information will help guide the Committee's ongoing efforts to protect our nation's data, computer systems and its citizens.

[The prepared statement of Chairman Wu follows:]

PREPARED STATEMENT OF CHAIRMAN DAVID WU

I want to welcome everyone to this morning's hearing on the administration's cyberspace policy review. This is the second of three hearings the Science and Technology Committee is holding on cybersecurity. Last week the Research and Science Education Subcommittee held a hearing on the research needs for improved cybersecurity, and next week my Technology and Innovation Subcommittee will hold a hearing on the cybersecurity activities at the National Institute of Standards and Technology and the Department of Homeland Security.

I have long been concerned by the lack of attention given to cybersecurity by the Federal Government. Previously, federal efforts were output oriented-focused on things like the number of programs, funds spent, or numbers of interagency working groups—rather than outcome driven. I am pleased that the new Administration has made cybersecurity a top priority and is focusing efforts on achieving outcomes such as fewer breaches of federal systems, fewer cases of identity theft, and the security of smart grid systems and health IT systems.

In order to achieve those important results, it was essential to first conduct a review of our federal cybersecurity structure. The Administration's cyberspace review does not make any brand new recommendations. However, it is valuable as a frank assessment of current federal activities and a roadmap for what needs to be fixed.

In general, the recommendations suggest improving interagency coordination and coordination with the private sector, modernizing the research agenda, and enhancing public education on cybersecurity.

By addressing each of these recommendations we are laying the building blocks for our new, outcomes-based approach to federal cybersecurity. The four agencies appearing before the Committee today have a significant role to play in creating that foundation. During today's hearing, I hope to learn how each agency intends to improve their current cybersecurity efforts in response to the Administration's review. This information will help guide the Committee's ongoing efforts to protect our nation's data and citizens.

Chairman WU. I want to thank our witnesses for appearing before us today, and now I would like to recognize Representative Smith for his opening statement.

Mr. SMITH. Thank you, Chairman Wu, and thank you for holding this hearing today to review the Administration's efforts to strengthen cybersecurity as outlined specifically in the White House's recently released Cyberspace Policy Review. While federal efforts to increase network security date back several years, they were brought to the forefront in early 2008 when President Bush formally established the Comprehensive National Cyber Security Initiative to deal with widespread and successful cyber attacks on federal networks. President Obama has committed to fully continue this effort under his Administration and emphasized its importance in a recent speech.

It seems the continuity across the Bush and Obama Administrations, as well as the increased attention being given to this issue in Congress, provide indication of a small but important advantage of where we were just a couple of years ago. Awareness of this problem and the need for action is now nearly universal. There is broad agreement on the seriousness and magnitude of our cybersecurity vulnerabilities and the complexity of the technical and policy changes that must be addressed to overcome them.

However, while there is a consensus on the problem, we are still at the earliest stages of identifying and implementing solutions, and we are working through relatively unchartered policy territory as we do so. Accordingly, I hope both Congress and the Administration will work to balance the pressure to act quickly and aggressively on cybersecurity with the need for thorough and deliberate consideration of all possible courses of action.

To this end, as we hold these hearings and consider legislative options later this summer, I hope to focus on three broad areas of cybersecurity policy: (1) R&D. Are we investing enough in R&D given its importance as the primary driver of increasing security over the long-term? (2) DHS-led efforts to secure the dot-gov domain. Are we confident that the reported $30 billion price tag of this initiative is appropriately focused, and is its centerpiece program EINSTEIN going to provide effective and lasting security? And (3) private sector critical infrastructure. What is the best approach to improving the security of these networks? Do new regulations or liability protections make sense or could they be counterproductive to our security goals?

I hope today's hearing will serve to begin the process of answering these questions. I thank the witnesses for being here, and I certainly look forward to a productive discussion. I yield back.

[The prepared statement of Mr. Smith follows:]

PREPARED STATEMENT OF REPRESENTATIVE ADRIAN SMITH

Mr. Chairman, thank you for holding this hearing today to review the Administration's efforts to strengthen cybersecurity, as outlined specifically in the White House's recently released Cyberspace Policy Review.

While federal efforts to increase network security date back several years, they were brought to the forefront in early 2008, when President Bush formally established the Comprehensive National Cybersecurity Initiative to deal with widespread and successful cyberattacks on federal networks. President Obama has committed to fully continue this effort under his administration and emphasized its importance in a recent speech.

It seems this continuity across the Bush and Obama Administrations—as well as the increased attention being given to this issue in Congress—provide indication of a small but important advantage over where we were just a couple of years ago: awareness of this problem and the need for action is now nearly universal. There is broad agreement on the seriousness and magnitude of our cybersecurity vulnerabilities, and the complexity of the technical and policy challenges that must be addressed to overcome them.

However, while there is a consensus on the problem, we are still at the earliest stages of identifying and implementing solutions, and we're working through relatively un-chartered policy territory as we do so. Accordingly, I hope both Congress and the Administration will work to balance the pressure to act quickly and aggressively on cybersecurity with the need for thorough and deliberate consideration of all possible courses of action.

To this end, as we hold these hearings and consider legislative options later this summer, I hope to focus on three broad areas of cybersecurity policy: (1) R&D—Are we investing enough in R&D given its importance as the primary driver of increasing security over the long-term?; (2) DHS-led efforts to secure the dot-gov domain—are we confident that the reported $30 billion price tag of this initiative is appropriately focused, and is its centerpiece program EINSTEIN going to provide effective and lasting security?; and (3) private sector critical infrastructure—what is the best approach to improving the security of these networks—do new regulations or liability protections make sense, or could they be counterproductive to our security goals?

I hope today's hearing will serve to begin the process of answering these questions. I thank the witnesses for being here and I look forward to a productive discussion.

Chairman WU. Thank you very much, Mr. Smith. And now I would like to recognize Representative Lipinski, Chairman of the Research Subcommittee, for his opening statement.

Chairman LIPINSKI. Good afternoon. I would like to thank Chairman Wu for joining me in holding this hearing. I look forward to working with him and other Members of this committee on the critical issue of cybersecurity.

Last week my Research and Science Education Subcommittee held a hearing on the state of cybersecurity R&D, and several of our witnesses emphasized the need for better partnerships and information sharing between the Federal Government and the private sector. We also discussed the challenges facing incentivizing agencies, companies, and individuals, especially those that don't face an immediate or obvious threat to adopt established best practices and to disclose breaches in security, and the expert panel echoed recent reports regarding concerns over lack of prioritization in the federal R&D portfolio.

One additional issue we discussed in last week's hearing was the importance of education. The panel emphasized that our IT workforce needs to be taught the skills necessary to incorporate security into software and systems from the beginning. But IT professionals are not the only ones who need to be better educated. The panel agreed that increasing the public's awareness of the risks and consequences of poor security practices is also essential. People are the beneficiaries of IT but also the weakest link in IT security, and

computer scientists need to team with social scientists to gain a better understanding of how humans interact with and utilize technology.

We need a cultural change in the ways that Americans practice their computer hygiene.

Now, today I look forward to hearing from our witnesses about their agency's responses to the cyberspace policy review. As I said, this is a critical issue, and I am very happy that the Administration has focused in on it and we are doing so here on the Committee.

A secure and resilient cyberspace is vital not only for the Federal Government, but for businesses large and small and for every single American. This goal can only be realized through our combined efforts and a multi-disciplinary approach to the problem. So all of our witnesses and their agencies will play a key role in maintaining this vital cyberspace. I want to thank the witnesses for taking the time to appear before us this afternoon, and I look forward to your testimony.

[The prepared statement of Chairman Lipinski follows:]

PREPARED STATEMENT OF CHAIRMAN DANIEL LIPINSKI

Good afternoon. I'd like to thank Chairman Wu for joining me in holding this hearing, and I look forward to working with him on this critical issue of cybersecurity.

Last week, my Research & Science Education Subcommittee held a hearing on the state of cybersecurity R&D. Several of our witnesses emphasized the need for better partnerships and information sharing between the Federal Government and the private sector. We also discussed the challenges faced in incentivizing agencies, companies, and individuals—especially those that don't face an immediate or obvious threat—to adopt established best practices and to disclose breaches in security. And the expert panel echoed recent reports regarding concerns over a lack of prioritization in the federal R&D portfolio.

One additional issue we discussed in last week's hearing was the importance of education. The panel emphasized that our IT workforce needs to be taught the skills necessary to incorporate security into software and systems from the beginning. But IT professionals are not the only ones who need to be better educated. The panel agreed that increasing the public's awareness of the risks and consequences of poor security practices is also essential. People are the beneficiaries of IT but also the weakest link in IT security, and computer scientists need to team with social scientists to gain a better understanding of how humans interact with and utilize technology. We need a "cultural change" in the ways that Americans practice "computer hygiene."

I look forward to hearing from our witnesses today about their agencies' responses to the Cyberspace Policy Review. As I said, this is a critical issue. A secure and resilient cyberspace is vital not only for the Federal Government, but for businesses—large and small—and for every single American. This goal can only be realized through our combined efforts, and a multi-disciplinary approach to the problem. So all of you and your agencies will play a key role in maintaining a vital cyberspace.

I want to thank the witnesses for taking the time to appear before us this afternoon and I look forward to your testimony.

Chairman WU. Thank you, Chairman Lipinski. And now I would like to recognize Mr. Ehlers for his opening statement, the Ranking Member of the Research Subcommittee.

Mr. EHLERS. Thank you, Mr. Chairman. As the last and probably least, I will try to keep my comments very short.

The security of our information is vitally important to all Federal Government entities and that includes the House of Representatives. Many of my colleagues are aware that our own networks are targeted daily by people and governments who would like to do

harm to us, our government, or to find out personal information that has been provided to us by our constituents or other friends in other countries.

It takes strategic planning and organization to avoid and address these attacks. When considering the impacts of information security on policy development related to electronic health records, national defense and technology development, for example, it quickly becomes obvious how important trusted networks are to the public and to legislators.

All of the federal agencies testifying at the witness table today play a critical role in protecting the security of our systems while maintaining the necessary freedom to exchange unfettered communication.

I look forward to your comments on how the agencies are advancing the national cybersecurity efforts, and I expect to learn a great deal from each one of you today. Thank you very much.

[The prepared statement of Mr. Ehlers follows:]

PREPARED STATEMENT OF REPRESENTATIVE VERNON J. EHLERS

The security of our information is vitally important to all Federal Government entities, including the House of Representatives. Many of my colleagues are aware that our own networks are targeted daily by people who would like to do harm to our government, and it takes strategic planning and organization to avoid and address these attacks. When considering the impacts of information security on policy development related to electronic health records, national defense, and technology development, for example, it quickly becomes obvious how important trusted networks are to the public and to legislators.

All of the federal agencies testifying at the witness table today play a critical role in protecting the security of our systems while maintaining the necessary freedom to exchange unfettered communication. I look forward to their comments on how the agencies are advancing our national cybersecurity efforts.

Chairman WU. Thank you, Dr. Ehlers. If there are other Members who wish to submit opening statements, your statements will be added to the record at this point.

[The prepared statement of Mr. Mitchell follows:]

PREPARED STATEMENT OF REPRESENTATIVE HARRY E. MITCHELL

Thank you, Mr. Chairman.

As the world becomes increasingly connected through the Internet, it is critical to ensure that we have an effective and secure cyberspace policy.

Today we will discuss the findings and recommendations of the Obama Administration's 60-day Cyberspace Policy Review.

We will also 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)'s response to the Administration's policy review.

I look forward to hearing more from our witnesses on what steps need to be taken to establish a more comprehensive cyberspace policy that will improve our cybersecurity.

I yield back.

Chairman WU. And now it is my pleasure to introduce our 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 at 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, and Dr. Peter Fonash is the Acting Deputy Assistant Secretary at the Of-

fice of Cyber Security Communications at the U.S. Department of Homeland Security.

The witnesses will have five minutes for spoken testimony, and your written testimony will be included in the record in their entirety. And when you complete you testimony, we will begin with questions. Each Member will have five minutes to question the panel. Ms. Furlani, please proceed.

STATEMENT OF MS. CITA M. FURLANI, DIRECTOR, INFORMATION TECHNOLOGY LABORATORY, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), U.S. DEPARTMENT OF COMMERCE

Ms. FURLANI. Thank you, Chairman Wu and Chairman Lipinski, Ranking Members Smith and Ehlers, and Members of the Subcommittees. I appreciate the opportunity to appear before you today to discuss our role in cybersecurity and our perspective on the Administration's Cyberspace Policy Review.

Through our work in information technology, NIST accelerates the development and deployment of information and communication systems that are reliable, usable, inter-operable, and secure. It advances measurement science through innovations in mathematics, statistics, and computer science and conducts research to develop the measurements and standards infrastructure for emerging information technologies and applications.

Many of our vital programs impact national security, such as improving the accuracy and inter-operability of biometrics recognition systems, and facilitating communications among first responders.

Research activities range from innovations in identity management and verification, to metrics for complex systems, to development of practical and secure cryptography in a quantum computing environment, to automation of discovery and maintenance of system security configurations and status, and to techniques for specification and automation of access authorization in line with many different kinds of access policies.

As you are aware, beginning in the early 1970's, NIST has developed standards to support federal agencies' information assurance requirements. Through the *Federal Information Security Management Act*, or FISMA, Congress again reaffirmed NIST's leadership role in developing standards for cybersecurity. FISMA provides for the development and promulgation of Federal Information Processing Standards, or FIPS, that are compulsory and binding for federal computer systems. NIST's mission in cybersecurity is to work with federal agencies, industries, and academia to research, develop and deploy information security standards and technology to protect information systems against threats to the confidentiality, integrity, and availability of information and services.

Consistent with this mission and with the recommendations of the President's Cyberspace Policy Review, NIST is actively engaged with private industry, academia, non-national security federal departments and agencies, the intelligence community, and other elements of the law enforcement and national security communities in coordination and prioritization of cybersecurity research, standards development, standards conformance demonstration, and cybersecurity education and outreach.

The national security community, a number of state governments, and major private sector organizations are also adopting the risk management framework and cybersecurity controls designed by NIST for the Federal Government. NIST is engaging industry to harmonize product assurance requirements to align with industry business models and system development practices.

We play a leading security role in supply chain risk management, health care information technology, the Smart Grid, biometrics and face authentication, next generation voting systems, and cloud computing. We work with the intelligence and counterterrorism communities to facilitate cross sector information sharing among federal, State and local government organizations. We team with the Department of Justice and the Small Business Administration in extending cybersecurity education and training beyond the Federal Government into the private sector.

For the first time, and as part of the ongoing initiative to develop a unified information security framework for the Federal Government and its contractors, NIST has included security controls in its catalog for both national security and non-national security systems. The updated security control catalog incorporates best practices in information security from the United States Department of Defense, the intelligence community, and civil agencies to produce the most broad-based and comprehensive set of safeguards and countermeasures ever developed for information systems.

Under the provisions of the *National Technology Transfer and Advancement Act,* NIST is also tasked with the key role of encouraging and coordinating federal agency development and use of voluntary consensus standards and coordinating the public-private sector development of standards and conformity assessment activities through consensus standards organizations. NIST will continue to conduct the research necessary to enable and provide cybersecurity specifications, standards, assurance processes, training, and technical expertise needed for securing the U.S. Government and critical infrastructure information systems to mitigate the growing threat. NIST will continue to closely coordinate with domestic and international private sector cybersecurity programs and national security organizations.

Thank you for the opportunity to testify today on NIST's work in the cybersecurity arena and our views on the President's Cyberspace Policy Review. I will be happy to answer any questions you may have.

[The prepared statement of Ms. Furlani follows:]

PREPARED STATEMENT OF CITA M. FURLANI

Introduction

Chairmen Wu and Lipinski, Ranking Members Smith and Ehlers, and Members of the Subcommittees, I am Cita Furlani, the Director of the Information Technology Laboratory (ITL) at the Department of Commerce's National Institute of Standards and Technology (NIST). Thank you for the opportunity to appear before you today to discuss our role in cybersecurity and our perspective on the Administration's 60 Day Cyberspace Policy Review.

As one of the major research components within NIST, our information technology work accelerates the development and deployment of information and communication systems that are reliable, usable, inter-operable, and secure; advances measurement science through innovations in mathematics, statistics, and computer science; and conducts research to develop the measurements and standards infrastructure

for emerging information technologies and applications. NIST accomplishes these goals through collaborative partnerships with our customers and stakeholders in industry, government, academia, and consortia. Based on input from these customers and stakeholders, we have focused our R&D agenda on eight broad program areas: complex systems; cyber and network security; enabling scientific discovery; identity management systems; information discovery, use and sharing; pervasive information technologies; trustworthy information systems; and virtual measurement systems.

Many of our vital programs impact national security, such as improving the accuracy and inter-operability of biometrics recognition systems and facilitating communications among first responders. The combination of our mission and legislation such as the *Federal Information Security Management Act* (FISMA) the *Computer Security Research and Development Act,* the *USA PATRIOT Act,* the *Enhanced Border Security Act,* and the *Help America Vote Act* lead to rich programmatic diversity.

As you are aware, beginning in the early 1970s with enactment of the *Brooks Act,* NIST has developed standards to support federal agencies' information assurance requirements for many years. Through FISMA, Congress again reaffirmed NIST's leadership role in developing standards for cybersecurity. FISMA provides for the development and promulgation of Federal Information Processing Standards (FIPS) that are "compulsory and binding" for federal computer systems. The responsibility for the development of FIPS rests with NIST, and the authority to promulgate mandatory FIPS is given to the Secretary of Commerce. Section 303 of FISMA states that NIST shall:

- have the mission of developing standards, guidelines, and associated methods and techniques for information systems;
- develop standards and guidelines, including minimum requirements, for information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency, other than national security systems; and
- develop standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems.

NIST's mission in cybersecurity is to work with federal agencies, industry, and academia to research, develop and deploy information security standards and technology to protect information systems against threats to the confidentiality, integrity and availability of information and services. Consistent with this mission and with the recommendations of the President's recent 60 Day Cyberspace Policy Review, NIST is actively engaged with private industry, academia, non-national security federal departments and agencies, the intelligence community, and other elements of the law enforcement and national security communities in coordination and prioritization of cybersecurity research, standards development, standards conformance demonstration and cybersecurity education and outreach activities. Research activities range from innovations in identity management and verification, to metrics for complex systems, to development of practical and secure cryptography in a quantum computing environment, to automation of discovery and maintenance of system security configurations and status, to techniques for specification and automation of access authorization in line with many different kinds of access policies.

NIST addresses cybersecurity challenges throughout the information and communications infrastructure through its cross-community engagements. Enabled by Congressional funding increases in 2002 and in response to FISMA legislation, NIST is responsible for establishing and updating, on a recurring basis, the Federal Government risk management framework and cybersecurity controls. The national security community, a number of State governments and major private sector organizations are also adopting the risk management framework and cybersecurity controls designed by NIST. NIST is engaging industry to harmonize product assurance requirements to align with industry business models and system development practices. NIST is also playing a leading security role in supply chain risk management, health care information technology (HCIT), the Smart Grid, biometrics/face authentication, next generation voting systems, and cloud computing. NIST is working with the intelligence and counterterrorism communities to facilitate cross sector information sharing among Federal, State and local government organizations. NIST teams with the Department of Justice and the Small Business Administration in extending cybersecurity education and training beyond the Federal Government into the private sector.

Recognizing the importance of security-related standards beyond the Federal Government, NIST leads national and international consensus standards activities in

cryptography, biometrics, electronic credentialing, secure network protocols, software and systems reliability, and security conformance testing.

Under the provisions of the *National Technology Transfer and Advancement Act* (P.L. 104–113) and OMB Circular A–119, NIST is tasked with the key role of encouraging and coordinating federal agency use of voluntary consensus standards and participation in the development of relevant standards, as well as promoting coordination between the public and private sectors in the development of standards and in conformity assessment activities. NIST works with other agencies to coordinate standards issues and priorities with the private sector through consensus standards organizations such as the American National Standards Institute (ANSI), the International Organization for Standardization (ISO), the Institute of Electrical and Electronic Engineers (IEEE), the Internet Engineering Task Force (IETF), and the International Telecommunication Union (ITU).

Key contributions NIST has made include:

- Development of the current federal cryptographic and cybersecurity assurance standards that have been adopted by many State governments, national governments, and much of industry;
- Development of the identity credentialing and management standard for federal employees and contractors (also becoming the de facto national standard);
- Development of the standard and conformance test capability for inter-operable multi-vendor fingerprint minutia capture and verification;
- Development and demonstration of quantum key distribution;
- Establishment of a national cyber vulnerability database; and
- Establishment and oversight of an international cryptographic algorithm and module validation program. (This Cryptographic Module Validation Program (CMVP) achieved a significant milestone on August 15, 2008, by issuing the program's 1,000th certificate.)

NIST hosts the Information Security Automation Program (ISAP), which formalizes and advances efforts to enable the automation and standardization of technical security operations, including automated vulnerability management and policy compliance evaluations. The NIST National Vulnerability Database (NVD) is the United States Government repository of standards-based vulnerability management reference data. The NVD makes available information on vulnerabilities, impact measurements, detection techniques, and remediation assistance. It provides reference data that enable the ISAP's security automation capabilities. NIST's security automation program is based on the NIST Security Checklist program and the Security Content Automation Protocol (SCAP) activity. The SCAP Validation Program performs conformance testing to ensure that products correctly implement SCAP. NVD also plays a pivotal role in the Payment Card Industry (PCI) in their efforts to mitigate vulnerabilities in credit card systems. The PCI has mandated that NVD's vulnerability severity scores be used for measuring the risk to payment card servers world-wide and for determining which vulnerabilities must be fixed.

Included in the scope of NIST cybersecurity activities are the usability of systems such as voting machines and software interfaces; research in mathematical foundations to determine the security of information systems; the National Software Reference Library, computer forensics tool testing, software assurance metrics, tools, and evaluation; approaches to balancing safety, security, reliability, and performance in SCADA and other Industrial Control Systems used in manufacturing and other critical infrastructure industries; technologies for detection of anomalous behavior, quarantines; standards, modeling, and measurement to achieve end-to-end security over heterogeneous, multi-domain networks; biometrics evaluation, usability, and standards (fingerprint, face, iris, voice/speaker, multi-modal biometrics) and initiating an international competition for a next generation Secure Hash Algorithm (SHA–3). NIST and the National Science Foundation are co-funding a workshop in July on usability issues associated with security. Among the topics to be investigated are methods to inform individual users of actions they take that could imperil their systems also providing informative justifications, methods and tools to assist administrators of systems in the configuration of their systems to provide secure operation, and forensic tools to help administrators deal with the aftermath of attacks.

Recognizing the value of interagency coordination of research as well as of standards development, NIST actively contributes to the Networking and Information Technology Research and Development (NITRD) program and the development of the NITRD five-year strategic plan. Within the past year, as provided in the *America COMPETES Act* (P.L. 110–69), the NITRD Program has assumed expanded re-

sponsibilities for coordination of federal cyber R&D and NIST is well represented in, and leverages, these activities. In addition, NIST collaborates with academia, e.g., individual institutions such as Purdue, and consortia, such as the Institute for Information Infrastructure Protection (or I3P).

NIST works with other members of the Cyber Security and Information Assurance Interagency Working Group in establishing priorities for research and development to prevent, resist, detect, respond to, and/or recover from actions that compromise or threaten to compromise the availability, integrity, or confidentiality of computer- and network-based systems. These systems provide both the basic infrastructure and advanced communications in every sector of the economy, including critical infrastructures such as power grids, emergency communications systems, financial systems, and air-traffic-control networks. These systems also support national defense, national and homeland security, and other vital federal missions, and themselves constitute critical elements of the IT infrastructure. Broad areas of concern which NIST research addresses include Internet and network security; confidentiality, availability, and integrity of information and computer-based systems; new approaches to achieving hardware and software security; testing and assessment of computer-based systems security; and reconstitution and recovery of computer-based systems and data.

60–Day Cyberspace Policy Review

We concur in the findings of the 60–Day Cyber Review relative to the increasingly serious and pervasive threat posed by breaches of—or threats to—our cyber systems, and relative to the need to strengthen the capability of the Executive Office of the President to coordinate the Federal Government's response to that threat. We also concur in the report's observation that it is our total national information infrastructure, not just the federal information infrastructure that is faced with the aforementioned threat. We agree that a coordinated response is necessary to prevent catastrophic consequences for those critical infrastructures which integrate information systems into their operations.

While agreeing that it is necessary to integrate the responses of national security organizations and those of federal organizations that do not have a primarily national security mission, we observe that the intelligence community, the other elements of the national security community, and NIST are, in response to the *Federal Information Security Management Act of 2002*, actively coordinating their standards and processes for cybersecurity. This effort is producing a single set of requirements, rather than the past's three independent sets of requirements (Intelligence community, national security systems and NIST) for consumers and providers of information processing and interchanges resources.

On June 3rd, NIST announced the release of the final public draft of Special Publication 800–53, Revision 3, Recommended Security Controls for Federal Information Systems and Organizations. The final public draft of Special Publication 800–53, Revision 3, is historic in nature.

For the first time, and as part of the ongoing initiative to develop a unified information security framework for the Federal Government and its contractors, NIST has included security controls in its catalog for both national security and non-national security systems. The updated security control catalog incorporates best practices in information security from the United States Department of Defense, Intelligence Community, and civil agencies, to produce the most broad-based and comprehensive set of safeguards and countermeasures ever developed for information systems.

We are encouraged to observe that the 60–Day Cyberspace Policy Review recognizes that cybersecurity strategies and solutions must be structured in a manner that accommodates commerce, economic growth, scientific collaboration, and individual liberties. The report reflects the notion that we are not looking for "lockdown solutions" that achieve security at the expense of robust commerce, essential services or civil liberties.

Recognizing the economic impact of cyberspace, NIST is working to provide measurement techniques to facilitate offsetting the cost of both public sector and private sector security solutions by decreases in losses or cost of insurance or increases in business due to increases in trust. Meeting the cyber threat to our national infrastructure would be accelerated by both the public and private sectors if new measurement techniques can demonstrate that increased security is good business sense. We note that not all of these measures need to be technical or regulatory in nature. Some simple, relatively inexpensive, procedural steps can have a materially positive effect on security. One example is the financial sector's having introduced a delay into the conversion of electronically transferred funds into tangible assets, a delay sufficient to permit invocation of fraud detection processes.

We were particularly encouraged by the report's recognition of the role of international standards in protecting our information infrastructure. Our infrastructure is inextricably integrated into a complex of global networks. NIST's role in documentary standards has long been established in law and executive direction. We are actively working with our sister agencies on improving our common understanding of how we can collectively participate, in cooperation with the private sector, in fostering international standards and protocols that are conducive to a free and safe information processing and interchange environment.

NIST and the National Telecommunications and Information Administration (NTIA) are working with the Internet Corporation for Assigned Names and Numbers (ICANN) and VeriSign on an initiative to enhance the security and stability of the Internet. The parties are working on an interim approach to deployment, by year's end, of a security technology—Domain Name System Security Extensions (DNSSEC)—at the authoritative root zone (i.e., the address book) of the Internet. There will be further consultations with the Internet technical community as the testing and implementation plans are developed. In collaboration with the Department of Homeland Security Science and Technology Directorate, NIST has been an active participant within the international community in developing the DNSSEC protocols and has collaborated with various U.S. agencies in deploying DNSSEC within the .gov domain.

We, at the NIST and the larger Department of Commerce, recognize that we have an essential role to play in realizing the vision set forth in the 60–Day Cyberspace Policy Review. We look forward to working with our Federal Government partners, with our private sector collaborators, and with our international colleagues to establish a comprehensive set of technical solutions, standards, guidelines, and procedural measures necessary to realizing this vision.

Conclusion

NIST will continue to conduct the research necessary to enable and to provide cybersecurity specifications, standards, assurance processes, training and technical expertise needed for securing the U.S. Government and critical infrastructure information systems to mitigate the growing threat. NIST will continue to closely coordinate with domestic and international private sector cybersecurity programs and national security organizations. Finally, consistent with the NIST Three-Year Planning Report, NIST plans to expand its focus on cybersecurity challenges associated with health care IT, the Smart Grid, automation of federal systems security conformance and status determination, and cybersecurity leap-ahead research.

Thank you for the opportunity to testify today on NIST's work in the cybersecurity arena and our views on the President's 60–Day Cyberspace Policy Review. I would be happy to answer any questions you may have.

BIOGRAPHY FOR CITA M. FURLANI

Cita M. Furlani is Director of the Information Technology Laboratory (ITL). ITL is one of nine research Laboratories within the National Institute of Standards and Technology (NIST) with an annual budget of $85 million, 335 employees, and about 150 guest researchers from industry, universities, and foreign laboratories.

Furlani oversees a research program designed to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology through research and development in information technology, mathematics, and statistics. Through its efforts, ITL seeks to enhance productivity and public safety, facilitate trade, and improve the quality of life.

Furlani has several leadership responsibilities in addition to those at NIST. Currently, she is Co-Chair of the Interagency Working Group on Digital Data, Co-Chair of the Subcommittee on Quantum Information Science, and Co-Chair for Strategic Planning for the Subcommittee on Networking and Information Technology Research and Development, all under the auspices of the National Science and Technology Council. She also serves as Co-Chair of the Technology Infrastructure Subcommittee of the Interagency CIO Council.

Furlani has served as the Chief Information Officer (CIO) for NIST. As CIO, Furlani was the principal adviser to the NIST Director on the planning, execution, evaluation, and delivery of information technology services and support.

Furlani also served as Director of the National Coordination Office for Networking and Information Technology Research and Development. This office, reporting to the White House through the Office of Science and Technology Policy and the National Science and Technology Council, coordinates the planning, budget, and assessment activities for the 12-agency Networking and Information Technology R&D Program.

Previously, Furlani was Director of the Information Technology and Electronics Office within the Advanced Technology Program (ATP) at NIST. Before joining ATP, Furlani served as Chief of the Office of Enterprise Integration, ITL, NIST, coordinating Department of Commerce activities in the area of enterprise integration. Furlani also served as special assistant to the NIST Director in the Director's role as Chair of the Committee on Applications and Technology of the Administration's Information Infrastructure Task Force. Previously, Furlani was on detail as technical staff to the Director of NIST in the position of Senior Program Analyst. Prior to August 1992, she managed research and development programs within the NIST Manufacturing Engineering Laboratory, applying information technology to manufacturing since 1981.

She earned a Master of Science degree in electronics and computer engineering from George Mason University and a Bachelor of Arts degree in physics and mathematics from Texas Christian University. She was awarded two Department of Commerce Bronze Medal Awards in 1985 and 1993 and the Department of Commerce Silver Medal Award, in 1995.

Chairman WU. Thank you, Ms. Furlani. Dr. Wing, please proceed.

STATEMENT OF DR. JEANNETTE M. WING, ASSISTANT DIRECTOR, COMPUTER AND INFORMATION SCIENCE AND ENGINEERING DIRECTORATE, NATIONAL SCIENCE FOUNDATION (NSF)

Dr. WING. Thank you very much. Good afternoon, Chairman Wu and Chairman Lipinski, Ranking Members Smith and Ehlers, and Members of the Subcommittees. I am Jeannette Wing, and I am the Assistant Director of the Computer and Information Science and Engineering Directorate at the National Science Foundation.

I am delighted to have the opportunity to speak with you today about NSF's support for cybersecurity research at the frontiers of knowledge, investments that capitalize on the intellectual capacity of the best and the brightest in our nation's colleges and universities, as well as their many partners in the private sector. The research outcomes generated with NSF support will undoubtedly contribute to the security, stability and integrity of our global cyber infrastructure for many years to come.

To begin, I would like to emphasize that many cybersecurity measures deployed today build upon the fundamental research outcomes generated decades ago. Thus, as the recent 60-Day Cyberspace Policy Review concludes, a national strategy to secure cyberspace in both the near- and the long-term must include investments in fundamental, unclassified, long-term research.

Allow me to share with you just a few important fundamental research contributions made to date by the open research community, many originally developed with applications other than security in mind.

Cryptographic schemes and cryptographic-based authentication, enabling today's Internet commerce, such as online banking.

Program analyses and verification techniques, enables early detection of software vulnerabilities, thereby often preventing cyber attacks such as phishing, worms and botnets.

Machine learning and data mining approaches are now used in filtering spam and detecting credit card fraud.

CAPTCHAs, the distorted text that only humans, not machines, can decipher, ensuring that it is indeed a human, not a bot, who is buying a ticket online.

These and many other research results developed with NSF funding are being used routinely in numerous corporations today. Moreover, NSF-funded projects have spawned start-up companies that bring critical technologies to the marketplace, creating new jobs, expanding the economy, and helping to secure cyberspace.

This year, NSF will invest almost $137 million in cutting-edge research on the science and engineering of trustworthy systems. Our interdisciplinary Trustworthy Computing Program, is a significant component of this investment and supports more than 800 principal investigators, co-principal investigators, and graduate students.

We contribute to the Comprehensive National Cyber Security Initiative, CNCI, through this program with the focus on three vital areas, the scientific foundations of trustworthiness, privacy, and usability.

NSF coordinates its cybersecurity research and planning activities with other agencies primarily through the Networking and Information Technology Research and Development program, NITRD, and the InfoSec Research Council. We play a leadership role in both activities.

NSF and the academic community greatly appreciated the opportunity to contribute to the 60-Day Cyberspace Policy Review. We are pleased that the review recognizes the importance of investments in both fundamental unclassified cybersecurity research, the kind of research NSF supports, and cybersecurity education. The review also recognizes the importance of a strong academia-industry-government partnership in which NSF plays a central enabling role.

For example, the NSF Science and Technology Center, called TRUST, and three Cyber TRUST Centers, all work directly with industry partners to speed the transition of research outcomes into products and services.

Looking ahead, there are several areas ripe for industry-university collaboration. First, industry has data that are otherwise unavailable to academics. Providing access to real data, appropriately sanitized, anonymized, and scrubbed, based on real adversaries and real users of operational systems and networks will allow researchers to test their theories and to gain new insights.

Second, industry has problems looming on the horizon that they just don't have time to solve or they can't even imagine because they are so focused on the present. These are exactly the kinds of problems academic researchers can work on, anticipating the threats of tomorrow so that when they arrive, solutions will be ready.

In my testimony today, I have provided examples of the ways in which NSF works with its partners in the Federal Government, the private sector, and academe to catalyze research advances in cybersecurity.

With robust sustained support for research in both the executive and legislative branches, we have a unique opportunity to increase our nation's investments in fundamental, open, long-term cybersecurity research. Investing now for the future means a more secure future.

This concludes my remarks. Thank you very much.

VerDate 11-MAY-2000 11:39 Jan 29, 2010 Jkt 050171 PO 00000 Frm 00028 Fmt 6633 Sfmt 6601 C:\DWORK\T&I09\061609\50171 SCIENCE1 PsN: SCIENCE1

[The prepared statement of Dr. Wing follows:]

PREPARED STATEMENT OF JEANNETTE M. WING

Good afternoon, Chairman Wu and Chairman Lipinski, Ranking Members Smith and Ehlers, and Members of the Subcommittees. I am Jeannette Wing, and I am the Assistant Director of the Computer and Information Science and Engineering Directorate at the National Science Foundation.

I am delighted to have the opportunity to talk with you today about NSF's support for cybersecurity research at the frontiers of knowledge—investments that capitalize on the intellectual capacity of the best and the brightest in our nation's colleges and universities, as well as their many partners in the private sector. The research outcomes generated with NSF support will undoubtedly contribute to the security, stability and integrity of our global cyberinfrastructure for many years to come.

To begin, it is essential that I note that many cybersecurity measures deployed today capitalize on fundamental research outcomes generated decades ago. Thus, as the recent 60-Day Cyberspace Policy Review concludes, a national strategy to secure cyberspace in both the near- and the long-term must include investments in fundamental, unclassified, open, long-term research. Investments in such research will allow our society to continue to benefit from a robust, secure, dependable cyberinfrastructure that supports all application sectors, including those on which our lives depend.

Allow me to share with you just a few important fundamental research contributions made to date by the open research community, many developed with applications other than security in mind and long before situations arose that demanded their use.

The basic research community developed:

- Cryptographic schemes and cryptographic-based authentication, enabling today's Internet commerce, supporting secure digital signatures and online credit card transactions, and providing some of the building blocks needed for the safe, secure and private exchange of electronic health records;
- Program analyses and verification techniques, enabling the early detection of software vulnerabilities and flaws, thereby often preventing cyber attacks such as phishing, worms and botnets;
- Innovative machine learning and data mining approaches now used in spam filtering, and methods for detecting attacks such as those involving credit card fraud; and the final example,
- CAPTCHAs, the distorted text that only humans—not machines or hots—can decipher, to ensure that it is indeed a human, and not a bot, who is buying a ticket online or setting up an e-mail account.

These research outcomes and many others developed with NSF funding are being used in numerous corporations including Amazon, Apple, e-Bay, Google, Intel, Microsoft, and Yahoo!. Moreover, NSF-funded projects have spawned start-up companies that bring critical technologies to the marketplace, creating new jobs, expanding the economy, and helping to secure cyberspace.

Please summarize the current range of National Science Foundation supported cybersecurity research, including associated funding.

NSF has been investing in cybersecurity research for many years.[1] In FY 2009, we will invest almost $137 million in fundamental research in the science of trustworthiness and related trustworthy systems and technologies. This includes $20 million from the *American Recovery and Reinvestment Act*. Approximately one half of this $137 million is allocated to our interdisciplinary Trustworthy Computing program, which in FY 2009 is funded at a level of $65 million and supports more than 800 principal investigators, co-principal investigators, and graduate students. In addition to the Trustworthy Computing program, we continue to make cybersecurity investments in the core scientific sub-disciplines of the computing and human sciences, including the foundations of communications and information, networking technology and systems, algorithmic foundations, information integration and informatics, and in the social and economic implications of developing secure, trustworthy systems.

[1] FY 2005: $68.81M, FY 2006: $76.73M, FY 2007: $96.70M, FY 2008: $106.90M, FY 2009 estimate: $136.70M (including $20M ARRA), FY 2010 Request: $126.70M

The totality of NSF investments supports a broad range of topics in trustworthy systems and applications. NSF supports foundational research in: cryptography, including key management, conditional and revocable anonymity; defense mechanisms against large-scale attacks such as worms, viruses, and distributed denial of service; formal models and methods for specifying, verifying, and analyzing system security; hardware enhancements for security, such as virtualization and trusted platform modules; metrics, especially for risk-based measurement; privacy, including privacy-preserving data-mining, location privacy, and privacy in RFID networks; network security, including for wireless and sensor networks and pervasive computing; and testbeds to run scalable experiments and to analyze anonymized network traffic data. NSF-funded research also addresses cybersecurity in the context of many application areas, including critical infrastructure (including the power grid), health records, voice over IP, geospatial databases, digital media, electronic voting, and federated systems.

The relentless pace of innovation in information technology and related services leads inevitably to new research questions, opportunities and challenges. For example, increasing interest in "cloud computing" leads to new opportunities but also raises new research challenges in security and privacy, and innovations in service-oriented architectures raise new research challenges in resiliency and verification. In the longer-term, new computing paradigms such as quantum computing will raise new research questions in cryptography and computational complexity.

As you may know, FY 2009 represents the first full year of the interagency Comprehensive National Cybersecurity Initiative—CNCI. NSF's contributions to the CNCI include a specific focus on three critical areas:

- The scientific foundations of trustworthiness, so that new trustworthy systems, technologies, and tools can be developed and understood from first principles. New models, logics, algorithms, and theories are being explored for analyzing and reasoning about all aspects of trustworthiness—security, privacy, reliability, and usability—about all communication, control, and data components of systems and their composition. Researchers are exploring the fundamentals of cryptography, inventing new specification and programming languages and techniques to prevent or detect security vulnerabilities in software and hardware, defining new security architectures for system design, and exploring new computing models that have potential to improve trustworthiness and our ability to reason with different aspects of trustworthiness.
- The essential systems property of protecting privacy. NSF is supporting the exploration of new scientific and computational models, methods, logics, algorithms, and software tools to define and reason about privacy, to detect and resolve conflicts among privacy policies, to safeguard information of individuals wherever it may digitally reside, and to explore the interplay among privacy, security and legal policies. One major technical challenge is identity management, especially for federated systems that may be beyond the control of any one organization; academic researchers are exploring attack-resistant methods and protocols for identity management, commensurate with application requirements to preserve privacy and with security and legal requirements to provide accountability.
- Usability—the methods, tools and techniques that make it easy for people to use computing systems while protecting both people and systems from unforeseeable attacks on their security and privacy. Users range from individuals concerned about their home computers to administrators responsible for large enterprises. Incorporating trustworthiness into a system should not place undue demands on human users or impact human or system performance. Since people can be the weakest link in security, striking a balance between control and convenience is a key challenge. Researchers are developing new approaches to integrating and balancing different system functionalities, understanding human perception of trust including privacy, informing users of potential pitfalls, and predicting the impact of user decisions. New methods are needed, supported by automation, to promote usability and provide users with security controls they can understand. An especially active area of research is digital forensics, where new automated methods will help all users respond effectively in the aftermath of a security incident.

How is NSF coordinating its own cybersecurity research and planning activities with other relevant federal agencies?

At NSF, we coordinate our cybersecurity research and planning activities with other federal agencies, including the Departments of Defense (DOD) and Homeland

Security (DHS) and the agencies of the Intelligence Community, through the following "mission-bridging" activities:

- NSF plays a leadership role in the interagency Networking and Information Technology Research and Development (NITRD) Program. The National Science and Technology Council's NITRD Sub-Committee, of which I am Co-Chair, has played a prominent role in the coordination of the Federal Government's cybersecurity research investments. For example,
  - The NITRD Senior Steering Group (SSG) for Cyber Security is overseeing the unclassified research and development component of the CNCI. We recently established the National Cyber Leap Year during which we asked our research leaders in government, academia, and industry, to propose "game-changing" concepts for securing cyberspace. Our next step is to hold focused meetings with the community to pursue some of the more promising ideas, toward an integrated private-public approach that considers technical, social, and economic factors in cybersecurity. This work is immediately responsive to one of the near-term action recommendations published recently in the 60-Day Cyberspace Policy Review.
  - The NITRD CyberSecurity and Information Assurance Interagency Working Group (CSIA IWG) coordinates cybersecurity and information assurance research and development across the thirteen member agencies, including DOD, the Department of Energy (DOE) and the National Security Agency (NSA). In 2006, the CSIA IWG published a national research and development agenda for strengthening the security of the Nation's cyberinfrastructure. This report continues to inform our investments today.
- NSF also plays a leadership role in the multi-agency Infosec Research Council (IRC), whose members include the DOD, agencies representing the Intelligence Community and a number of other federal agencies and entities (e.g., DOE, National Institute of Standards and Technology, and National Library of Medicine). The IRC provides a forum for the discussion of critical scientific and technical issues in cybersecurity, serves as a catalyst for the establishment of new programs and technical emphases, and helps minimize duplication of effort. In the past several years, IRC members have hosted a number of academic-industry-government workshops, such as the recent workshop on the Science of Security Workshop, which identified new principles and methodologies in support of a more foundational approach to security. This workshop was co-funded by NSF, the Intelligence Advanced Research Project Activity (IARPA), and NSA.

These and other interagency settings, both formal and informal, provide a range of opportunities for interagency coordination and collaboration.

In particular, how is NSF coordinating its (unclassified) research and planning activities with Department of Defense or other federal classified research and research infrastructure, including cyber test beds?

Jointly sponsoring workshops, such as the one I just cited, is representative of the types of interactions that take place between agencies supporting classified and/or unclassified components of the federal cybersecurity research portfolio. There is, of course, a rather significant classified component in the CNCI. Coordination between the larger classified component and the more modest unclassified component is achieved through the engagement of individuals who participate in both. These individuals share and promulgate knowledge generated in the unclassified component with those participating in the classified component.

Through some of the coordinating mechanisms I have just described, NSF also works with its sister agencies in the deployment of cybersecurity testbeds. For example, the cyber-*DE*fense *T*echnology *E*xperimental *R*esearch Environment project (DETER)—a testbed that supports research on next-generation cybersecurity technologies—has been supported jointly by DHS and NSF. In another example, the Wisconsin Advanced Internet Laboratory (WAIL), which is supported by NSF, the Defense Advanced Research Project Agency (DARPA)[2] and DHS, allows networking and distributed systems researchers to recreate end-to-end instances of the real Internet, thereby permitting realistic network testing in support of security. As we

[2] DARPA does not provide funding for the Wisconsin Advanced Internet Laboratory as indicated in the written testimony. NSF noted this error on June 19, 2009.

look to the future, the DARPA National Cyber Range (NCR) is envisioned as a testbed that will allow researchers to perform qualitative and quantitative assessments of the security of cyber technologies and scenarios. Among the many experimental testbeds that have been developed, DARPA is considering DETER and WAIL as starting points for the NCR—demonstrating the value of "mission-bridging" from NSF's basic research mission to the quite focused application needs of other agencies. If the NCR is opened to unclassified research, then NSF would welcome the opportunity to coordinate with DARPA to provide academic researchers with an opportunity to run their experiments on this testbed.

What changes, if any, does NSF plan to make to its research portfolio, planning, or interagency coordination efforts in response to the findings and recommendations in the Administration's 60-day federal cybersecurity review?

NSF and the academic community very much appreciated the opportunity to contribute to the 60-day Cyberspace Policy Review. As I stated in my opening remarks, the Review clearly recognizes the importance of investments in fundamental, unclassified research, in support of which NSF plays a significant role.

The Review also recognizes the importance of cybersecurity education. Besides our support of research, NSF plays an increasingly important role in the preparation of current and future generations of computing professionals and of a scientifically-literate national workforce. We are grateful that the Review recognizes the important role of several of our education programs, most notably the Pathways to Revitalized Undergraduate Education in Computing, and the Scholarships for Service programs.

NSF's current portfolio of investments spans the many important topics highlighted in the Review. Further, our interdisciplinary reach to the broad academic community, and beyond into the private sector, provides an unparalleled opportunity to establish bold, new "game-changing" directions in long-term cybersecurity research that are informed both by social and economic needs and by national security requirements. Our aspirations for the Trustworthy Computing program, which takes a holistic, interdisciplinary approach to establishing the science of trustworthiness and its embodiment in the engineering of trustworthy computing systems and technologies, are consistent with the review's recommendations.

NSF will continue to support interagency workshops that promote interagency collaboration and coordination. Workshops are planned on how to measure success in security-related research activities, on developing metrics to assess the security and privacy of complex systems, and on how to achieve security in the financial infrastructure. This last workshop will be coordinated with the Department of the Treasury.

NSF and its many partners in academe, industry, and government stand ready to respond to the national imperative to secure cyberspace, both today and for the foreseeable future. We welcome the opportunity to collaborate with our partners in creating a comprehensive response to the recommendations expressed in the review.

To what extent is NSF's cybersecurity research portfolio shaped by the cybersecurity needs and related research priorities of the private sector? How is NSF soliciting input from the private sector regarding its research portfolio?

In the academia-industry-government ecosystem, organizations and individuals in all three sectors bear a responsibility for shaping a future cyberinfrastructure that is usable, secure, dependable, and resistant to attack, for the benefit of science, our economy, and our society. The recent Cyberspace Policy Review clearly recognizes the value of a healthy academia-industry-government ecosystem in strengthening our nation's cybersecurity posture.

At a strategic level, NSF's research investments are shaped by advice provided by private sector representatives serving on the National Science Board and NSF Advisory Committees.

NSF also catalyzes the formation of strong partnerships between academia and the private sector by providing programmatic incentives that encourage both sectors to work together, thereby speeding the transition of research and education outcomes into products and services. For example, the NSF Team for Research in Ubiquitous Security Technology (TRUST) Science and Technology Center works with a number of industry partners who 1). help define the Center's strategic intent and research and education priorities through the Center's External Advisory Board, and 2). interact directly with faculty and students on individual research projects. Industry partners include Cisco, Deloitte and Touche, eBay, GE, HP, ING, Intel,

Microsoft, Nortel Networks, Oracle, Qualcom, Raytheon, Silicon Valley Bank, Sun Microsystems, Symantec, and Visa.

NSF's Cyber Trust program also supports three Centers with strong industry partnerships. For example, the Trustworthy Cyber Infrastructure for the Power grid (TCIP) center, which also receives support from DHS and DOE, works with its industry partners to create cybersecurity research advances that will make the Nation's power grid more secure, reliable and safe. Industry and other partners in this venture include ABB, Amerren, Areva, California ISO, Cisco, Entergy, EPRI, Exelon, GE, Gerhrs, Instep, ISIsoft, Kema, Multili, Open Systems International, Pacific Northwest National Laboratory, Power World Corporation, Siemens, and Starthis.

In addition to academic-industry partnerships encouraged through NSF programmatic incentives, many NSF-supported faculty and students have informal connections with industry, and many students in computing fields do summer internships in industry. Using these informal mechanisms, research results from NSF investments in cybersecurity also often find their way into industry products and services. For example, a team of researchers from UC–Berkeley, Stanford, and University of Maryland College Park developed an open source version of their static analysis tools for finding software vulnerabilities. These tools have been adapted by Microsoft and other large software developers and incorporated into their products.

Looking to our cybersecurity future, there are several areas ripe for industry-university collaboration. First, industry has data that are otherwise unavailable to academics. Providing access to real data—appropriately sanitized, anonymized, and otherwise scrubbed—based on real adversaries and real users of operational systems and networks is essential. This access enables researchers to test whether their theoretical ideas play out in practice. Do they scale? What are the edge cases? Furthermore, researchers gain new insights by examining real data. Patterns and anomalies emerge from looking at real data that would not from synthetic data. These discoveries in turn raise new scientific questions. Second, industry has problems looming in the horizon that they just don't have time to solve or problems they can't even imagine because they are so focused on the present; those are exactly the kinds of problems academic researchers can work on: anticipating the threats of tomorrow so that when they arrive, potential solutions will be available. Moreover, academics are freer to think out of the box and thus may come up with creative solutions that while impractical today, may be quite practical in the future.

In my testimony today, I've tried to provide examples of the ways in which NSF works with its partners in the Federal Government, in the private sector, and in academe to catalyze long-term research advances in cybersecurity. In his May 29 speech on the roll-out of the 60-day Cyberspace Policy Review, the President stated that "America's economic prosperity in the 21st century will depend on cybersecurity" and the Administration "will continue to invest in the cutting-edge research and development necessary for the innovation and discovery we need to meet the digital challenges of our time." Your Subcommittees also clearly recognize the importance of research advances in cybersecurity to the Nation's future.

With robust sustained support for fundamental research in both the executive and legislative branches, we have a unique opportunity to increase our nation's investments in fundamental cybersecurity research, thereby securing our nation's future for many decades to come.

This concludes my remarks. I would be happy to answer any questions at this time.

BIOGRAPHY FOR JEANNETTE M. WING

Dr. Jeannette M. Wing is the President's Professor of Computer Science in the Computer Science Department at Carnegie Mellon University. She received her S.B. and S.M. degrees in Electrical Engineering and Computer Science in 1979 and her Ph.D. degree in Computer Science in 1983, all from the Massachusetts Institute of Technology. Currently on leave from CMU, she is the Assistant Director of the Computer and Information Science and Engineering Directorate at the National Science Foundation.

Professor Wing's general research interests are in the areas of specification and verification, concurrent and distributed systems, programming languages, and software engineering. Her current interest is on the foundations of trustworthy computing where by trustworthy she includes reliability, security, privacy, and usability. Her current projects are on specifying and verifying privacy policies.

She has published extensively in top journals and major conferences and has given nearly 300 invited, keynote, and distinguished lectures. She was or is on the

editorial board of twelve journals, including the *Journal of the ACM* and the *Communications of the ACM*.

Professor Wing has been a member of many advisory boards, including: the Networking and Information Technology (NITRD) Technical Advisory Group to the President's Council of Advisors on Science and Technology (PCAST), the National Academies of Sciences's Computer Science and Telecommunications Board, the DARPA Information Science and Technology (ISAT) Board, NSF's CISE Advisory Committee, Microsoft's Trustworthy Computing Academic Advisory Board, the Intel Research Pittsburgh's Advisory Board, Dartmouth's Institute for Security Technology Studies Advisory Committee, and the Idaho National Laboratory and Homeland Security Strategic Advisory Committee. She was a Member-at-Large on ACM Council and served on the ACM Kanellakis Award Committee and the ACM Karlstrom Outstanding Educator Award Committee. She was on the Microsoft New Faculty Fellowship Selection Committee and the Sloan Research Fellowships Program Committee. She was the Co-Chair of the Technical Symposium of Formal Methods '99, co-organizer of the UW–MSR CMU 2003 Software Security Summer Institute, and Co-Chair of the First International Symposium on Secure Software Engineering.

Administratively at Carnegie Mellon, she served as Head of the Computer Science Department during 2004–2007, overseeing 90 faculty. She was Associate Dean for Academic Affairs for five years, overseeing the operations of the educational programs offered by the School of Computer Science, including at the time: ten doctoral programs or specializations, ten Master's programs, and the Bachelor's program. She also served as Associate Department Head for nine years, running the Ph.D. Program in Computer Science.

She was on the Computer Science faculty at the University of Southern California and has worked at Bell Laboratories, USC/Information Sciences Institute, and Xerox Palo Alto Research Laboratories. She spent sabbaticals at MIT in 1992 and at Microsoft Research 2002–2003. She has consulted for Digital Equipment Corporation, the Mellon Institute (Carnegie Mellon Research Institute), System Development Corporation, and the Jet Propulsion Laboratory. She is a member of AAAS, ACM, IEEE, Sigma Xi, Phi Beta Kappa, Tau Beta Pi, and Eta Kappa Nu. She was elected an ACM Fellow in 1998, IEEE Fellow in 2003, and AAAS Fellow in 2007.

Chairman WU. Thank you very much, Dr. Wing. Dr. Leheny, I am going to get you started, and Chairman Lipinski is going to take over for a while. Dr. Leheny, please proceed.

STATEMENT OF DR. ROBERT F. LEHENY, ACTING DIRECTOR, DEFENSE ADVANCE RESEARCH PROJECTS AGENCY (DARPA)

Dr. LEHENY. Mr. Chairman, Subcommittee Members and staff, thank you very much for this opportunity to discuss DARPA's programs, information assurance, and cybersecurity.

As I believe you are already aware, DARPA's mission is to invest in high-risk, high-reward technologies that create new capabilities for our military. And information assurance and cybersecurity are important elements in our current portfolio of programs. Let me begin today by commenting on the significance of robust secure self-forming networks to the defense department.

Like many commercial enterprises, the department is transforming to network centric operations, so DARPA's programs are focused on ensuring that these networks can operate independently in a robust and secure manner. We are interested in two types of networks, strategic high-speed optical and satellite based global networks, networks relying on commercial hardware technologies for the most part. For these types of networks, our focus is largely on operations, survivability under attack, and security.

At the other extreme are practical, largely wireless networks, networks directly supporting the war fighter on the front lines. Wireless networks present both hardware and software challenges. They must be agile and adaptive, capable of operating in any envi-

ronment, as well as be able to manage, defend, and heal themselves at speeds beyond human capabilities. And they must be self-forming without recourse to the infrastructure or cell towers of the commercial provider.

As network capabilities become ever more essential to operations, these networks above all else must be secure. We will spend about $127 million on information assurance and cybersecurity in the current fiscal year, and we are requesting an increase of more than 14 percent to $164 million for 2010. While most of these investments are targeted to software architecture and protocol issues, to ensure networks are secure from the ground up, their underlying hardware must also be secure. So in what is truly a DARPA hard problem, we are investing in a program we call TRUST, oddly enough the same name that the NSF has for one of its programs, but we are doing something completely different. What we are doing is investigating methods for detecting malicious features inserted into semiconductor chips during their design, manufacture, and programming. All of these efforts focus on the department challenges, but we believe our successes, as has been the case in the past, will eventually impact commercial network technologies as well.

At this time, perhaps our most visible program, one of particular interest to this committee which we took on as part of the Comprehensive National Cyber Initiative, is our program to develop a National Cyber Range. Recognizing that scientific progress has always been paced by advances in our ability to observe, test and perform rigorous experiments, we are designing this range to be a vehicle for a significantly advancing progress in cyber understanding and capabilities, to be a tool for rapid, realistic, and quantitative simulation assessment of cyber technologies. Researchers will be able to operate at either the classified or unclassified levels and with many more nodes than current cyber test ranges with highly automated tools and regiment techniques, they will have access to revolutionary research capabilities, capabilities that will allow rapid network simulation under real-world conditions, enabling efficient development and testing of information assurance and cybersecurity strategies.

The program has three phases. In the current first phase, we began by seeking ideas from multiple sources which after a government panel review resulted in our placing seven teams under contract to develop competing designs for delivery later this summer. At that time, the government team will evaluate and select the best among these designs to continue into a Phase II program to produce a limited number of prototype ranges. In a third phase, the most capable prototype range will be further developed into the operational range to be completed in 2012. DARPA is managing the National Cyber Range development, but we will transition the completed range to another organization for operation. The details are a work in progress. Presently two government working groups are studying the issues. One is developing a technical vision and business model for the range operations. The other is focused on security issues for accrediting the range for use by all agencies across the government. In the end, I believe the range will operate like other national research assets with a panel to review and prioritize

user proposals and an administrator to maintain facilities and facilitate research or access.

Regarding how we coordinate our research with other agencies, I can assure you that we actively coordinate our efforts. Two specific examples include the multi-agency participation in the development of the National Cyber Range, and our teaming with the NSF to organize two cybersecurity workshops this summer. But in general, in the process of developing new programs, our program managers routinely engage with their counterparts in other agencies to scope out the best way forward to achieve a specific research goal. Regarding the 60–Day Cyberspace Policy Review, this high-level document ranges over a wide variety of policy issues, but I note that it specifically recognizes the importance of innovation in achieving cybersecurity, explicitly calling out the supply chain threat which our TRUST program is addressing and the importance of modeling and simulation capabilities that the NCR will enable.

In conclusion, as the department expands its net-centric operation, information assurance remains a critical concern. In dealing with this concern, we are committed to working with organizations across the government to contribute to the national goals for a secure cyberspace, and when the new DARPA Director is in place, refining our plans, programs and budgets for cybersecurity will be high on our agenda.

I would be pleased to answer your questions.

[The prepared statement of Dr. Leheny follows:]

PREPARED STATEMENT OF ROBERT F. LEHENY

Mr. Chairman, Subcommittee Members and staff: I am Bob Leheny, Acting Director of the Defense Advanced Research Projects Agency (DARPA). I am pleased to appear before you today to discuss DARPA's ongoing work in cybersecurity, or what we in the Department of Defense (DOD) call ''information assurance.''

I'd like to set the context for my remarks today by briefly describing DARPA's mission and how we work.

DARPA's mission is to prevent technological surprise for us and to create technological surprise for our adversaries. DARPA conducts this mission by searching for revolutionary high-payoff ideas and sponsoring research projects that bridge the gap between fundamental discoveries and their military applications. Stealth aircraft, developed at DARPA more than 25 years ago, is one among many important examples of how we create technological surprise.

To understand DARPA's role in DOD's science and technology (S&T) establishment, consider an investment timeline that runs from ''near'' to ''far,'' indicative of the time required for an investment to be incorporated into an acquisition program. The ''near side'' represents investments that characterize much of the work of the Department's other S&T organizations, which tend to gravitate to the near-term because they emphasize investments in capabilities required to meet today's mission requirements. These investments are excellent S&T and are crucial to DOD because they continuously hone U.S. military capabilities, e.g., improving the efficiency of jet engines and making existing radios more reliable. This S&T is usually focused on known systems and problems.

At the other end of the investment timeline—the ''far side''—are the smaller basic research investments made by various federal agencies and the Military Services that support fundamental discoveries, where new science, ideas, and radical concepts typically first surface. Investigators working on the far side generate ideas for entirely new types of devices or new ways to put together capabilities in a revolutionary manner, but often find that obtaining funding is difficult, if not impossible.

DARPA was created to bridge the gap between these two groups. The Agency finds the people and ideas on the far side and accelerates those ideas to the near side for transition to the DOD S&T and acquisition communities as quickly as possible. DARPA's work is high-risk and high-payoff precisely because it bridges the gap between fundamental discoveries and their military use.

DARPA's success depends heavily on the freedom of its program managers to pursue the far side ideas that other S&T organizations overlook or, for a variety of reasons, decide not to consider. DARPA hires program managers for limited terms of four to six years, which ensures a steady input of new energy and ideas. Given their relatively short tenure, these program managers focus their time on quickly generating ideas and starting new programs. DARPA's senior leadership provides an overall technical vision and oversees the organizational coordination and collaboration activities required of any DOD organization, thus freeing the program managers to focus on their programs. This approach has enabled DARPA to pursue the ideas and programs that have benefited DOD for more than 50 years.

DARPA's strategy for accomplishing its mission is embodied in a set of strategic thrusts that guide its investments. The current strategic research thrusts that DARPA emphasizes today are:

- Robust, Secure, Self-Forming Networks
- Detection, Precision ID, Tracking, and Destruction of Elusive Targets
- Urban Area Operations
- Advanced Manned and Unmanned Systems
- Detection, Characterization, and Assessment of Underground Structures
- Space
- Increasing the Tooth-to-Tail Ratio
- Bio-Revolution
- Core Technologies, which span investments in quantum science and technology, bio-info-micro, materials, power and energy, microsystems, information technology, mathematics, manufacturing science and technology, and lasers.

Today, I will discuss DARPA's vision for DOD's Robust, Secure, Self-Forming Networks and the investments in information assurance to secure those networks.

Robust, Secure, Self-Forming Networks

DOD is in the middle of a transformation to network-centric operations, which has as its goal turning information superiority into a distinct advantage so U.S. forces can operate far more effectively than any adversary. Network-centric operations fuse the typically separate functions of intelligence and operations to dramatically speed up the observe-orient-decide-act (OODA) loop.

At the core of this concept are robust, secure, self-forming networks. These networks must be at least as reliable, available, secure, and survivable as the weapons and forces they connect. They must distribute huge amounts of data quickly and precisely across a battlefield, a theater, or the globe, delivering the right information at the right place at the right time. The networks must form, manage, defend and, when disrupted, heal very quickly.

Military network technology requirements are divided according to their application into either tactical or strategic networks. *Tactical networks* are largely wireless and directly support units and their equipment on the front lines. They must be agile, adaptive and versatile, and connect units and their equipment that are operating together, sometimes with different communication equipment, at local area ranges in all environments, including urban areas. *Strategic networks* are largely optical wired and/or satellite-based, are often operated by commercial suppliers, and provide broadband links between overseas command centers and the United States. Strategic networks globally link air, ground, and naval forces for operational maneuver and strategic strike and enable the distribution of knowledge, understanding, and supply throughout the force.

Network-centric operations require connectivity between the strategic and tactical echelons so they can rapidly and effectively share information. Technology advancements now provide the opportunity to connect these two families of networks. DARPA is bridging strategic and tactical operations with high-speed, high-capacity communications networks. The DOD strategic, high-speed fiber optic network—the Global Information Grid (GIG)—is an integrated network with a data rate of hundreds to thousands of megabits per second. To reach deployed elements, data on the GIG must be converted into a wireless format for reliable transmission to the various units within theater. This creates problems in the timely delivery of information.

To connect the tactical warrior to the GIG, DARPA is developing high-speed network technology that can robustly disseminate voice, video, text, and situation awareness information to the various military echelons and coalition forces. To accomplish this, the high data rate capability of optical communications is being com-

bined with the high reliability and adverse-weather performance of radio frequency (RF) communications.

The goal of DARPA's Optical RF Communications Adjunct (ORCA) program is to create a high data rate backbone network via several airborne assets that nominally fly at 25,000 feet and up to 200 kilometers apart and provide GIG services to ground elements up 50 kilometers away from any one node. ORCA provides billions of information bits per second, error-free on an optical link and, at radio frequencies, hundreds of millions of information bits per second when clouds block the optical link.

For applications at sea, DARPA is working to bridge strategic and tactical maritime operations with a revolutionary new capability for submarine communications based on a blue laser efficient enough to make submarine laser communications at depth and speed a near-term reality. If successful, it will dramatically change how submarines communicate and greatly improve their operations and effectiveness, enabling submarines to become truly persistent nodes for network-centric operations at sea.

At the tactical ground level, radio inter-operability has plagued DOD for decades. To connect tactical ground, airborne, and satellite communications platforms and terminals together, the Network-Centric Radio System (NCRS) program has developed a mobile, self-healing, ad hoc network gateway that provides total radio/network inter-operability among these platforms moving in any terrain. NCRS builds inter-operability into the network itself—rather than into each radio—allowing any radio to communicate with any other radio. Now, previously incompatible legacy tactical radios can link seamlessly among themselves and to more modern systems, including military and commercial satellite systems. DARPA is taking this technology and working on commercial components and practices to make NCRS more affordable at low rate initial production quantities. A follow-on program, Mobile Ad hoc Information Network GATEway (MAINGATE), is focused on providing this capability at a low unit cost ($60,000 each) in small volumes (1,000 units).

Another wireless challenge is frequency spectrum; it is scarce and valuable. DARPA's NeXt Generation (XG) Communications technology is making up to 10 times more spectrum available by taking advantage of spectrum assigned to others, but unused at a particular place and time. XG technology senses the spectrum being used and dynamically makes use of the spectrum that is not busy. Recently, XG conducted a series of successful experiments and demonstrations at several military locations, and various organizations within DOD are planning to transition XG technology broadly into current and existing wireless communication systems.

DARPA is developing communication networks specifically for the kind of urban environments our troops are encountering today. As is the case for civilian wireless networks, urban clutter can create multiple signals from diverse reflections (“multipath”) of the initial signal, and the result is weak or fading communications. This problem is being turned into an opportunity through the DARPA Mobile Networked Multiple-Input/Multiple-Output (MNM) program, which is actually exploiting multipath phenomena to *improve* communications between moving vehicles in cities without using a fixed communications infrastructure. MNM has demonstrated reliable non-line-of-sight communications during on-the-move field trials in urban environments. The program successfully exploited multipath to increase information throughput and reliability while maintaining high data rates. It also demonstrated reliable communications in the face of interference by enabling multiple signals to simultaneously occupy the same frequency band, resulting in increased capacity of that channel.

Building on XG, MNM, and other technologies, the Wireless Network after Next (WNaN) program is developing an affordable communication system for reaching to the “tactical edge.” The WNaN low-cost, highly capable radio will allow the military to communicate with every warfighter and every fielded device at all operational levels. WNaN technology will exploit high-volume, commercial components and manufacturing techniques so DOD can affordably evolve the capability. The radio cost will be low enough so that they can be refreshed after a few years of use with updated, more capable radios—as are today's commercial cell phones. DARPA is working with the Army to make a “low cost hand-held networking radio” for about $500 apiece a reality. In fact, we recently signed a memorandum of agreement that could lead to the Army buying large numbers of units for military use.

Information Assurance for DOD Networks

The vision for DOD's networks covers great scope and depth, starting with the building blocks of component hardware and software, ranging from smaller networks for individual systems and tactical use to huge global networks; from wired to wireless; from mobile to fixed; and many combinations in between. These networks give the U.S. military significant advantages, which make them a very attrac-

tive, high value target for any adversary. The United States must assume its adversaries will seek ways to destroy, disrupt, distort, or infiltrate DOD's networks.

Those networks must be reliable in any environment for extended periods and protected against cyber threats. As technologies are developed and deployed to successfully block overt cyber attacks, adversaries will likely attempt to insert malicious code to disrupt the networks. DOD, with some of the most sophisticated and complex networks and facing the most sophisticated attacks, must rigorously protect its networks or suffer terrible consequences. The ever-growing sophistication of these threats has surpassed the ability of current commercial markets to provide DOD with rapid and robust solutions.

While many threats and problems are common to most types of networks—private, civilian government, and military—and many private and non-DOD researchers are addressing them, DARPA's efforts are focused on technologies to solve the Defense Department's information assurance operational challenges. Funding for our information assurance research is primarily contained in two places in our budget: an applied research budget project called "Information Assurance and Reliability" and a program element called "Cyber Security Initiative," which covers the National Cyber Range. The total in these for FY09 is about $127M, and we are requesting about $164M in FY10. The details on these requests may be found in our budget, which is available online at *www.darpa.mil/budget.html*.

Critical to DOD's transformation to network-centric operations are the wireless networks known as Mobile Ad Hoc NETworks (MANETs), which are designed to fluidly and automatically connect moving vehicles and dismounts as needed without a static network infrastructure. A rough analogy is a cell phone network made up *only* of cell phones—without cell towers or a telephone company. For example, a television ad for a telecommunications company shows a large crowd of people standing behind its network. MANETs must operate without this support, yet remain fully functional networks while being vigorously attacked.

The DARPA Intrinsically Assurable Mobile Ad Hoc Network (IAMANET) program is aimed directly at building DOD MANETs that are secure from the ground up. IAMANET is developing network architectures and protocols to authenticate and authorize all traffic on a MANET, quarantine problems so they don't spread, and prevent data from corruption and unauthorized exfiltration. In contrast, the current Internet does not deny unauthorized traffic by default and violates the "principle of least privilege," where a user is given no more privilege than required to perform a given task. Existing protocols are not resistant to malicious acts that can produce faulty outputs and inconsistent behavior. IAMANET technology will provide a smart router technology for ad hoc network environments that will not forward malicious traffic, preventing infections from spreading through the network and securing information within the network.

IAMANET builds on earlier DARPA research from the Dynamic Quarantine of Worms (DQW) program. DQW technology creates an integrated system that automatically detects and responds to worm-based attacks against military networks, provides advanced warning to other DOD networks, studies and determines the worm's propagation, and automatically immunizes the network against these worms. The system quickly quarantines so-called "zero-day worms" to limit the number of machines affected and restores the infected machines to an uncontaminated state in minutes, rather than hours and days. The Marines are now conducting tests of DQW-protected systems.

MANETs are of such significance to DOD that DARPA is sponsoring basic research to develop Information Theory for Mobile Ad Hoc Networks (ITMANET) to provide a more powerful theory for mobile wireless networks. The ITMANET program is motivated in part by a major scientific accomplishment of the last century: Claude Shannon's information theory, which provides a mathematical foundation for understanding information capacity in wired, point-to-point networks. This theory is an essential foundation for today's information revolution, but is incomplete when dealing with wireless MANETs. ITMANET is extending Shannon's classic description of information capacity to the more complex mobile ad hoc network case. Stanford University and the University of Texas are leading two research teams in this effort, which involves 24 faculty members from several universities. Important program results are being reported in peer-reviewed professional journals, and, based on this research, a popular science magazine is planning a tutorial article on MANETs to popularize the concepts among a wider audience. While this work may not seem to be strictly information assurance, DARPA researchers believe it will help us understand the limits of what can and cannot be done in MANETs and inform the design of MANETs that are more secure.

DARPA's information assurance programs for wired networks will likely yield results that could be useful to a wide range of users beyond DOD.

The Trustworthy Systems program is developing innovative methods to detect unusual traffic in networks. These methods promise to be orders of magnitude more effective than traditional approaches by leveraging recent advances in statistical physics, information theory, and thermodynamics. The goal is to detect 99 percent of attacks launched with no more than a single false alarm per day—all at gateway speeds, in the gigabits-per-second range.

The Self-Regenerative Systems (SRS) program is developing techniques to allow networks to work through attacks and automatically adjust themselves to provide critical functions in the presence of attacks. Over time, SRS will "learn" their own vulnerabilities and how to correct them, even protecting against incorrect or improper actions by authorized users. Started in 2004, the SRS program involves several universities and research firms and is advancing four key cyber defense technologies: automated software diversity, scalable redundancy, insider threat mitigation, and self-healing. The current phase of the program will move SRS technologies from the laboratory to an actual DOD system to show that the system can automatically heal itself from expert attack, while maintaining a viable level of service.

The DARPA Application Communities (AC) program is building an automatic cyber defense infrastructure for large deployments of similar applications in many places, for example, the same web browser running simultaneously on many separate computers. As a network comes under attack, continued comparison across the network permits the online construction of a universal software patch for all affected machines. The core technology for the AC program was developed at MIT and will be demonstrated in the current phase of the program in conjunction with MIT's commercial partner.

All networks rely on hardware, and to work properly that hardware must be secure. With much of the microelectronics used in DOD and other systems manufactured off-shore, the question naturally arises, "How do we know we are getting what we asked for in the microelectronics and *only* what we asked for?" The integrity of the hardware components is commonly not addressed when considering cybersecurity and networks, but it is a key issue in DOD information assurance. To the extent DOD systems use microelectronics purchased from several vendors, including foreign sources, they are at risk.

DARPA's Trusted, Uncompromised Semiconductor Technology (TRUST) program, a major information assurance program, is directly tackling this issue. Pursuing a series of complementary technologies and techniques to ensure that DOD's microelectronics will do only what they are supposed to do and nothing more, TRUST program research addresses the full production cycle of microelectronics, including design and fabrication. The program is studying ways to determine whether malicious features have been inserted during the design or fabrication of application-specific integrated circuits or during the programming of field programmable gate arrays. DARPA is at the forefront of research in this area, confronting these issues in a comprehensive manner for the first time with expected results that will enhance and ensure the trustworthiness of microelectronics—regardless of where they have been manufactured.

National Cyber Range

DARPA's most prominent information assurance program is the National Cyber Range (NCR) project, which is part of the Comprehensive National Cybersecurity Initiative (CNCI). DARPA was selected to run this program because we have some experience in the area of cybersecurity testing.

The NCR will result in a testbed on which researchers and developers can simulate and measure technologies and their performance in a realistic environment, allowing cybersecurity technology testing under real-world conditions and across a variety of network types.

DARPA believes the NCR will accelerate the development of leap-ahead cybersecurity technology for the larger research community. The fundamental idea underlying the rationale to develop a large-scale cyber test range is the recognition that scientific progress is often paced by advances in the instrumentation available to observe and test new phenomena and to run rigorous experiments to verify the significance of these observations and theoretical insights they stimulate. Just as developments in microscopes and telescope technologies opened new worlds to scientific exploration and revolutionized our understanding of nature, the NCR, if successful, will provide the same opportunity for the cybersecurity research community.

The design goal for the NCR is to enable researchers to rapidly create network architectures under a variety of conditions, from high operational demand to aggressive cyber attack, and develop responses based on the collected data. Simulations conducted with the highly automated cyber range will allow a variety of user and network behaviors, providing researchers insight and deeper understanding of how cybersecurity and situational awareness tools function in complex environments.

When completed, the NCR will allow realistic, quantifiable tests and assessments of cybersecurity scenarios and defensive technologies, revolutionizing cybersecurity testing by offering vastly improved cyber testing capabilities in terms of:

- Scope. The NCR will allow unclassified and classified testing on the same facilities, including wired and wireless networks, MANETs, supervisory control and data acquisition systems, and other features to simulate an extremely large variety of networks. It will allow defensive technologies to be tested against realistic offensives and greatly improve and accelerate researchers' abilities to produce solutions and rapidly deploy them.
- Scale. The NCR will have orders of magnitude more nodes than currently available test ranges, providing a much more realistic and valid test environment.
- Flexibility Through Automation. Under software control, the NCR will be able to quickly set up a wide variety of test networks and permit multiple, independent experiments on the same infrastructure. A graphical user interface will allow test directors to use a drag-and-drop feature to quickly lay out a network architecture, its hosts, system latency, environmental characteristics, and other pertinent test qualities and requirements. Once this infrastructure is created, it will be ready for testing immediately; the impact will be to dramatically change the time required to create a test environment from months to minutes.
- Efficiency. The NCR's state-of-the-art instrumentation and forensics technology will enable far better use of test time.

I think that NCR could operate much like other major National research assets and laboratories. A number of potential operating models exist, including the DOD's High Performance Computing Modernization Program, which has been run by the DOD since the early 1990s and makes high performance computing facilities available to Defense researchers for both classified and unclassified projects.

I believe, for example, that NCR could have a panel that reviews and prioritizes proposals submitted by potential users for time on the range. One of their guiding principles would be to ensure that the portfolio of research fulfills the mission of the range. Such a panel would then schedule who gets access to the range and when, and what they can do on the range. An administrator would facilitate users' access and use of the range and ensure their individual research goals on the range are met. I am sure that other possible operating models exist.

Two primary technical challenges must be tackled to achieve NCR's goals: (1) How are large-scale, highly heterogeneous networks simulated realistically, and what is the scale and scope needed for realistic experiments?; and (2) What instruments can be created to monitor performance during experiments to provide the greatest meaningful understanding of the results, even providing quantitative measures of performance? Real-world cybersecurity events are taking place all the time, but existing network administration techniques provide little insight into their cause without considerable effort. The point of the NCR is to incorporate highly sophisticated, fast, flexible, and efficient instrumentation and administration technologies, in a controlled environment, to enable full understanding of such phenomena rapidly and with little effort.

In November 2007, DARPA released an unclassified Request for Information where we solicited the community for ideas to improve cyber testing. In May 2008, DARPA released a Broad Agency Announcement and conducted a two-day unclassified industry day soliciting solutions from the community and answering questions posed by the community. A government-wide source selection process selected the best of breed from those proposed. The NCR program is in its first phase. During this phase, there are seven teams of defense contractors, universities, small businesses, vendors, and service providers working on competing designs to be completed and delivered this summer. The next phase will be to take several selected design teams forward to build small-scale prototypes. We expect that selection and build phase to be completed in fall of next year, and then move on to completion and operation of the range.

DARPA will not own or operate the NCR when completed. Historically, DARPA facilities and institutional interests have been held to an absolute minimum, allowing the Agency to be open to new ideas. To remain consistent with this management philosophy, DARPA will not own or operate the NCR once it is built.

The NCR is an integral part of the CNCI, and within NCR are two key working groups. The NCR Joint Working Group is a stakeholders' panel headed by DARPA that is developing the technical vision and business model for the NCR. This work informs the technical capabilities needed and provides options on how the NCR will

operate. Many issues are being studied, including who will manage the NCR, how it will be funded, who will have access, and conditions for use. Working group members represent DOD; the Intelligence Community; Departments of Homeland Security, Energy, and Treasury; National Science Foundation; Federal Bureau of Investigation; National Institute of Standards and Technology; the New York State Governor's Office; and the New Jersey State Police. They are invited to participate in all the steps from concept development to performer selection and periodic program reviews.

A separate working group focuses on the crucial issue of NCR security requirements. The range will have to be certified to run classified and unclassified testing, and the various agencies have different security requirements and nomenclatures. This working group seeks security protocols that will allow the NCR to be properly accredited by agencies from across the Government.

Coordination of Research

Much of the coordination of DARPA research with other government agencies occurs as a bottom-up process within technical communities. DARPA program managers are hired from government, industry, and academia in large measure because they are world-class technical experts with extensive knowledge of the research being done in their technical areas. In the last eight years, roughly one-third of DARPA program managers have come from industry, one-third from other parts of DOD, one-quarter from academia, and one-tenth from elsewhere. More than 95 percent of DARPA's program managers have advanced degrees and are subject matter experts from a wide variety of backgrounds. DARPA's policy of rotating program managers after four to six years ensures a steady stream of new people bringing fresh ideas to the Agency.

Because DARPA conducts none of its research in-house, its program managers look externally for ideas and research performers. During the process of starting programs, they seek good ideas wherever those ideas can be found, frequently by hosting workshops attended by researchers and other government experts. Engaging a wide spectrum of experts in a field through this extensive outreach effort is how DARPA coordinates ideas and research.

With that overall process in mind, let me give you some examples of how we have worked with the National Science Foundation (NSF) in information assurance.

DARPA co-funded three projects through the NSF Cybertrust Program (led by Stanford, University of Texas, and Princeton) dealing with fundamental software techniques for high assurance and security. NSF administered these grants to university researchers after their selection through the Foundation's standard, community-based, merit review process.

This summer, DARPA and NSF will co-sponsor two research workshops related to cybersecurity. Both workshops will bring together key thought leaders from universities, National Institute of Standards and Technology, Department of Homeland Security, National Science Foundation, and DARPA. The first workshop is in clean slate security architectures, which will identify paths to fundamentally redesigning computers for modern threats. The second workshop is meant to begin re-thinking the Internet. As you know, DARPA played a key role in developing the Internet, and our interest in the future Internet design workshop is to identify fundamental new network concepts that are far more resistant to attack than the current Internet.

60–Day Cyberspace Policy Review

The report that came out of the 60-day *Cyberspace Policy Review* is a high-level document covering a very wide variety of policy issues, including leadership, organization, legal, education and training, and operations and incident response. With respect to research issues, the area of DARPA's expertise, the review clearly recognizes the centrality of innovation to our national cybersecurity capabilities. In particular, it contains a discussion of the supply chain threats that we are addressing in our TRUST program—a problem that may not be widely appreciated outside the national security community. It also discusses the need for modeling and simulation, capabilities that could be provided by the NCR when it is completed. In general, between the game-changing technology we are promoting and the new tools and facilities of the NCR, DARPA will be able to make a significant contribution to the innovation goals of the *Cyberspace Policy Review*.

We are at the early stages of what will come out of the 60-day review, but having senior leadership at the White House looking hard at cybersecurity across the Federal Government will keep it high on the national agenda and stimulate progress throughout the field. As this process moves forward and we get a new Director at DARPA, we will be sure to continue to evaluate our own plans, programs and budg-

ets for cybersecurity. We have been a leader in promoting cybersecurity research, and we look forward to continuing our role promoting radical innovation for national security as the implications of 60-day review develop more fully.

The DOD's move toward network-centric operations means that information assurance will remain a crucial and long-standing concern. I hope my testimony today has given you a sense of DARPA's plans and ambitions.

I would be pleased to answer your questions.

BIOGRAPHY FOR ROBERT F. LEHENY

Dr. Robert F. Leheny was named Acting Director of the Defense Advanced Research Projects Agency (DARPA) February 20, 2009. He continues to serve as Deputy Director of DARPA, a position he has occupied since June 2, 2003.

DARPA is the principal Agency within the Department of Defense for research, development, and demonstration of concepts, devices, and systems that provide highly advanced military capabilities.

Prior to assuming his current positions, Dr. Leheny served as Director of DARPA's Microsystems Technology Office. He joined DARPA in October 1993 as a Program Manager in the area of optoelectronics.

Prior to joining DARPA, from 1987 to 1993, Dr. Leheny was an Executive Director for Network Technology Research in the Applied Research Laboratory of Bell Communications Research, Inc. (Bellcore, now known as Telcordia Technologies, Inc.), Red Bank, NJ. In this position he was responsible for managing an organization researching materials and device designs for communication systems. From 1984 to 1987, he was Director of the Electronic Device Research Group in the same Laboratory at Bellcore. From 1967 to 1983 he was a member of technical staff in Electronics Research Lab at Bell Laboratories, Inc., Holmdel, NJ. From 1962 to 1967, he was a graduate student at Columbia University and from 1960 to 1962, he was employed as a Radar Systems Engineer with the Sperry Gyroscope Co., Great Neck, NY.

Dr. Leheny received his BS from the University of Connecticut in 1960 and a Doctor of Engineering Science Degree from Columbia University in 1966. In 1983, he was named a Bell Labs Distinguished Member of Technical Staff and in 1992 he was named a Distinguished Graduate of the University of Connecticut School of Engineering. In 2003, Dr. Leheny was presented with the DOD Distinguished Civilian Service Award, the highest award the Department of Defense can give to career civil servants. He has published over 70 papers, co-edited a book and authored four book chapters. He is a Fellow of the IEEE and a member of the American Physical Society, American Association for the Advancement of Science, and the New York Academy of Sciences.

Chairman LIPINSKI. [Presiding] Thank you, Dr. Leheny. I now recognize Dr. Fonash for five minutes.

STATEMENT OF DR. PETER M. FONASH, ACTING DEPUTY ASSISTANT SECRETARY, OFFICE OF CYBERSECURITY AND COMMUNICATIONS, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, U.S. DEPARTMENT OF HOMELAND SECURITY (DHS)

Dr. FONASH. Good afternoon, Chairman Wu, Chairman Lipinski, and Members of the Subcommittees. Thank you for the opportunity to discuss the White House's recently released Cyber Policy Review as it relates to the Department of Homeland Security's ongoing efforts to secure the federal, civil, executive branch networks and information systems and to coordinate activities focused on securing the Nation's critical infrastructure.

One of the greatest threats facing our nation is a cyber attack to the critical infrastructure on which we depend. Our society relies on technology and telecommunications to support our economy and critical government functions. The cyber threats to these systems are real, growing, and evolving. They are large, diverse and range from independent, unsophisticated, opportunistic hackers to technically competent adversaries and nation states.

The Nation must be vigilant, proactive and innovative as it addresses and mitigates the service disruptions. The Department's National Cyber Security Division, or NCSD, serves as the national focal point for cybersecurity on behalf of DHS. It works with the private sector and Federal, State, local, tribal and international governments to assess and mitigate cyber risk and prepare for, prevent, and respond to cyber incidents.

The Cyberspace Policy Review assesses the current state of U.S. cybersecurity policies and structures. Based on this assessment, future decisions will be made regarding U.S. cybersecurity policy and appropriate structures to execute it. It is anticipated that those decisions will focus on the following five key areas outlined in the Review which build upon existing programs and activities: (1) developing a new, comprehensive strategy to secure America's information and communications infrastructure; (2) ensuring an organized and unified response to future cybersecurity incidents; (3) strengthening public, private, and international partnerships; (4) investing in cutting-edge research and development; and (5) beginning a national campaign to promote cybersecurity awareness and digital literacy and to build a digital workforce for the 21st century.

Within those areas, a series of near- and mid-term actions are set forth. DHS and NCSD, working with interagency partners, are actively engaged in advancing these actions. As many of them align with current NCSD activities, such as cybersecurity-related information sharing with federal, State, local and private sector partners, supply chain risk management, cyber workforce development, and the promotion of cybersecurity through national public awareness and education efforts, NCSD's fiscal year 2010 budget request provides further justification details on how DHS tends to grow and support these and other cybersecurity activities necessary to protect the Nation from cyber threats.

Before I address some of NCSD's current initiatives, let me emphasize that privacy and civil liberty considerations are at the center of our efforts. Protecting the privacy of Americans and their personal information is not just a priority, it is required by law and we take it very seriously.

DHS leads a multi-agency approach to coordinate the security of federal, civil, executive branch networks. The United States Computer Emergency Readiness Team, or US–CERT, serves as a central federal information security incidence center and is the focal point for the security of federal civil executive branch networks. Agencies report instances to US–CERT, and it guides agencies on enhancing detection capabilities and works with them to mitigate information security incidence. US–CERT compiles and analyzes incident information, shares the information with the operators of federal information systems. US–CERT provides products ranging from current and potential information security threats to alerts about vulnerabilities.

In addition, US–CERT is improving its capabilities to protect the federal enterprise in response to growing cyber threats, in large part to ramp up the current activities due to the Comprehensive National Cybersecurity Initiative, or CNCI. Over the last year, DHS has led the CNCI effort to establish a front-line defense for federal executive branch. As part of this effort, DHS works with

the Office of Management and Budget to reduce federal executive branch's external connections through the Trusted Internet Connection, or TIC, program. Consolidating such connections is the first step to creating front-line defense. As we reduce external connections, we will deploy EINSTEIN, an intrusion detection system, at trusted Internet connections which will allow us to more effectively analyze malicious activity across federal executive branch networks. We also work with federal agencies to develop additional capabilities to detect and eventually prevent intrusions. Such collaboration will help inform the products necessary to provide actionable information to our critical infrastructure community.

In addition to coordinating the security of federal civil branch networks, we work with industry and government partners to secure the Nation's critical infrastructure networks. The vast majority of the Nation's cyber infrastructure is owned by the private sector. As such, cybersecurity is not exclusively a federal responsibility, and the key to our assured success is protecting cyber infrastructures' collaboration with the private sector. It is for this reason DHS will continue to strengthen and build upon a public-private partnership framework created under the National Infrastructure Protection Plan, or NIPP. The NIPP was used for one of the CNCI initiatives whose focus is on improving protection of privately owned critical network infrastructure through public-private partnership. It is often referred to as Project 12.

State, local, tribal governments and international communities also play crucial roles in improving cybersecurity. Recognizing the contributions that can be made by leveraging such partnerships, DHS works with all levels of government and in the international community to help them increase awareness. DHS also works with other agencies to develop a plan for retaining a skilled, trained workforce. We need to build the next generation of our cybersecurity workforce that will help us maintain a competitive advantage. Over the coming years, we will focus resources on the education and training of our current workforce and developing and recruiting new talent. DHS is also encouraging university programs and provides scholarships to promising students.

In conclusion, as a nation becomes ever more dependent upon cyber networks, we must address cybersecurity strategically. Overcoming new cybersecurity challenges is a difficult task requiring a coordinated, focused approach to better secure the Nation's technology communications infrastructure. President Obama's Cyberspace Policy Review reaffirms that cybersecurity is among the most significant issues facing the Nation's economic and national security and it solidifies the priority that the Administration places on improving cybersecurity.

Thank you for your time today. I appreciate the opportunity to discuss the Department's efforts in advancing our cybersecurity posture. I would be happy to answer any questions from the Subcommittee.

[The prepared statement of Dr. Fonash follows:]

PREPARED STATEMENT OF PETER M. FONASH

Introduction

Good afternoon, Chairman Wu, Chairman Lipinski and Members of the Subcommittees. Thank you for the opportunity to speak about the Department of Homeland Security's (DHS) ongoing efforts to secure the Federal Executive Branch civilian networks and information systems, the White House's recently released Cyberspace Policy Review, as well as coordinating activities focused on securing portions of the Nation's critical infrastructure.

One of the greatest threats facing our nation is a cyber attack to our critical infrastructure and key resources (CIKR), on which our nation depends. Our information communications technology systems are integral to our daily lives. Our society relies on technology and telecommunications to support our economy and business operations, and also support critical functions of government. An attack could cause disruption to any or all of our key sectors and could jeopardize not only the private sector, but the government's ability to provide critical services to the public. Such an attack could also create cascading effects throughout the country due to the integrated and global nature of business today.

The cyber threats to these systems are very real, growing, and evolving. The Nation must be vigilant, proactive, and innovative in its efforts to address and mitigate disruptions of service. What makes this endeavor ever more challenging is the volume and composition of these threats. They are large and diverse and range from independent unsophisticated opportunistic hackers to very technically competent adversaries and nation states.

Our adversaries—both criminal and nation states—have become increasingly sophisticated in their methods and ability to coordinate malicious activities. The United States Government is aware of, and has responded to, malicious cyber activity directed at its civilian and military systems and networks over the past few years. We continue to remain concerned that this activity is growing more sophisticated, more targeted, and more prevalent.

I am here to underscore the Department's resolve to collaborate and share actionable information with stakeholders to mitigate known threats. Engagement, however, cannot be a one-way information flow with the goal of simply relaying information. We must create a two-way dialogue and facilitate continuous feedback that helps us improve notification products, such as informational notices and situational awareness reports.

Information sharing is an essential part of cybersecurity and we must continue to increase our current public/private information sharing and coordination efforts via the National Infrastructure Protection Plan (NIPP) framework. Using the NIPP framework, DHS has built robust working channels to exchange and integrate information with and among our partners in industry. Our efforts in this area have already begun. Through the Cross-Sector Cyber Security Working Group (CSCSWG), we have convened an Information Sharing Subgroup to look at ways to facilitate the bi-directional sharing of cyber information, indications, and warnings through the operational capabilities within and across the sectors and government. Specifically, we are looking at how to better share cyber threat and vulnerability information with those in industry who need it, understanding that some of this information is very sensitive. We are also developing plans on how to work with industry partners to obtain greater situational awareness on the status of CIKR networks.

As you know, DHS is the lead agency in a multi-agency approach in coordinating the security of Federal Executive Branch civilian networks. In large part, activities currently under way are due to the creation of the Comprehensive National Cybersecurity Initiative (CNCI), which is designed to further protect federal networks and explore new ways to assist industries in securing their infrastructure. There is wide agreement that the CNCI moved the ball in the right direction. However, more needs to be done. President Obama's call for, and subsequent completion of, the White House Cyberspace Policy Review reaffirms that cybersecurity and cyber threats are among the most significant issues facing the economic and national security of our nation.

At DHS we have been focused on three main areas as part of the CNCI:

1) Establishing a front line of defense;
2) Seeking ways to defend against a full spectrum of threats through intelligence and supply chain security; and
3) Taking cybersecurity to the next level through workforce education.

Over the last year, DHS has been leading the effort to establish a front line of defense by reducing vulnerabilities and preventing network intrusions in the Fed-

eral Executive Branch civilian networks. We are improving our cybersecurity posture in this area by focusing government efforts on reducing external connections through the Trusted Internet Connection program and deploying EINSTEIN, our intrusion detection system. DHS is also working in close coordination with our interagency partners to develop additional capabilities and capacity to detect and eventually prevent intrusions. Such collaboration with our federal partners will also help to inform the products necessary to provide actionable information to our CIKR community.

The Department is also seeking ways to better protect Federal Executive Branch civilian information systems and networks from the full spectrum of threats, such as from malicious code embedded in hardware or software products. This requires improving our global supply chain defense through increased awareness of threats, vulnerabilities, and consequences as well as collaborating with the National Institute of Standards and Technology in the development of standards, policies and best practices across the federal civilian enterprise. In conjunction with the Department of Defense (DOD), DHS is working to increase the capabilities of all federal departments and agencies to ensure the protection of their supply chains as well as their ability to mitigate risks.

A strong workforce is also necessary to ensure the continual advancement of our cybersecurity posture. Successful detection and mitigation of threats requires us to maintain a workforce at a high skill level. For the safety of our information systems and networks, now and in the future, DHS is focusing its resources on building the next generation cyber workforce by improving workforce training and education, recruiting new talent, and providing funding for college and university scholarships.

In addition, we are working with industry and government partners to secure the Nation's critical infrastructure networks. As you well know, the Federal Government does not own the Nation's information technology networks or communication infrastructures. The vast majority of the Nation's cyber infrastructure is in the hands of the private sector. For this reason, cybersecurity is not exclusively a federal responsibility, and as I mentioned earlier, collaboration with the private sector is essential.

The Department's National Cyber Security Division (NCSD) serves as the national focal point for cybersecurity on behalf of the Department. The NCSD works in concert with the DHS Science and Technology Directorate to cohesively develop technologies that address current and future technology gaps. The NCSD also works with the private sector and Federal, State, local, tribal and international governments to assess and mitigate cyber risk and prepare for, prevent, and respond to cyber incidents. The Department maintains a strong and positive relationship with the National Security Agency (NSA). NSA has provided a number of senior level detailees to the Office of Cybersecurity and Communication (CS&C) and the National Cyber Security Division (NCSD) within CS&C. These personnel assist in the execution of CNCI and provide integral technical and operational expertise to the Department as we build our capacity and capabilities. It is a true team effort. More broadly, NCSD through United States Computer Emergency Readiness Team (US–CERT) coordinates and shares incident information with law enforcement, the intelligence community, as well as other key stakeholders.

DHS is committed to advancing the resiliency of the government's cyber posture to better secure Federal Executive Branch civilian systems. DHS has a number of initiatives under way that I will discuss with you today. Before I move onto the initiatives, let me emphasize, for the record, privacy and civil liberties considerations are at the center of our efforts. Protecting privacy and ensuring the proper use of personally identifiable information is not just a priority; it is required by law and something we take very seriously.

Securing Our Federal Networks

US–CERT has been identified by the Office of Management and Budget (OMB) as the central federal information security incident center required by the *Federal Information Security Management Act of 2002* (FISMA) and serves as the operational center for the security of cyberspace of Federal Executive Branch civilian networks and CIKR networks. Agencies report incidents to US–CERT, including the identification of malicious code, denial of service, improper usage, as well as incidents that involve Personally Identifiable Information (PII). Operating a 24/7/365 operations center, the US–CERT is the lead entity in the national effort to provide timely technical assistance to operators of agency information systems regarding cybersecurity incidents. In this capacity the US–CERT guides agencies on detecting and handling information security incidents, compiles and analyzes information about incidents that threaten information security, and informs operators of agency

information systems about current and potential information security threats, and vulnerabilities.

US–CERT, working with OMB, is building additional capacity to fulfill its responsibilities under FISMA, as well as to better protect the Federal Executive Branch civilian systems and networks or ".gov." As a means of securing these networks, DHS is focused on implementing the Trusted Internet Connection (TIC) Initiative, which is led by the Office of Management and Budget. In addition, DHS is enhancing its EINSTEIN system, an intrusion detection capability, and deploying it at TICs across the Federal Government and at Networx Managed Trusted Internet Protocol Service (MTIPS) locations. Both of these programs support the efforts of the US–CERT—our 24/7/365 operations center that provides early watch, warning, and detection capabilities that enable us to more swiftly to identify and respond to malicious activity and to coordinate with our public and private sector partners.

The TIC initiative is a multi-faceted program which seeks to improve the U.S. Government's cybersecurity posture and build capacity to respond to incidents by reducing and consolidating the number of external connections which Federal Executive agencies have to the Internet. The multitude of external access points gives our adversaries too many avenues to seek out vulnerabilities and exploit potential security gaps in our networks. By limiting the number of entranceways into our networks to a smaller number, we can better monitor traffic entering and exiting the network and more rapidly identify when it is penetrated by an attacker.

During this process, the U.S. Government has learned a great deal about the federal networks. We initially identified more than 4,500 external access points, including Internet points of presence, across the Federal Government. Over the past year, departments and agencies have reduced that number. While it is important for the government to reduce external access points, we also must ensure configuration management of the technical architecture. Through the DHS-led multi-agency TIC technical working group, comprised of TIC Access Providers, we are working to develop and implement a standard technical architecture for perimeter security which is tested through the DHS TIC compliance validation process.

Consolidating external connections and configuration management are the first step to creating a front line of defense. As we reduce external connections, we will deploy the EINSTEIN system at those TIC locations. This will allow us to more effectively analyze activity across Federal Executive Branch civilian networks. The EINSTEIN system helps to identify unusual network traffic patterns and trends that signal unauthorized network activity, allowing US–CERT to identify and respond to potential threats. DHS installed the first TIC on its own network and deployed the upgraded EINSTEIN 2 system. We will be using the lessons learned from our implementation process to assist other departments and agencies as we continue to build more TIC locations and install more EINSTEIN 2 systems.

In addition to installing the EINSTEIN 2 system on DHS's network, we created the National Cybersecurity Protection System (NCPS) to create the framework under which EINSTEN 2 and future upgrades will be developed and deployed. NCPS is part of the overall formal acquisition program developed to enable the acquisition of technology that supports the NCSD mission including US–CERT and CNCI-related tasking.

NCPS supports the acquisition and deployment of EINSTEIN 2. We have created a plan for EINSTEIN 2 deployment that includes four phases each with the following status:

- Phase 1—DHS Deployment: Deployment is complete and operating at initial operating capability.
- Phase 2—Deployment at five selected Departments or Agencies: Deployment has been completed and DHS expects initial operating capability at these locations in June 2009. Technical discussions for deployment and installation of the EINSTEIN 2 system at the final Phase 2 location are ongoing.
- Phase 3—Deployment at Networx/MTIPS Vendor Sites: Conducted technical discussions with each of the Networx/MTIPS contract awarded vendors. As the vendors complete their technical architectures, DHS is providing the EINSTEIN 2 capability and working with departments and agencies on implementation. DHS has commenced installation activities with one MTIPS awarded vendor.
- Phase 4—Deploy to remaining Single Service TIC Access Provider Departments or Agencies: Technical discussions have begun with some of the remaining agencies. Deployments will occur as these agencies become more technically stable in their TIC implementations.

In the future, NCPS will provide US–CERT analysts with an automated capability to better aggregate, correlate, and visualize information. In addition, DHS envisions developing an Intrusion Prevention System, EINSTEIN 3, for Federal Executive Branch networks and systems. The system once fully deployed will provide the government with an early warning system and situational awareness, near real-time identification of malicious activity, and a more comprehensive network defense.

Together, TIC's reduction of Internet access points and EINSTEIN's situational awareness capabilities are examples of two of DHS's key initiatives designed to secure federal networks. The eventual expansion of the EINSTEIN system, to include intrusion prevention, will create an environment that will make it more difficult, more time-consuming, and more expensive for our cyber adversaries to reach our federal networks.

US–CERT is also taking additional steps to improve its capabilities and better protect the federal enterprise in response to the growing threat. We recently hired additional personnel to advance US–CERT's capacity to improve information sharing and help government and industry analyze and respond to cyber threats and vulnerabilities. This will further enable us to respond more rapidly and mitigate damage when attacks do occur. Work is also ongoing to improve collaboration with federal departments and agencies. For example, US–CERT recently developed the Joint Agency Cyber Knowledge Exchange (JACKE) to improve situational awareness and recommend actions for federal agency security operation centers. We are actively looking to expand the participation of the JACKE program to include all 26 major departments and agencies.

Working with the National Institute of Standards and Technology, DHS has established the U.S. National Vulnerability Database, the government's repository of standard reference data on computer vulnerabilities. Its data is built upon the NIST Security Content Automation Protocol which enables NVD data to be used by commercial products for standardization and automation of vulnerability management, measurement, and technical policy compliance checking.

Defending Against a Full Spectrum of Threats

Globalization of the commercial information and communications technology marketplace provides increased opportunities for those bent on doing the United States harm by penetrating our supply chain and poisoning critical software and hardware. We need to make sure that products do not contain malicious code embedded in hardware or software that could compromise our systems and help our adversaries gain valuable national security information or disrupt our networks. Thus, it is imperative that we work towards a stronger supply chain defense to reduce the potential for adversaries to manipulate our information technology and communications products before they are installed.

Protecting U.S. Government networks through global supply chain risk management requires a multi-pronged approach. DHS and the DOD have formed a partnership to coordinate supply chain risk management (SCRM) activities in the government. DHS has taken responsibility for non-national security related systems, while DOD is responsible for national security systems. Addressing this risk requires greater awareness of threats, vulnerabilities, and consequences. It will also require sound acquisition policies and practices, and will require the adoption of supply chain and risk managements standards and best practices. We are working with the National Institute of Standards and Technology and several other agencies towards the long-term goal of enhancing Federal Government skills and capabilities, and to provide departments and agencies with the necessary tool sets to better manage and mitigate supply chain risk.

The DHS SCRM Program will improve our capabilities through conducting SCRM pilots and establishing formal working groups within the government and private sector to inform program activities. The program is structured to meet requirements through testing, counterintelligence risk methodologies, best practices, controls, and other elements of supply chain risk management. Finally, enhancing our public-private partnership is essential, as the Federal Government cannot by itself ensure the integrity of the supply chain.

Leveraging/Partnerships

Key to succeeding in protecting our cyber infrastructure is collaboration with the private sector. As previously noted, most of our critical infrastructure and the Nation's cyber networks are owned and operated by private industry. Thus, a comprehensive, holistic cybersecurity strategy cannot be successful without an intensive engagement and collaboration with the private sector. Both government and private sectors have much to gain from working and sharing information with one another.

The creation of a strong partnership between these two sectors will help greatly in securing our cyber systems.

One of the initiatives under the CNCI was dedicated to improving protection of privately owned critical network infrastructure through public private partnership (Project 12). This is one of the ways DHS is trying work with the private sector to improve and institutionalize information sharing. As a part of this initiative, we are also looking to increase our public-private information sharing and coordination efforts and are engaging in discussions with the private sector to encourage collaboration with the business community nationwide. These discussions serve as information forums for businesses to better understand the cyber threats identified by government and for government to understand better the private sector's prodigious cybersecurity capabilities. This bi-directional information flow is crucial. DHS is also working to leverage the good work that DOD has done with the defense industrial base sector to increase actionable bi-directional information sharing of real and usable information with other sectors.

State, local, tribal governments and international communities also play crucial roles in improving the U.S. cybersecurity posture. Recognizing the contributions that can be made by leveraging such partnerships, DHS is working with all levels of government across the Nation to help increase awareness regarding cybersecurity and related preparedness and response issues. Specifically, DHS provides technical and operational assistance to State cybersecurity partners to assist in planning and executing cyber exercises. To expand this effort, NCSD is developing a repeatable cyber exercise assistance program that will be deployed to assist states with their cyber exercise needs. This program will include background and educational materials, the potential for a ''train the cyber exercise trainer'' program, staff and technical assistance with developing and executing exercises, as well as tools and resources to build upon past exercise efforts, and to integrate into future efforts such as the Cyber Storm Exercise series.

Cyber threats do not stop at traditional physical boundaries, so DHS collaborates with the international community to manage global cyber risk. In coordination with the our federal partners, we are engaging both with multilateral organizations and in multilateral forums, such as the European Union, the Group of 8, and the Meridian Conference, to enhance information sharing and situational awareness, improve incident response capabilities and coordinate on strategic policy issues.

Cybersecurity Workforce Education: Improving and Maintaining Our Workforce

In addition to being responsible for advances in our cybersecurity posture, DHS is working with other agencies to develop a plan for the retention of a skilled, trained workforce. Our adversaries are skilled and motivated, requiring us to constantly stay one step ahead of their actions. In order to address cybersecurity challenges, we need to build the next generation of our cybersecurity workforce that will help us develop a competitive advantage. Thus, we are focusing our resources on education and training of our current workforce, as well as recruiting new talent in order to develop a world-class workforce. DHS is also encouraging university programs and providing scholarships to promising students.

DHS believes that workforce development is critically important to our cybersecurity mission. DHS is actively recruiting and looking to fill new cybersecurity positions at NCSD. These positions range from entry level to management. For example, increases to US–CERT's staff, as DHS's watch and warning center, greatly enhance its ability and capacity for preparedness and response activities. We are actively recruiting for these open positions in order to improve our capabilities and expand our core leadership team.

Beyond the government domain, DHS is focusing its efforts on providing individuals within the cybersecurity sector of private industry with a baseline set of cyber skills. To achieve this, DHS worked across the public and private sector to develop the first Information Technology Security Essential Body of Knowledge to provide the cybersecurity community with the baseline skills and knowledge all information technology security professionals should possess to successfully perform their jobs. Cybersecurity is the responsibility of us all. Thus, we are striving to minimize our cyber gaps and vulnerabilities through both top-down and bottom-up approaches.

As part of our shared responsibility, we cannot simply focus on the present. We must also look to the future. This requires us to not only shape the workforce, but the community of computer users as well. Cybersecurity and cyber safety are learned behaviors, and we need to teach children how to be secure online. Here we are building from the ground up. By teaching children skills at a young age, we are laying the foundation from which our future cybersecurity workforce will come, while simultaneously improving our cyber defense. DHS is working with the Na-

tional Cybersecurity Alliance (NCSA) to make this vision a reality. In addition to ongoing work with the K–12 community, the NCSA recently launched its Cybersecurity Awareness Volunteer Education (C–SAVE) Project. This program encourages security professionals to put their knowledge and expertise to work in their local schools and help fill a tremendous gap in educating young people to use the Internet securely and safely. We are very pleased to be working with the NCSA on this program as this is a crucial endeavor to ensure the continued success and advancement of our cybersecurity mission.

White House Cyberspace Policy Review

On February 17, 2009, President Obama initiated a White House Cyberspace Policy Review of cybersecurity policies and issues affecting the Nation. On May 29, 2009, the results of that review were published by the White House in a report entitled *Assuring a Trusted and Resilient Information and Communications Infrastructure.* The review solidified the priority that the Administration places on improving the Nation's cybersecurity, and DHS will continue to have a key role as the lead agency for securing Federal Executive Branch civilian networks and collaborating with the private sector to enhance the cybersecurity of non-Federal CIKR networks.

DHS will have a significant role in several near-term actions outlined in the report, including updating the national strategy, strengthening international partnerships, increasing public awareness, and preparing a national response plan for cyber incidents. These near-term actions will enable DHS in collaboration with its government and industry partners to continue to address the growing and evolving cyber threat. Additionally, the operational goals of the comprehensive national strategy will include better coordination, response, recovery, and mitigation capacity across all stakeholder communities.

Conclusion

The cyber threat is rapidly growing and evolving. As the Nation becomes ever more dependent upon cyber networks, we must address cybersecurity swiftly and surely. Overcoming new cybersecurity challenges is a difficult task requiring a coordinated, focused approach to better secure the Nation's information technology and communications infrastructures. Accordingly, DHS is actively working with its federal partners to secure the ".gov" domain by implementing a holistic strategy for securing our civilian networks and systems.

Through government-wide programs such as TIC and EINSTEIN, we are enhancing the government's cybersecurity posture by reducing the number of external connections, including connections to the internet, while improving our detection and response capabilities. We are also striving to create a strong supply chain defense and develop an enduring, robust workforce.

It cannot be over-emphasized that, while DHS is focused on developing the necessary analytical, response, and technical capabilities to create a comprehensive network defense to secure the Nation's CIKR, we are not in this alone. A truly comprehensive cyber strategy requires an open partnership with the private sector, and it is in this arena that we are continually working to advance our mission. Everyone plays a role in cybersecurity, from the Federal, State, local, tribal and international governments to the private sector to the citizens who access computers for personal use. DHS is committed to its cybersecurity mission and will continue to reach out to these parties to promote cyber awareness, identify best practices, mitigate risks and improve its ability to respond to cyber incidents. The Department is also actively pursuing avenues to further collaboration and information sharing with these partners. The developments DHS has made in strengthening federal systems, enhancing our operational cyber response capabilities, and strengthening the public-private partnership have been significant, but we are committed to doing more.

Thank you for your time today. I appreciate the opportunity to discuss the Department's efforts in advancing our cybersecurity posture and increasing our security of federal networks. I will be happy to answer any questions from the Subcommittees.

BIOGRAPHY FOR PETER M. FONASH

Dr. Peter M. Fonash is currently the Chief Technology Officer for the Department of Homeland Security's Assistant Secretary for CS&C. He assumed the additional duty of Acting Director of NCSD on 16 March 2009. He has been a member of the Senior Executive Service since 1998.

Prior to this appointment, Dr. Fonash was Deputy Manager and Director of the National Communications System (NCS), serving nine months as the acting Deputy

Manager, and then becoming the full-time Director in April 2005. From 1998 until July 2004, Dr. Fonash was Chief, NCS Technology and Programs Division. He managed priority communications services technology development, network modeling and analysis, specialized telecommunications research and development, and priority services standards.

Before arriving at the NCS, Dr. Fonash served as the Chief with the Defense Information System's Agency Joint Combat Support Applications Division, providing technical software integration services to the functional communities and guiding functional applications' compliance with the standard common operational environment. He also worked for the Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence, and was responsible for Defense communications infrastructure policy and program oversight. He was also Chairman of the Office of the Secretary of Defense Information Technology (IT) Architecture Council

From 1986 to 1994 Dr. Fonash held various Defense Information Systems Agency (DISA) technical positions, including Director of Technology, and Chief of the Advanced Technology Office. He wrote DISA's strategic plan and managed the development of the Technical Architecture for Information Management—the forerunner of today's Enterprise Architecture.

Before joining the Federal Government, Dr. Fonash worked for AT&T and the Burroughs Corporation (Unisys).

Dr. Fonash has a Bachelor of Science in Electrical Engineering and a Master of Science from the University of Pennsylvania, a Master of Business Administration from the University of Pennsylvania Wharton School, and a Doctor of Philosophy in Information Technology and Engineering from George Mason University. His Ph.D. dissertation was on software reuse metrics.

DISCUSSION

Chairman LIPINSKI. Thank you, Dr. Fonash. We will now move onto questions. Chairman Wu is down there. I am not sure if you want to take back the Chair here or lead off with questions or shall I go?

Chairman WU. Go ahead.

Chairman LIPINSKI. Okay. This Chair will recognize himself for five minutes to lead off with the questions. Dr. Wing, you know, I was there yesterday at NSF and met with Dr. Bement and the AD's. Some of these things that I am going to ask about are not going to be a surprise to you or anyone actually who knows my background as a social scientist. I brought up in my opening statement that one of the most important things that I think is often overlooked and probably the weakest link that we have right now for cybersecurity is the general population.

Now, I want to lead off by asking, what is NSF doing right now in terms of research? What research is being funded by the NSF or where are you trying to search out for research that involves social science aspects of cybersecurity and facilitating collaboration between social scientists and computer scientists?

Dr. WING. Thank you for your question. It gives me an opportunity to speak about the Trustworthy Computing program which is one of the things I wanted to do when I got to the National Science Foundation, was to actually broaden the scope of what we were doing in cybersecurity to make sure to include topics like privacy and usability, which absolutely includes understanding social science and how humans behave, how organizations behave.

And so one of the things we specifically did was to broaden the scope of our Cyber TRUST Program to include privacy and usability, to work with our social science colleagues to make sure that, for instance, we have reviewers from their communities look-

ing at proposals that speak directly to these kinds of issues. In fact, cybersecurity is of course not just security, reliability, privacy, and usability. It is not just the technical issues that all of us scientists and engineers like to address, but there are much broader issues like legal and ethical which, if you look at the whole problem, we really need expertise from both the scientific and engineering communities as well as these less-technical communities.

So we are very much keen at the National Science Foundation in looking at the broader picture.

Chairman LIPINSKI. Thank you, Dr. Wing. I want to throw out a general question for each one of you actually going along these lines to tell me what rules do you have at your agency, what type of education do you do for your employees so that they do not wind up practicing bad computer hygiene at the agency? So we will start with Ms. Furlani. Tell me if there is anything that you do along those lines for your employees.

Ms. FURLANI. Well, of course, because we write the standards for the Federal Government, we expect our employees to live up to a higher standard. So we do work very diligently with our Chief Information Officer to ensure the understanding of what needs to be accomplished to protect the systems and the citizens that are interacting with us are deployed appropriately into the staff. It is something that we pay a lot of attention to in probably a more unique situation than others.

Chairman LIPINSKI. Actually, I have a friend who works for NIST who was going around to places where you can get your pictures printed up. He was trying to get to see where he could find a certain—I don't know if it was a virus or what exactly it was, but he was trying to find places where he could pick that up because he knew that this was going around to just get a better handle on all of this. Thank you. Dr. Wing.

Dr. WING. Yes, at NSF we have a Secure Information Technology Awareness Program. Every single NSF employee is required to go through a training every year, and it covers all the topics from how to choose a good password to shutting down your machine to make sure that screens with confidential information are not displayed and so on. And there are policy documents about this thick that everyone is expected to read. So we have a very serious—we take security very seriously, and everyone goes through this training program.

Chairman LIPINSKI. Dr. Leheny.

Dr. LEHENY. DARPA is a relatively small agency with under 200 government employees. We have a large number of contractors that work within our environment. We have no formal training program with regard to computer security, but as an agency within the Defense Department, our computers are a part of a larger enclave that is monitored very closely. We have a very robust information resource directorate that is available to help people work their way through problems they might be having with their computers. And so far we have been successful in locking large numbers—as you might imagine, our computer system is regularly under attack, and we have had good success at preventing those attacks from having any adverse affect on the operations of our computers.

Chairman LIPINSKI. Thank you, Dr. Leheny. Dr. Fonash.

Dr. FONASH. Yes, sir. Thank you. First of all, we follow all the FISMA best practices, and we closely follow FISMA. Our CIO is the person responsible for making sure those things are implemented across our department. We also are very much into security awareness training, and we annually require people to take security awareness. In fact, I have to take that tonight when I get home.

We also have to sort of eat our own dog food in the sense of what we do is again, I mentioned the TRUST Internet connections, and we actually have two TRUST Internet connections and we are moving to have all our network traffic go through those trusted Internet connections. And we have a close relationship between our security operations center and our US–CERT. Thank you.

Chairman LIPINSKI. Thank you. My time is expired. I will now recognize Mr. Smith.

Mr. SMITH. Thank you, Mr. Chairman. For Dr. Fonash, if we could maybe discuss a little bit the prioritization of the defenses, and with the deployment of EINSTEIN I know that approximately five agencies right now have already been deployed with EINSTEIN, is that correct?

Dr. FONASH. We have deployed. The systems are not operational yet. We are actually right now in the process of—there are several agreements that have to be set up. There is the service-level agreement, there is a memorandum of understanding. So those have to go through legal reviews, and in particular we have to address privacy issues. So we actually physically have those things established at those locations, but we are working the legal issues at this point in time.

Mr. SMITH. And then following will be eventually all agencies?

Dr. FONASH. Well, the idea is we are doing it in phases. What we are doing, first of all, is we are doing it at DHS, and that is one of the five agencies I included. And then we are working now with Justice, Department of Agriculture, and State Department and NASA in terms of deploying trusted Internet connections, actual, the physical EINSTEIN devices to those locations. We have also worked with GSA, and we actually put on contract, we actually made contract modifications working with GSA on the networks contract, and now agencies can go to the networks contract and get those services, trusted Internet connection services, from the networks contract vehicle. And so we are actually working with the carriers right now, AT&T, Sprint, Verizon to get them so that they can provide the capabilities. For example, they have to have a secure facility to do this trusted Internet connection. So right now the carriers are working those particular instances of what equipment they need to put in place so they can offer those services.

So that will be available to any agency that wants to do that. And then our next phase would deploy at 25 additional agencies and then the rest at some future point in time.

Mr. SMITH. And so can you speak to the prioritization and perhaps the need to deploy with every single agency?

Dr. FONASH. I think that clearly the larger the agency and the more—you know, beauty is in the eye of the beholder, sir. So let me say that. So each agency has to make its own determination

how important it feels its need to get this trusted Internet connection. We clearly at DHS have moved forward and actually have installed trusted Internet connections. In addition to that, we believe that State and Justice and NASA and Department of Agriculture, key locations that needed those trusted Internet connections, and then we have made available to anyone who feels that they have the need to immediately move to those contract vehicle. Those contract vehicles will be available and actually the services will be offered to use those capabilities through the networks contract, and that is the determination by those individual agencies as they want to move toward that capability.

And then we have a list of 25 other agencies that we can provide to you if you wish in terms of what we feel are the top 25——

Mr. SMITH. Okay. Thank you.

Dr. FONASH.—beyond that.

Mr. SMITH. Relating to privacy, I appreciate the fact that the President said, with emphasis, that he would seek not to include monitoring the private sector networks or Internet traffic. Then in the *New York Times* last Saturday stated that senior Administration officials have admitted those assurances may be challenging to guarantee and practice and that some Administration officials have begun to discuss whether laws or regulations must be changed to allow law enforcement, military or intelligence agencies greater access to networks or Internet providers when significant evidence of a national security threat was found. So I mean, maybe it is easier said than done to say that no private sector networks or Internet traffic would be included in this.

How would you respond?

Dr. FONASH. What we do is because of the capabilities that we have with EINSTEIN we are actually able to—we do not track the individual personal part of the messages. What we do is we drop that and what we do is we track information, what is called header information, basically the information, where it came from, where it is going to, and we also will look at—if we also recognize code, we will have patterns. A particular code, a particular program has certain pattern, a bit pattern in it, so you are able to actually recognize for example malware. So if you have Conficker traffic or some type of malicious code going past, you can actually recognize what is called the signature of that and pick that up. But for example, we wouldn't get into the privacy of a person's e-mail unless there was some issue, a national security issue, or something like that. But clearly what you can do is protect the privacy by looking at the header information, and there will be issues about PKI capture as we go forward, but we will address that. We will make sure we are doing that linked up with the privacy people, you know, making sure we are protecting the privacy of the individual.

Mr. SMITH. And do you suggest any legislative or regulatory changes?

Dr. FONASH. I think that is something that needs to be addressed as we go forward. At this point in time, I cannot recommend it.

Mr. SMITH. You do not recommend it?

Dr. FONASH. I would not be one to say yes or no at this point in time. I think that is an issue that needs further study.

Mr. SMITH. Okay. Thank you.

Chairman WU. The gentleman from New Mexico, recognized for five minutes.

Mr. LUJÁN. Mr. Chairman, thank you very much. I know that I read a lot in the testimonies about the need for coordination. If you could briefly touch upon how you were together, how the coordinating is working. If it is not working, what suggestions you may have, and also if any of you worked directly with any of the expertise that we have within any of our NNSA laboratories.

Dr. WING. So let me take that question on coordination. The coordination happens at all levels, and the best coordination happens in fact at the lowest level or with the technical people, at different agencies working together, informing each other about what each agency does in terms of what we fund, what we actually do. So we have program directors who talk to each other at the different agencies, and we coordinate things like running joint workshops to reach the academic community, the private sector jointly, and that coordination works beautifully from my perspective.

We also have more formal techniques for coordination. For instance, NITRD, Networking Information Technology Research and Development Program, and specifically we have been overseeing the senior steering group of the CNCI, the National Cyber Leap Year that is happening right now, and we are working very well together on that.

Let me also say as far as NSF goes, in working with other agencies like DHS and DARPA, we are actually working together on deploying cybersecurity testbeds. A couple of the testbeds that we jointly support with the other agencies, like DHS and DARPA, are actually starting points for DARPA's cyber range. So I think we coordinate quite well together.

Mr. LUJÁN. Dr. Wing, do you work at all with any of the expertise at any of our NSA laboratories, that you are aware?

Dr. WING. They contribute to NITRD.

Mr. LUJÁN. To which?

Dr. WING. NITRD.

Mr. LUJÁN. And what is NITRD?

Dr. WING. The Networking Information Technology Research and Development program.

Mr. LUJÁN. Okay.

Dr. WING. It is a coordination—an organization that coordinates over 13 federal agencies on networking information technology and research and development.

Mr. LUJÁN. Okay.

Dr. LEHENY. I would support Dr. Wing's comments about how coordination occurs largely at the program manager working level. As you may be aware, DARPA is an agency that does almost all of its research activities outside the Agency by contract. Over 90 percent of our budget goes out as contracts to industry, academia and federal laboratories. Specifically, Sandia, for example, is an active participant in many of our programs including the National Cyber Range Development that I spoke about in my oral testimony. I would like to point out that innovation and creativity in research is an individual property or characteristic of individuals, and it is not a type of activity that works well when it is driven from above. I like to characterize DARPA as a bottoms-up organization. It is

not the case that I wake up in the morning and come into work and ask my secretary to send me a program manager to manage great ideas I had overnight. Rather, it is the case that I arrive at work, open my e-mail and find that one of my program managers is trying to get on my calendar to come and tell me about his or her great idea. And it is in that way that new ideas, new programs, are created.

Of course, in order to support the argument for creating a program, a program manager has to reach out to other workers in their particular field in order to be able to put together a case for why a particular program should be started and executed, relying solely on their own internal creation of the program idea. It is usually not a good way to make a convincing case. You want to draw on as wide a body of people familiar with the technology and the challenges that the program is going to address that you possibly can in order to make the strongest case that you can.

Mr. LUJÁN. Thank you, Mr. Chairman. As my time expires, I want to see if I may be available, if time permits, for a second round of questions. I would like to still look a little bit more into the true collaboration with the NNSA laboratories. Not too long ago we did include an amendment to NITRD to include our national laboratories because there was a concern that maybe we weren't using the coordination as much as we should have been in the past. And so I would like to explore a little bit more and specifically pin down to the expertise that does exist within NSA with the attacks that they experience on a regular basis and then a few other questions I may have. So thank you very much, Mr. Chairman.

Chairman WU. Very good. We will come back to the gentleman.

Now, the gentleman from Michigan, Dr. Ehlers, is recognized for five minutes.

Mr. EHLERS. Thank you, Mr. Chairman. And I have a question for Dr. Wing, although any of you could try to answer it if you wish. But I was surprised to discover approximately six months ago that the number of students in colleges and universities deciding to major in computer science has gone down dramatically and also that there is not that much interest in high schools in getting involved. Everyone likes to play with their computer, but not very many are saying I would like to do this and build a better computer some time in my life. Since you are at NSF, you have access to all this data. What is happening? Is the enrollment continuing to be down? I raise this in the context of this hearing because if we are not producing the right people, we are not going to get anywhere with our discussions on cybersecurity, and particularly implementation of new ideas and new approaches. Could you enlighten me on that?

Dr. WING. Yes, thank you very much for that question. It is a concern, of course, at the National Science Foundation and my directorate about the decline in enrollments in the computer science undergraduate level. We had seen a decline for the past few years, primarily because of the dot-com bust and other worries. But fortunately, this past year we actually saw an uptick, and the community at large is much more optimistic now about seeing the enrollments go back up. So we are crossing our fingers and hoping that that will be a trend, a positive trend.

I do share your concern that we are not producing enough trained and educated students in computing, not just because they are likely the ones to be designing and building next generation information technology systems that we are all going to enjoy using on a daily basis, but we are working as a community to try to increase the pipeline to increase—to improve how it is we project what computer science is so that we can attract the best and brightest to the field.

Mr. EHLERS. I hope you are successful. It looks like Dr. Leheny would like to make a comment, too.

Dr. LEHENY. Yes. Thank you very much for this opportunity. DARPA has no specific charter to advance undergraduate or below education. However, we have two programs that I would like to inform you about that I think are attempting to overcome some of the issues that you raise.

The first program is one we call Computer Science Study Group. It is a program targeted to untenured, young faculty members in computer science, and it is a three-year program. Over the period of three years the support level for the individual in the program could reach as much as a million dollars, and as part of the program, we bring these individuals onto military installations and expose them to specific areas of interest to the Defense Department in the hope that we can encourage them to think about their research agenda in terms of solving the kinds of problems that the Defense Department has to deal with.

Currently, with the three-year program, as I mentioned, we bringing in about ten untenured faculty into the program each year. We currently have about 30 in the program. As you may be aware, a few years ago, we ran a series of what we called grand challenges which were targeted to demonstrate the ability of unmanned automobiles to navigate through difficult terrain. We found that there was an enormous amount of interest among students in that program and in participating in that program. And so we asked in our budget last year for a modest amount of funds, on the order of a couple million dollars, to create a special program that would reach out to high school students, particularly students interested in things like robotics in an attempt to stimulate interest among students and the kinds of problems that we have to deal with. Thank you.

Mr. EHLERS. Also the robotics FIRST program is——

Dr. LEHENY. Yes, that is one of the groups that we expect to be supporting.

Mr. EHLERS. Dr. Wing, you have something else?

Dr. WING. Yes, Mr. Ehlers. I forgot to mention one of the programs that my directorate runs is called CPATH, and it was recognized in fact by the 60-Day Cyberspace Policy Review as a way to again address a problem that you are concerned about, attracting the best and the brightest to computer science. And the whole notion of the program is to really revitalize the undergraduate curriculum in computer science. And one of the things I am very keen on doing is to actually do outreach to the K through 12 level because I do believe that it is increasing the pipe even before they get to college to explain what computing is all about and to get

them into the field. So I wanted to mention the CPATH program. Thank you.

Mr. EHLERS. Well, that is good. Thank you. And I try to do my part. As members of Congress, we get invited to speak in schools regularly, and whenever I speak in high schools I always tell the students they have to choose their subjects very carefully and they should not overlook math and science because when they get out and start looking for a job, they will discover that they will either be a nerd or work for a nerd and ask which they would prefer doing. And of course, they don't believe that, and then I simply ask them who is the richest man in the world? And finally the light starts to dawn a bit.

But you know, they just haven't heard this. They don't realize it. They don't understand the possibilities. They may love to play with their computer, even to do esoteric things with it. But the thought of doing that as a career doesn't always cross their mind, probably because they don't have a contact with people who do that on a regular basis.

Thank you very much. I yield back.

Chairman WU. Thank you, Dr. Ehlers. The National Science Foundation has data that indicates you are having success in your efforts.

The gentleman from New York, recognized for five minutes.

Mr. TONKO. Thank you, Mr. Chair. Dr. Wing, the investments that are made long-term wise in cybersecurity research by our Federal Government and certainly by the private sector can bear great benefits. How do you see us or NSF facilitating and encouraging the transfer of research from academia into that equation?

Dr. WING. Well, this a very good question because it is specifically relevant for cybersecurity, obviously. Academics can do their research, write their papers, produce students, and so on, but what really matters in the end is protecting and securing our cyberspace. And if the private sector owns most of that, then there has to be this more engagement between the academic community and the private sector.

NSF, as I mentioned, through the Science and Technology Centers that we run here and the Cyber TRUST Centers that NSF supports, has direct connections to industry. There are industrial partners who serve on the advisory boards on all of these centers and also—so they are formal mechanisms that we have. Even the large awards that we grant through the PIs or our normal programs, often those PIs will have connections to industry.

It goes without saying that a lot of the researchers, especially in cybersecurity, want to see that their research ideas are relevant and can help. And so they have a personal motivation to actually work with industry. Some of the techniques just get out there immediately. So for instance, one of the results recently has been in developing secure web browsers. And so now one of the open source web browsing companies has picked up those techniques immediately. A part of it is because many of the researchers have personal contacts in industry, and these kinds of things transfer informally but quickly.

Another mechanism that is not formal but very useful is many of the students, graduate students, that are funded through NSF

often take summer internships at companies like Google and Microsoft and Yahoo and so on, and one of the reasons that they do that is in fact how they can get access to real data. So there is great incentive to actually do that. Plus it is a very good opportunity for students to see what it is like to do research in an industrial setting.

So there is a lot of free flow of information in that way, and it is easy for academics to talk to industry and get ideas out there.

Mr. TONKO. On the flip side, how do you envision the private sector having the greatest influence or impact on creating the research agenda for NSF? Do they have a way to influence that agenda?

Dr. WING. Well, our agenda is officially—it is actually very much like what Dr. Leneny was saying. We are a very bottom-up organization as well, and it is the academic community that speaks to us as far as where they see the frontiers of research going, where the frontiers of science going, what the challenging science questions are, and they come to us with brilliant ideas and say, well, this is where the field is going. And in those conversations, we are always engaging industry. So whenever we run these planning workshops, industry is as invited as the academic community. So even from the very beginning, we try to engage the private sector in these kinds of strategic, agenda-setting programs, processes. We of course have the National Science Board where there is industry input through the Science Board. That helps the Foundation, helps us set priorities. And then as I mentioned before, some of the larger centers that we fund, like the TRUST Center, and we actually have four Cyber TRUST Centers, have industrial members on the advisory boards.

So there are formal and informal mechanisms that industry can use to provide input into the academic research agenda.

Mr. TONKO. And is there room for a lot more participation from the private sector or do you think that the awareness is out there and it has been pretty much heightened in the last couple of years, or do you think there is room for improvement in that?

Dr. WING. I actually think there is a heightened interest, so I have gotten specific queries from IBM, AT&T labs, besides the usual IT companies like Microsoft, Google, and so on. We interact with them very closely on all sorts of reasons. But specifically, I have been hearing from some of these companies that they would like to participate more in telling the academics what the real problems are and what they should be working on, and the academics, you know, can listen.

The other mechanism I forgot to mention is of course in our review process, through the panel reviews, through the committee of visitors that we have. We always have industry representatives there to help with the reviews so that they can give some sanity check. Well, that is an interesting problem, but it is not relevant for industry. They can also help in the committee of visitors and provide input on the portfolio of investments that we make.

So there are a lot of ways in which industry, either informally or formally, provides input to NSF.

Mr. TONKO. Thank you. Thank you, Chair.

Chairman WU. Thank the gentleman. Mr. Smith, recognized for five minutes.

Mr. SMITH. I am inclined to ask about the use and application of sanity checks, but maybe there is not enough time here. I am just teasing.

Dr. Fonash, if you wouldn't mind further discussion here, when it comes to public-private partnerships, I was pleased that the President did say that the Administration will not dictate security standards for private companies but will instead collaborate with industry to find technology solutions. Is that your take on his comments, briefly?

Dr. FONASH. Yes, sir, I believe that is correct. What we need to do is, you know, our mission right now is predominantly focused on protecting the Federal Government and protecting the dot-mil domain and then working with our private partners, and in particular, our critical infrastructures and making sure that they are aware of the situation so we do a lot of information sharing, so we are working on information sharing programs so they are aware of the threat and so that they take the appropriate measures to protect the network. And I think it is the issue of the—appropriate level of security for the infrastructure which depends upon if you are dealing with a critical defense contractor who has critical national security information and is protecting that versus Walmart protecting the latest sales price on their network. So it is a relative issue. It is an issue that is somewhat based on the business case, you know, in terms of what is the risk, and you have to do risk mitigation.

Mr. SMITH. Right.

Dr. FONASH. And so you put the appropriate investment in based on risk.

Mr. SMITH. In your testimony you mentioned public-private partnership objectives as being key. Could you elaborate on that and you know, really maybe define how we go about that? I mean, I know that we want to take care of government and then the private sector, but I think we need to acknowledge that already there is a great degree of overlap there and already public-private partnerships do exist, and there is transfer of information across the Internet between government and the private sector. So how do we sort through that and especially with the broadened use of the key objective being public-private partnerships?

Dr. FONASH. So the Federal Government clearly does not operate in a vacuum. We do our business. You know, the critical infrastructure that we even actually use on our own networks is actually owned by the ISPs or commercial carriers such as Verizon or AT&T. So we heavily rely on the public infrastructure to provide us services, to provide us communications, for us to do our business. And so what we do is we actually have under national infrastructure protection, have set up a process where we work with the critical infrastructures in terms of protecting those critical infrastructures. And we, the National Cyber Security Division, are actually the sector lead for the IT infrastructure. And then within cybersecurity and communications is the sector for cybersecurity and communications is the national communications system, and that is actually the sector lead for communications. So the two critical communications and IT sectors are within that authority, and we work closely with industry to develop risk mitigation. We are

actually developing right now an IT risk mitigation process, and we will publish that in the near future so there is actually a process where they can actually look at the IT sector and determine, you know, how they do risk mitigation. That is actually a process that we actually developed with industry.

Going back to the R&D, we actually work with industry. There is a government sector committee and there is actually a public industry sector community. And within that industry sector committee, there is actually a group that works with us on the R&D portion. And they actually provide us what they believe are the IT R&D requirements and the communications R&D requirements which we then pass on to the R&D community through our S&T directorate and also through attendance of their appropriate meetings.

So we work that way. We also work from an operational point of view. We work for the US–CERT which provides the information sharing, and information security center that we run for the Federal Government. But we make that information available to our private partners in terms of the warnings. And we also are building upon something the Defense Department started was Defense Industrial Base, if you are familiar with the Defense Industrial Base. What that is is through the contracting process at DOD——

Mr. SMITH. We can maybe get into that. I just have limited time here, and I was just wondering, you talked a little bit about critical infrastructure protection. Can you perhaps indicate whether or not there is any intent to take the critical infrastructure off of the so-called Internet grid as a means of protection?

Dr. FONASH. At this point in time, there are no plans to make it off the grid because for the most part, there are two reasons. First of all, the cost in terms of trying to make the government and private sector a private network. The cost is very large. It wouldn't be robust in many ways because—for example, because you have a separate network, you wouldn't have the robustness of the public network, and so I don't think there would be any—and then also from a security point of view, since you are really all using the same network—when you talk about the Internet, you are really talking about AT&T, Verizon and Sprint. And so everyone uses those networks. So it is a common carrier perspective here. So it is very difficult to take it off grid. So what we have to do is work together with industry in making sure it is secure, and you can have portions of it that are more secure. So for example looking at DNSSEC is something that we're looking at and going toward and going on the trusted Internet connection so that certain enclaves are more secure than others.

Mr. SMITH. Okay. Thank you.

Chairman WU. Thank you. Mr. Luján, recognized for five minutes.

Mr. LUJÁN. Thank you very much, Mr. Chairman. Ms. Furlani, I will begin with you. I have a few questions about the role that NIST pays with the payment card industry, if you can help me understand that and the coordination with that and what requirements maybe NIST has established for PCI.

Ms. FURLANI. What we have is the national vulnerability database which works with industry and with government to provide

data on what the vulnerabilities are. And the PCI, the payment card industry, decided to use that database as their mechanism to determine whether their companies meet certain criteria. We don't tell them what to do, but we provide the resources that they can measure against and understand whether their criteria are being met before they issue a payment card.

Mr. LUJÁN. So let me see if I understand that correctly. NIST does not mandate or prescribe any standards if you will that PCI has to follow? They utilize your database as a tool, but there is no requirement that NIST provides for them, is that correct?

Ms. FURLANI. We are not a regulatory agency except for the standards for the Federal Government to use in their cybersecurity.

Mr. LUJÁN. Are you aware of any organization that has standards that the credit card industry has to follow in protecting consumer information against cybersecurity crimes?

Ms. FURLANI. I am not.

Mr. LUJÁN. And Ms. Furlani, I am not, either. I have looked into this. I just thought maybe there is something out there. The reason I bring it up, Mr. Chairman, if there is no objection, I would like to submit an article from the *National Journal* 2/7/09, *The Cybercrime Wave,* into the record, that maybe we could review which outlines some of the alarming rates of crime, security breaches that are increasing year to year, money lost, Mr. Chairman, and I would make this available to the Committee and make sure we get a copy for the record if there is no objection, Mr. Chairman.

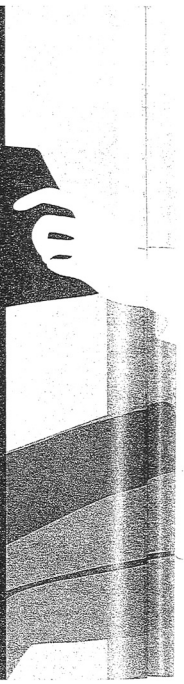
Chairman WU. No objection, so ordered.

[The information follows:]

Cover Story

Grifters, fraudsters, and thieves go virtual.

The Cybercrime Wave



By Shane Harris

If you're in the market for a bunch of stolen credit card numbers, then *ccarder* is your man. Or woman. It's not clear what *ccarder*'s gender is, but this much is certain: Around 1 p.m. Eastern Standard Time on a recent Friday, someone using that handle hung out a shingle in cyberspace and offered to verify, free of charge, the authenticity of stolen credit card numbers.

Ccarder traffics in said services through a storefront in an online chat room that's accessible from any Internet connection in the world. As an enticement to potential customers, *ccarder* would check any numbers they already had in their possession, hoping to turn them into buyers for hundreds, maybe even thousands, more. *Ccarder* was looking for customers who had only a few numbers, and the free verification service is a pretty common gimmick. *Ccarder* is not unlike the excessively perfumed vendors who stake out department-store counters, offering to spritz passersby with the latest fragrance in the hope that they'll buy the bottle.

Jason Thomas decided to take *ccarder* up on the offer. He runs a small cyber-analysis unit at West Virginia University, and he has

spent most of his career studying hackers and Internet security. Thomas clicked on a link that *ccarder* had put up in the chat room. It took him to a bare-bones website featuring a familiar set of blank data fields waiting to be filled in with a credit card number, expiration date, and three-digit security code, precisely the same information you would provide to any online merchant to pay for items in your shopping cart.

Thomas typed in strings of random numbers and then transmitted the information to *ccarder*. As it happened, the process that *ccarder* used to inspect the phony numbers was stolen too. *Ccarder* had hijacked the shopping cart feature of a charity based in the United Kingdom, even including its logo. *Ccarder* then ran a small transaction—1 British pound—through the same application that the charity uses to accept donations, which in turn connects to a payment processing system. In an instant, it recognized that Thomas's number was invalid.

Had Thomas been looking for real purloined credit card numbers, he could have typed a message to *ccarder* inquiring about price, quantity, and all the particulars necessary to complete the sale and take possession of the goods. Thomas sees these kinds of negotiations all the time, as well as purchases for a slew of other illicit items: child pornography, Social Security numbers, marijuana, checking account numbers, the requisite laboratory equipment to manufacture methamphetamine, small arms, parts needed to build improvised explosive devices, and packaged sets of unique personal information that allow the buyer to assume someone else's identity. In the cyber black market, buyers and sellers refer to these all-in-one packages as "fullz." Thomas has also seen the chat rooms, of which there are thousands emanating from computer servers around the world, used for trafficking in humans, not just their identities.

Online Offensive

87%

Increase in the number of "suspicious activity reports" on wire transfers filed by banks in the first half of 2008 over 2007.

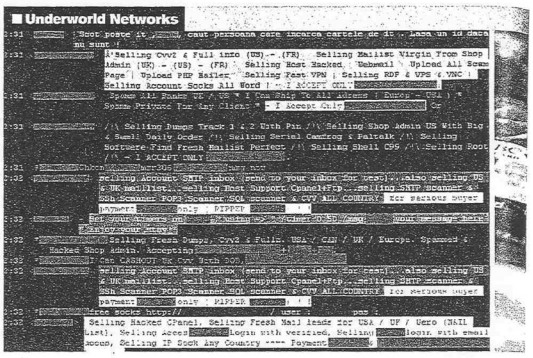
Thomas doesn't know for sure where *ccarder* is located, and whether he, or she, is a sentient being or a robotic software code set up to buy and sell automatically. But he does know, as do his fellow researchers

GETTY IMAGES/STOCK ILLUSTRATION SOURCE/BEK SHAKIROV

and clients—including federal law enforcement and intelligence officials—that *ccarder* is but one member of a worldwide organized criminal enterprise, which has discovered that using the Internet is a vastly more profitable, more efficient, and safer way to do business than robbing people on the street. And by almost every meaningful and verifiable measure, the business of online crime has never been better.

Washington Takes Notice

Federal law enforcement and intelligence officials are well aware of this development. Thomas and his team of researchers—most of them graduate students younger than 25 who grew up using computer technology—have briefed top officials, including FBI Director Robert Mueller. Team members describe the models of online behavior they've detected among money launderers, drug runners, and fraudsters.



Most of the activity that Thomas and others have studied involves Internet Relay Chat, an easy-to-install system that allows real-time communication and can be run on almost any computing device. Thomas says that hundreds of IRC networks are out there and that within them are tens of thousands of different channels. At any one time, millions of people can be using IRC, he says.

The proliferation of cybercrime has become a security issue for the new administration, too. Just days after his inauguration, President Obama announced his homeland-security agenda, which includes an anti-cybercrime component. Obama wants to "shut down the mechanisms used to transmit criminal profits," an online summary states. He envisions grants to train federal, state, and local agencies to "detect and prosecute cybercrime," and he intends to appoint a high-level cyber adviser who will report directly to him.

Last year, President Bush signed a law that more clearly defines certain types of cybercrime and makes it easier for federal prosecutors to bring indictments. The law lowers the threshold of monetary losses that a victim must incur to prosecute a cybertheft. And, for the first time, it stipulates the number of computers that qualifies as a "botnet," a network of hijacked machines remotely controlled by a hacker and used to conduct criminal activity. Generally, a computer user doesn't know that his or her machine has been seconded to the botnet. The law states that anyone who takes over 10 or more machines has commited a felony, regardless of the damage caused.

To date, the government has brought only two indictments under the new law, said Robert Holleyman, the president and chief executive of the Business Software Alliance, which was instrumental in pushing the measure through Congress. Holleyman applauded the use of the statute, but he cautioned that it was just a beginning. "The level of prosecutions," under this law and older statutes that apply to cybercrime, "has not kept up with the scale of growth" of criminal activity, he said.

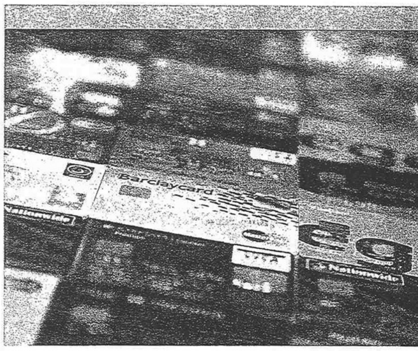
Although researchers have tracked that growth for several years, high-level White House and congressional reaction is a recent phenomenon. A sampling of that research helps explain why cybercrime has suddenly catapulted to the top of the national policy agenda.

The Identity Theft Resource Center, a nonprofit organization dedicated to studying and preventing identity theft, has been tracking security breaches involving unique personal information, particularly Social Security numbers, for three years. It catalogued 656 major breaches in 2008, an increase of 47 percent over the previous year's total of 446. The center culls its numbers from intrusions confirmed by

Digital Assault

- Criminals know that using the Internet is a vastly **more profitable, more efficient, and safer** way to do business than robbing people on the street.
- The total loss from **online fraud cases** referred to the Internet Crime Complaint Center in 2007 was $239 million.
- Credit card information is the product most in demand on the cyber black market, followed by **bank account numbers** and online stock-trading accounts.

source



Using a program called Internet Relay Chat (opposite), online criminals put out their shingles to sell stolen credit card numbers and specialized hacking services.

PHOTOS: (L TO R) SYMANTEC CORP.; GETTY IMAGES/PETER MacDIARMID

media sources and from notification lists sent to affected individuals by state government agencies after private information has been lost. But because the laws on disclosure are not uniform, the number of breaches is probably higher.

Other data reveal a rise in the kinds of activity most often associated with cybercrime. According to the Treasury Department's Financial Crimes Enforcement Network—an intelligence center that monitors criminal activity within banks, credit card companies, and other financial institutions—the first half of 2008 "reiterated the continuing trend upward" of activity related to identity theft. FinCEN, as Treasury's network is known, has also noted a troubling rise in wire-transfer fraud. In the first six months of 2008, "suspicious-activity reports," which banks file to help the government monitor abuses within the financial system, increased 87 percent compared with the first half of 2007.

According to financial-crime analysts, the increase in suspicious wire transfers largely corresponds to criminals' moving money out of individuals' bank accounts, often to offshore locations, after using a computer to obtain their account numbers. Victims sometimes hand that information over willingly, perhaps to a self-proclaimed representative of a high Nigerian official, who inquires in an e-mail whether the victim would be willing, for a fee, to turn over his checking account number for the processing and disposition of a tidy sum of millions of dollars that were left in limbo after his client's sudden demise. These bogus "phishing" messages prey upon the guileless, but they're perhaps the least worrisome component of the rising trend.

Tom Kellermann, a computer-security consultant who was the senior specialist in data risk-management in the World Bank Group's financial division, says that "account hijacking" has been on the rise for some time. In this variation of identity theft, a computer hacker gains unauthorized, often covert, access to a financial organization's account data, which can include its lists of millions of customers and their account numbers and passwords. More than four years ago, the Federal Deposit Insurance Corp., which guarantees account-holders' deposits, concluded that "unauthorized access to checking accounts is the fastest-growing form of identity theft."

"There's a robust marketplace for financial credentials," as the data are called, Kellermann said. "The hacker community is now aware of that."

The FinCEN report seems to show a silver lining. Suspicious-activity reports involving computer intrusion decreased 38 percent in the first six months of last year, compared with the same reporting period in 2007. The Internet Crime Complaint Center, a partnership of the FBI, the Justice Department, and state and local law enforcement agencies and prosecutors, which Thomas used to run, has also reported fewer individual complaints of Internet crime. That includes credit and debit card fraud, computer intrusion, and unsolicited spam and e-mail messages.

Although the number of computer intrusions apparently are down, the monetary losses associated with them are heading up. The total loss from all fraud cases referred to the crime center in 2007 was $239 million. That was up substantially from $198 million the previous year. Kellerman, Thomas, and other analysts agree that the losses associated with online criminal activity are piling up. That reflects a troubling evolution in cybercrime: It's more organized and more efficient than ever before, allowing criminals to make more money doing less work. The bank robber has become a quaint figure of folklore. Says Kellerman, "The modern-day Jesse James is virtual."

The Cyber Black Market

He's also not acting alone; he has a gang. The global structure of cybercrime, analysts say, has a distinct and disciplined supply chain. "It's not like Hollywood movies where there's individual 'sneakers,' " says Uriel Maimon, a senior researcher with RSA Security, which provides information-protection services to major corporations. "Different people work in different groups putting together different pieces of the puzzle."

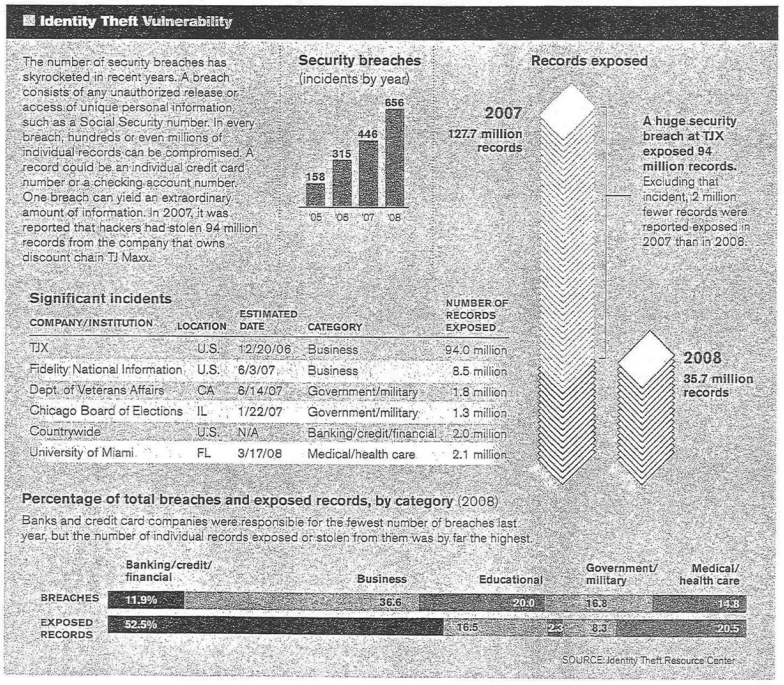
Maimon and others describe a kind of global outsourcing model, where hackers in different countries have perfected particular tools or services, which they sell or rent to criminals in other countries. Nigerians, for example, have carved out a niche harvesting e-mail addresses to use in phishing schemes. But they buy the phishing kits—the computer programs used to send those fake messages to millions of people—from software writers based abroad, usually in Russia and the United States, which have more colleges and universities that teach computer programming. Another group comprises the experts who find vulnerabilities on computers or in networking machinery and install malicious software that corrals computers into botnets. These botnet "herders" rent out their armies, perhaps to phishers or credit card dealers like *ccarder,* who could conceivably use the machines to harvest the Internet for more account numbers.

VerDate 11-MAY-2000 11:39 Jan 29, 2010 Jkt 050171 PO 00000 Frm 00067 Fmt 6633 Sfmt 6602 C:\DWORK\T&I09\061609\50171 SCIENCE1 PsN: SCIENCE1

The Internet underground's supply chain is diversified, just like its licit counterpart, the Internet economy. "The online underground economy ... has matured into a global market with the same supply and demand pressures and responses of any other economy." That was the conclusion of a yearlong analysis by Symantec Corp., a leading security software company, which studied online criminal behavior and its attendant business models. The report, published late last year, found that credit card information was the product most in demand on the cyber black market, accounting for nearly one-third of all goods advertised through those online chat channels. Credit card hawkers face such stiff competition that they post banner advertisements announcing new arrivals and lower prices.

The second-most-advertised items, Symantec found, were financial accounts, including bank account numbers and online stock-trading accounts. Once someone buys a stolen account, he has to extract the money. There are services for that, too, some of which involve off-line action. The Symantec researchers saw advertisements seeking intermediaries matching the gender and physical description of account holders; presumably, they would raise less suspicion when they showed up at a teller's window to withdraw the money. Although it might take longer to extract money from a checking account than to make purchases on a stolen credit card, the potential payout can be greater because most bank balances are higher than credit card cash-advance limits. Along with account numbers, Symantec saw devices for sale that are used to steal that information from databases. Indeed, the sale of stolen goods and the instruments to steal them in the first place go hand in hand.

The remainder of the top 10 list covers just about every personal financial instrument to be found in someone's wallet or, more likely, home computer—Social Security numbers,



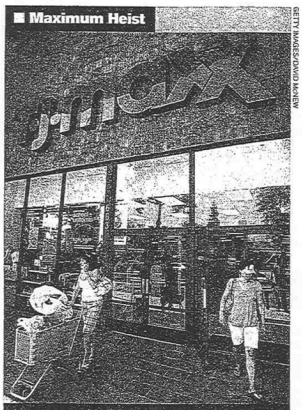
gift cards, department-store credit cards. E-mail addresses and login information for social-networking sites are also on the list. But credit card and financial data make up the majority of illicit goods and services offered. Prices range widely but appear to be pegged to the amount of money in an account. Corporate accounts, on average, sold for twice as much as personal accounts because they generally contained more cash, the Symantec investigators found. Still, for a relative pittance, one could buy a bounty of riches. "One particular bank account being advertised for $1,000 purportedly had a balance of $130,000," they wrote.

As more people bank online, pay their credit card bills over the Internet, or open electronic brokerage accounts, fraud is bound to rise. Surely, a considerable number of the pilfered accounts being sold underground were supplied by their unwitting, and arguably witless, owners. After all, what reasonably skeptical person, even one without a powerful command of the English language, would not raise an eyebrow at the overwrought and unjustifiably familiar missives of a Nigerian phisherman? "I have the courage to Crave indulgence for this important business believing that you will never let me down either now or in the future," reads one documented scam e-mail. Unless you know "Moses Odiaka" or "Dr. Mrs. Mariam Abacha," why would you reply to their messages, much less give them your checking account number?

And yet people do, to the delight of confidence men. These phishers have even assumed the nom de crime "419," a reference to the section of the Nigerian criminal code that outlaws their business. They take a big-picture view of their exploits. "419 is just a game; you are the loser, I am the winner," sings pop crooner Uzodinma Okpechi, whose single "I Go Chop Your Dollar" was a hit across Africa and was adopted by 419ers as their theme song. It celebrates the gullibility essential to this decidedly pre-Internet trick, which traces its roots to the early 1980s. The scam was first perpetrated using snail mail, sent from unemployed Nigerians to unscrupulous Western businessmen looking to cut deals with "oil officials."

But the surge in online financial crime cannot be attributed to the 419ers alone. Indeed, it appears that the most sophisticated thieves are not coaxing account information—they're taking it, without warning and often without a trace. And that has senior U.S. intelligence officials very worried.

■ Maximum Heist



GETTY IMAGES/DAVID MCNEW

The TJX Cos., which owns TJ Maxx and Marshalls, suffered a security breach in 2006 that lost tens of millions of account numbers.

The Breach

In January 2007, the TJX Cos., which owns the discount retail chains TJ Maxx and Marshalls, disclosed that it had "suffered an unauthorized intrusion" into the system that processes and stores its customers' credit and debit card numbers, as well as their checking account information. The breach, which affected stores in the United States, Canada, the United Kingdom, and Ireland, resulted in the loss of more than 45 *million* account numbers over an 18-month period, the company said. (Banks affected by the loss claim that more than twice as many numbers were stolen—97 million.) The company has said it believes that the perpetrators captured the information using wireless devices. The thieves may have been able to siphon off credit card numbers simply by sitting in store parking lots, without ever plugging into TJX's computers. In the quarter after it announced the breach, TJX absorbed a $118 million charge. At the time, the breach was the largest single loss of customer data ever reported.

It may have just been topped. Late last month, Heartland Payment Systems, which processes credit and debit card information, payrolls, and checks, announced that it, too, had been the victim of a data breach. Initial reports have suggested that more than 100 million individual cards have been compromised—more than twice the number that TJX acknowledged. Heartland executives have said that Visa and MasterCard alerted them to suspicious activity related to some transactions and that with the help of cyber-forensics experts, they discovered that a program designed to steal card data was implanted in the firm's network.

"We understand that this incident may be the result of a global cyber-fraud operation," Robert Baldwin, the company's president and chief financial officer, said in a statement. Since the breach, Heartland has said it will hasten the development of "end-to-end encryption" to protect information as it moves through the network or is stored in databases. The company has contacted more than 150,000 merchants to explain what happened. Heartland CEO Robert Carr said, "News media reports about the type and amount of data that may have been placed at risk of compromise in the data breach have been speculative." He added, "This data did not contain merchant data or cardholder Social Security numbers, unencrypted personal identification numbers [PIN], addresses, or telephone numbers, therefore making it highly unlikely it can be used for identity theft." He assured cardholders in an open letter that they would not be held financially responsible for unauthorized transactions, but he also said that they should "regularly monitor [their] card and bank statements" for any suspicious activity.

Such massive breaches have caught the attention of senior U.S. intelligence officials. One of them in particular, Melissa Hathaway, has been on a cyber-security whistle-stop tour of late, speaking to large public gatherings of technology officials and business executives, and writing op-eds about the woeful state of network

"The level of prosecutions [under federal and state cybercrime laws] has not kept up with the scale of growth" of criminal activity.
—Robert Holleyman

security and the determined nature of a slippery adversary.

Hathaway has made the connection between financial crime and government espionage. On several occasions, she has cited the case of a grocery chain in Britain, which unknowingly installed card-swiping devices in checkout lanes that had been clandestinely outfitted with special circuitry. The devices captured account numbers and PINs, which "were siphoned off and used to skim from, or in some cases empty, shoppers' bank accounts," Hathaway wrote in a recent op-ed piece.

"The same devices that thieves use to sneak into bank accounts, the same techniques that hackers use to disrupt Internet service or alter a digital profile, are being used by foreign military and spy services to besiege information systems that are vital to our nation's defense," Hathaway warned. To repel cyber-spies, the Bush administration launched a comprehensive national cyber-security initiative, which is now being taken up by the Obama White House. Hathaway was central to the initiative's rollout.

Economic Security

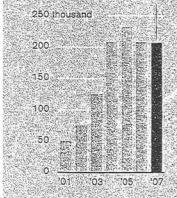
For intelligence and security officials, the line between financial crime and cyber-espionage—or perhaps even cyber-warfare—is a thin one. In their view, cyber-terrorists or nation-states could use the same devices to disrupt the U.S. economy broadly as cyber-thieves already do on a more targeted scale.

Indeed, Bush's cyber initiative was prompted by fears of economic and financial terrorism. In May 2007, Mike McConnell, then the director of national intelligence, told Bush in an Oval Office meeting that if the 9/11 attackers had chosen computers instead of airplanes as their weapons and had waged a massive assault on a U.S. bank, the economic consequences would have been "an order of magnitude greater" than those caused by the physical

Cybercrime Snapshot

The Internet Crime Complaint Center, a partnership of the FBI, the National White Collar Crime Center, and the Justice Department, catalogs complaints of cyber-related crime, such as computer intrusions or online fraud. Although the number of complaints has tapered off recently, the amount of money lost in these incidents has shot up. Analysts believe that cybercriminals are perfecting their techniques–stealing more with less effort.

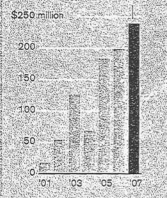
COMPLAINTS



TOP COMPLAINTS, BY CATEGORY (2007)

Online auction fraud	**35.7**
Nondelivery of goods, services, or payment	24.9
Confidence fraud*	6.7
Credit/debit card fraud	6.3
Check fraud or forgery	6.0
Computer fraud†	5.3
Identity theft	2.9
Financial institution fraud‡	2.7
Online threats	1.6
Nigerian letter fraud	1.1

MONEY LOST

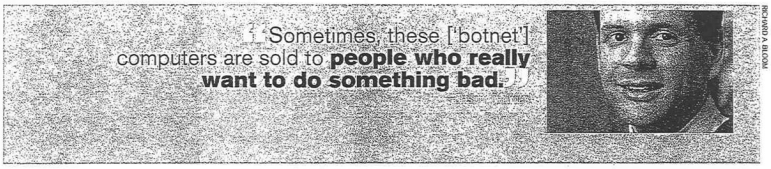


AVERAGE LOSS PER COMPLAINT (2007)

Investment fraud	**$3,548**
Check fraud or forgery	3,000
Nigerian letter fraud	1,923
Confidence fraud*	1,200
Auction fraud	484
Nondelivery of goods, services, or payment	466
Credit/debit card fraud	298

* Includes any crime in which the perpetrator gains the confidence, and then the cooperation of, the victim. Mail fraud is one prominent example.
† Computer software or internet capabilities are manipulated to commit a crime.
‡ Defrauding a bank or credit card company with stolen identification information.

SOURCES: "2007 Internet Crime Report"; National White Collar Crime Center; Bureau of Justice Assistance; FBI



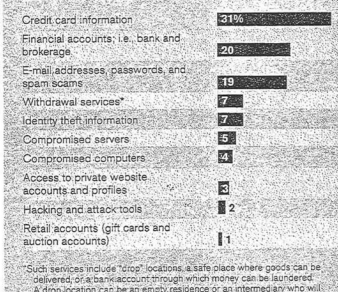
attack on the World Trade Center. The 9/11 attacks caused the New York Stock Exchange to shut down, brought business in the world's financial capital to a halt for several days, and deepened a national economic recession. Bush asked then-Treasury Secretary Henry Paulson Jr., who was at the meeting, if McConnell was correct, and Paulson assured the president that he was.

According to two former officials who were there, the conversation wasn't just about threats—McConnell offered Bush a potential solution. The Defense Department, especially the National Security Agency, was adept at fending off thousands of cyberattacks daily on its own networks, and, truth be told, at launching them on foreign adversaries. The subject of U.S. cyber-security arose in the context of a request by McConnell to conduct "information warfare" against insurgents in Iraq, turning the formidable cyber capabilities of the United States against adversaries who had shown remarkable technological deftness.

For Sale on the Cyber Black Market

Using Internet chat rooms, cyber-thieves and con artists buy stolen merchandise and sell their hacking services. Stolen credit card and bank account numbers are the hottest items for sale, but there's also a robust market of thieves-for-hire.

Percentage of black-market goods and services available for sale online, by category



*Such services include "drop" locations, a safe place where goods can be delivered, or a bank account through which money can be laundered. A drop location can be an empty residence or an intermediary who will reship goods to another location.

SOURCE: Symantec Corp.

According to the former officials, McConnell explained that the United States could conduct such offensive operations and the Defense Department understood how to protect military networks, but that no agency was providing a robust defense for the nation's infrastructure, which is owned almost entirely by private entities. McConnell suggested that the Defense Department and the NSA's capabilities could be turned inward, to protect the national cyber infrastructure, one of the former officials said.

Bush eventually issued an executive order that spawned the national cyber initiative. The Homeland Security Department is the nominal defender of civilian and domestic computer networks, although it lacks the resident expertise to accomplish that mission. Some individuals who have advised on the cyber-security initiative or are close to its participants say that the NSA is really running the show.

Cybercrime and cyber-espionage will be inexorably linked in any Obama policy on electronic security. Jason Thomas says that some botnets have grown to gargantuan proportions, numbering in the hundreds of thousands of computers. "Sometimes, these computers are sold to people who really want to do something bad," he says, such as a mass spam launch or a distributed denial-of-service attack, in which computers flood a server with automated signals and try to knock it off-line, the Internet version of a swarm of bees. "You're literally at the beck and call of whoever the botmaster is, and that is extraordinarily dangerous, both from a national security perspective and an individual perspective," Thomas says.

Kellermann, the former World Bank official, says that government is the only entity that can combat cybercrime in a consistent way. "I think it has become self-evident that the market will not solve this problem," he says. "The reality is, we've been building our vaults out of wood in cyberspace for too long." Kellermann was a member of a commission, sponsored by the Center for Strategic and International Studies, that recently wrapped up a comprehensive report on cyber threats and policies. The study was presented to the Obama administration.

In the hands of a determined adversary, the tools of cybercrime are easily converted to other tasks. In its recently released agenda on cyber-security, the White House said that Obama "will lead an effort to build a trustworthy and accountable cyber infrastructure that is resilient, protects America's competitive advantage, and advances our national and homeland security." The president and his advisers seem ready to take an all-encompassing view, one that recognizes the dynamic and interchangeable nature of the Internet underground and the cyber black market. They'll have their work cut out for them.

sharris@nationaljournal.com

Mr. LUJÁN. The reason I say that, Mr. Chairman, is as we look at this, I couldn't agree more with some of our colleagues. Coordination must take place from a public and private perspective to be able to protect consumers' information when they are getting hit at enormous rates. I think the average that an individual gets hit back to 2007 anyway that was measured according to the article is, depending on the type of crime, between $3,000 and $3,500, but just depending on what it may hit. We all know that we are trying to help people out more and more today, Mr. Chairman, that are sometimes getting taken advantage of. And this is an area where I think we could truly coordinate to provide some of those needed protections. One of the things, Mr. Chairman, that vendors, as an example, are required to do is to actually keep the data and back it up. And those are some of the areas where the largest breaches

occur. The article highlights a breach that most of us are familiar with, at TJMaxx where I think it was 90 million records were actually taken advantage of. To see truly what the requirement of the merchants are, vendors are, as we are looking at this cybersecurity loophole or lapses sometimes that take place to see what we can learn from there to be able to help individuals out. This is something that we touched on a little bit in our Homeland Security Committee hearing not too long ago, Mr. Chairman. I thought it was important to bring up.

Lastly, Mr. Chairman, the reason that I asked the question about the coordination is the first item in the report says that we need to improve interagency coordination. And so I know that we read about this, and what I would ask, Mr. Chairman, if our witnesses today are able to provide us with any thoughts or ideas, whether they support that point that was brought up or if they have suggestions on what can be brought up. Ms. Furlani, before I go, I would just like to highlight the point I was trying to make earlier, Mr. Chairman, around the expertise that we have within some of our NNSA laboratories who have to deal with cyber attacks on a daily basis. Not only do they have the sophistication from a technological perspective on some of the data sets that they have compiled with how we can combat some of these attacks, but they have an interface with the Government and private sector as well, especially because of the nature of them being classified and also being civilian organizations because of how they have been created and that we look to them to see how we could utilize that expertise. And with the time remaining, Mr. Chairman, I would go to Ms. Furlani.

Ms. FURLANI. I would like to specifically mention the interagency coordination that has led to our new draft Special Publication 800–53 which recommends security controls for low-, medium-, or high-risk systems and the agreement with the Director of National Intelligence CIO, the DOD, the Committee on National Security Systems, and of course, NIST, so there is one base line for all the Federal Government which will enable vendors to sell into the government much more easily. Then other agencies that have much higher security requirements than what NIST normally promulgates can set their standards higher. This was just recently released, and it is a true outcome of the coordination, particularly in response to the Cyber Security Review.

Chairman WU. Thank you very much, and I want to thank you all for appearing before the Committee this afternoon. 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 witnesses. The witnesses are excused, and the hearing is now adjourned.

[Whereupon, at 4:05 p.m., the Subcommittee was adjourned.]

Appendix:

ANSWERS TO POST-HEARING QUESTIONS

ANSWERS TO POST-HEARING QUESTIONS

Responses by Cita M. Furlani, Director, Information Technology Laboratory, National Institute of Standards and Technology (NIST), U.S. Department of Commerce

Questions submitted by Chairman David Wu

Q1. The Cyberspace Policy Review recommends an increased collaboration with international standards bodies and the private sector to foster international standards and cyber-crime protocols. What are your current international cybersecurity standards activities and how will you change them to meet this recommendation?

A1. NIST is actively participating with industry in international standards bodies, including the Internet Engineering Task Force (IETF), the Institute of Electrical and Electronics Engineers (IEEE), the International Standards Organization (ISO), and, in coordination with the State Department, the International Telecommunication Union's Telecommunication Standardization Sector (ITU–T). NIST participation includes leadership positions in the IETF, IEEE, and ISO in addition to its technical contributions. NIST's security standards activities are primarily focused on preemptive measures to enhance the security of systems and network protocols, but we are also supporting the development of standards for exchange of information about security incidents. In response to the recommendations of the Cyberspace Policy Review, NIST will work closely with other agencies, the private sector and international standards bodies to ensure that our leadership and technical efforts focus on the highest priority activities.

Q2. The Cyberspace Policy Review calls for increased collaboration with the private sector to create cybersecurity standards and guidelines. Witnesses at the Subcommittee's June 25 hearing also specifically recommended that NIST develop consensus standards for private industry with industry collaboration. How will you improve your collaborative efforts to implement these recommendations?

A2. While NIST's statutory authority makes Federal Information Processing Standards (FIPS) mandatory only for federal agencies, we always strive for broad, but voluntary, adoption of NIST standards. To promote convergence, NIST works collaboratively with industry in open standards forums (e.g., IETF, IEEE, and ISO) on many initiatives. We reference consensus standards in NIST publications where possible. In the rare cases where consensus standards are not the foundation, the NIST standards development process is an open process and always affords opportunities for public review and comment. Many standards efforts include public workshops to ensure the public, including industry, is informed about NIST standards activities and has early opportunities to provide input. In response to the Cyberspace Policy Review, NIST will work with the private sector to form new national standards bodies (e.g., within ANSI) as needed, to address additional cybersecurity requirements. In addition, NIST will increase its efforts to work with additional industry associations in the cybersecurity arena.

Q3. The Cyberspace Policy Review also recommends increased interagency coordination. How you will change your current efforts to meet this recommendation?

A3. NIST works closely with many federal agencies both formally and informally. NIST maintains the Computer Security Resource Center (CSRC) to distribute security standards and guidelines and encourage broad sharing of information security tools and practices. The Computer Security Program Managers Forum provides a mechanism for NIST to share information directly with federal agency information security program managers. As with industry, all agencies are provided the opportunity to review and comment on NIST standards before final publication and are invited to participate in our public workshops. NIST participates in cross-agency committees such as the Committee on National Security Systems (CNSS) and the CIO Council and its Information Security and Identity Management Committee (ISIMC). NIST is an active participant in the National Science and Technology Council's (NSTC) Networking and Information Technology Research and Development (NITRD) Subcommittee and the NITRD Cyber Security Information Assurance Interagency Working Group, as well as in the NSTC Subcommittee on Biometrics & Identity Management. NIST also participates in the Information and Communications Interagency Policy Committee and related subcommittees to share information security technical expertise as national security and economic policies are developed for cyberspace. NIST works actively with State and local governments to promote

adoption of NIST's security standards. To increase coordination in response to the Cyberspace Policy Review, NIST will reach out to additional multi-agency working groups to identify gaps and requirements for new capabilities to benefit all agencies.

ANSWERS TO POST-HEARING QUESTIONS

Responses by Jeannette M. Wing, Assistant Director, Computer and Information Science and Engineering Directorate, National Science Foundation (NSF)

Questions submitted by Chairman Daniel Lipinski

Q1. Witnesses at the June 10th hearing emphasized the importance of understanding human behavior to improve cybersecurity. What is NSF's current investment in the social aspects of cybersecurity and how is NSF facilitating collaboration between social scientists and computer scientists? Do we need new models for such collaborations?

A1. Cybersecurity must be addressed not just from a technical viewpoint, but also from social, economic, legal, and policy viewpoints. In FY09, NSF deliberately broadened the scope in its Trustworthy Computing Program to include privacy and usability, encouraging computer scientists to work with social scientists on these topics. NSF also supports research on economic models, including game theory, for network security. Here are some examples of projects NSF supports that address the socio-technical aspects of cybersecurity:

- A team from Stanford and New York University composed of computer scientists and social scientists developed a novel "Contextual Integrity Model," which considers social values and legal constraints in characterizing and evaluating the flow of information in organizations. The team has applied the Contextual Integrity Model to privacy policies such as *Health Insurance Portability and Accountability Act* (HIPAA), *Children's Online Privacy Protection Act* (COPPA), and Sarbanes-Oxley (SOX).
- Behavioral scientists and security researchers from the University of Massachusetts Lowell and Carnegie Mellon are working together to identify the factors that influence a user's trust in computer systems in general, and in robot systems in particular.
- Through the multi-disciplinary NSF Team for Research in Ubiquitous Secure Technology (TRUST), a lawyer, working with computer science colleagues, investigates how technology and the law interact. She spearheaded the California law that requires companies who lose individuals' personal information to disclose to the individuals impacted by the loss.
- A team at the NSF Cyber Trust Internet Epidemiology and Defenses Center at the University of California, San Diego and the University of California, Berkeley, is modeling the cyber underground economy, a glowing concern because there is significant criminal activity using the Internet. Of particular interest as a "metric" is what bots cost on the open market since there is as entire community that engages in bartering for such machines.

NSF facilitates collaborations between social scientists and computer scientists through these mechanisms: Direct funding of regular awards and Centers that support multiple principal investigators (PIs) from different disciplines (as in all the above examples); co-funding of awards between the Computer and Information Science and Engineering (CISE) Directorate and the Social, Behavioral, and Economics Sciences (SBE) Directorate; joint programs between CISE and SBE (e.g., Social-Computational Systems); Dear Colleague Letters joint with SBE (e.g., Research on Data Confidentiality) and/or with private foundations such as the Alfred P. Sloan and the Ewing Marion Kauffman Foundations (e.g., Creating New Cyber-Enabled Data on Innovation in Organizations, which has a specific focus on privacy); and workshops that bring together different communities (e.g., the National Academies' July 2009 Usability, Security, Privacy Workshop, co-sponsored by NSF and NIST). The NSF-wide Cyber-enabled Discovery and Innovation investment also provides an opportunity for collaboration between computer and social scientists. All these mechanisms, i.e., models of engagement, are extremely successful ways to foster collaborations between computer scientists and social scientists and they suffice to achieve the multi-disciplinary challenges of cybersecurity. For the future, we envision strengthening ties between the two communities as both recognize that cybersecurity is a multi-faceted problem: technical solutions are not sufficient, understanding human behavior is critical, and policy-makers must be informed of what is or is not technically feasible.

Q2. A major recommendation of the Administration's Cyberspace Policy Review is to increase cybersecurity education. The review specifically mentioned two NSF programs, Scholarship for Service and CPATH, in addition to those, how does

NSF plan to change or expand its programs to address the education needs identified in the review? Specifically, how can NSF address cybersecurity education at the K–12 level?

A2. In FY09, NSF challenged the computing community in its CISE Pathways to Revitalize Undergraduate Education in Computing (CPATH) Program to focus on teaching "computational thinking," the concepts underlying computer science, not just computer programming. Concepts such as algorithms, data structures, State machines, and invariants, which are driven by computational questions of efficiency and reliability are useful to everyone, regardless of one's field of study and regardless of one's eventual career or profession. To test out this view, the National Academies is conducting two workshops on "Computational Thinking for Everyone"; the first workshop was held in February 2009 and the second will be in early 2010. The focus of these workshops is particular for computational thinking in early grades, K–6.

The CPATH program also reaches out beyond the undergraduate level. Specifically, in the FY09 solicitation, we wrote ". . . CISE encourages the exploration of new models that extend from institutions of higher education into the K–12 environment; activities that engage K–12 teachers and students to facilitate the seamless transition of secondary students into Computational Thinking-focused undergraduate programs are particularly encouraged."

NSF is also expanding its Broadening Participation in Computing by supporting efforts which bring the two thrusts of computational thinking and K–12 together. For example, NSF is working with the College Board to revisit the Computer Science Advanced Placement course and exam; this multi-year effort will hopefully result in a novel CS sequence of courses that will stress computational concepts early and depict a rich and in-depth view of computer science to high school students.

For the future, we intend to promote a focus on computational concepts that would benefit everyone's analytical skills and a focus on outreach to K–12, through programs from across the Foundation.

Specific to cybersecurity, let's consider three populations of people: users of computing technology, developers of computing technology, and deployers of computing technology. Users of computing technology need to have some basic awareness of security hygiene; for example, not to open e-mail attachments in messages received from people one does not know. Through our Cyber Trust Centers and the TRUST Center (cited above), and even through our regular awards, we can leverage the participating institutions' reach into local communities to expand cybersecurity hygiene education. An example of such a project is MySecureCyberspace (*https://www.mysecurecyberspace.com/*), developed at Carnegie Mellon and partially funded by NSF. It is a portal for all age ranges, from children to seniors, who need to know the basics of safe and secure interaction for oneself and with others on the Internet.

Developers of computing technology are responsible for designing systems, especially software-intensive systems, with security in mind from the very beginning. They need to understand and be able to apply principles of software engineering, state-of-the-art tools to support secure coding, advanced programming languages that avoid entire classes of security vulnerabilities, and security architectures that derive from threat modeling. These technical topics are already covered in specific courses at most colleges and universities that offer computer science degree programs. Those who major in computer science will encounter these course offerings; non-majors who plan a career in software development should be encouraged to take such courses as well. To highlight the importance of these kinds of courses (for majors and non-majors), NSF is currently engaging the computer science community in a discussion on cybersecurity education at the undergraduate level.

Deployers of computing technology, for example, system administrators, are the front line defense in today's cybersecurity battlefield. They benefit most from programs such as Scholarship for Service and certification programs offered by professional organizations and industry. NSF's Education and Human Resources (EHR) Directorate will continue to support the Scholarship for Service program.

Questions submitted by Representative Ben R. Luján

Q1. The Cyberspace Policy Review recommends an increased level of interagency coordination and a renewed emphasis on cybersecurity research and development. Per the Administration's recommendation, what will NSF change in its current interagency activities? How is NSF leveraging the expertise of the National Labs and the Federally Funded Research and Development Centers?

A1. Through leadership positions, NSF already actively engages in interagency cybersecurity activities through these formal mechanisms:

- Networking and Information Technology Research and Development (NITRD) Program. The NSF CISE Assistant Director serves as the Agency Co-Chair of NITRD. NITRD has 13 member agencies.
  - The NITRD Senior Steering Group (SSG) is composed of senior representatives of agencies with national cybersecurity leadership positions. The NSF CISE AD serves as a co-chair for SSG. The SSG provides overall leadership for cybersecurity research and development (R&D) coordination, serving as a conduit between agencies and budget officials, between classified and unclassified federal R&D, and among government, academia, and industry. An example activity is the National Cyber Leap Year, as part of the Comprehensive National Cybersecurity Initiative (CNCI), which is identifying "game-changing" concepts for securing cyberspace.
  - The NITRD Cyber Security and Information Assurance Interagency Working Group (CSIA IWG) coordinates the efforts of NITRD agencies' cybersecurity programs, ensuring complementary and completeness (to the extent possible) in coverage of the cybersecurity R&D needs of the Nation. NSF program directors are active participants in CSIA IWG.
- The INFOSEC Research Council (IRC) consists of U.S. Government sponsors of information security research from the Department of Defense, the Intelligence Community, and Federal Civil Agencies. An NSF program director co-chairs the IRC. Discussions are both technical and strategic.

As there is heightened and growing interest by the Federal Government in R&D for cybersecurity, NSF expects to work in the future with other agencies more closely and in more and more activities, both informal and formal. NSF's deep and broad reach into the academic computer science community puts NSF in a unique position: to bring the attention of the academic community to nearer-term and/or mission-specific R&D cybersecurity needs of other federal agencies and to introduce federal agencies to the problem-solving capability, research results, and trained workforce of the academic community. As one example of how NSF's interactions have grown in just FY09, here is a list of cybersecurity workshops NSF has been instrumental in helping to foster, host, and coordinate with other agencies:

- Science of Security Workshop, co-funded by NSF, NSA, and IARPA (November 16–18, 2008). Goal: To deliberate on making security into a science with measurable metrics, inspired by established sciences and theories, such as biology, control theory, and reliability theory.
- Usability, Security, Privacy Workshop, hosted by the National Academies' Computer Science and Telecommunications Board (CSTB), co-funded by NSF and NIST (July 21–22, 2009). Goal: To advance objectives in usable security and privacy, taking into account the broad class of users, security administrators and services, and explore research opportunities and potential roles for the Federal Government, academia, and industry and ways to embed usability considerations in research, design, and development of secure systems.
- Workshop on Clean-Slate Security Architecture, hosted by NSF, co-funded by NSF and DARPA. (July 28, 2009). Goal: To frame a new security architecture that could be the basis for new host, network and applications.
- Workshop on Security Research for the Financial Infrastructure. Co-run with Treasury and co-funded by NSF and DHS (October 28–29, 2009). Goal: By bringing together the financial sector and academia, to gain a better understanding of the security problems faced by the financial sector and how the research community can help solve those problems.

Looking ahead, a possible outcome of holding such joint workshops is the creation of one or more joint programs between NSF and other agencies.

Through NITRD, NSF formally coordinates with national laboratories, including the Department of Energy's National Nuclear Security Agency (NNSA). NSF also participated in a joint workshop with DHS and IARPA, co-organized by MIT and Sandia National Laboratory in November 2007. This "NCDI (National Cyber Defense Initiative) Workshop-grass roots effort towards defining a cyber research agenda for the Nation" was a precursor to CNCI. Through the "DOE Workshops to Assess the Technology to Cope with Attacks to DOE systems, such as the Power Grid,"

held between 2007 and 2009 and organized by the Pacific Northwest National Laboratory, NSF presented research projects it funds on a more secure power grid, highlighting the Cyber Trust Trustworthy Computing infrastructure for the Power Grid (TCIP) Center at the University of Illinois, Urbana-Champaign. Finally, NSF funds academic researchers who themselves may directly collaborate with National Labs; for example, we recently funded a CAREER awardee at the University of New Mexico who collaborates with investigators at Sandia and Los Alamos on developing quantitative models of Internet censorship.

NSF supports researchers who can tap into the expertise of Federally Funded Research and Development Centers. In particular, NSF funds the Cyber Trust Situational Awareness for Everyone (SAFE) Center at Carnegie Mellon, whose researchers potentially can interact with the Carnegie Mellon Software Engineering Institute (SEI), which is an FFRDC. The SEI houses the Computer Emergency Response Team (CERT) Coordination Center, which collects data about security vulnerabilities and coordinates responses to security breaches.

Academic researchers funded by NSF often cannot interact more closely with members of the National Labs and FFRDCs if the systems of interest are classified, such as those within National Labs, or data are proprietary, such as that collected by CERT.

ANSWERS TO POST-HEARING QUESTIONS

Responses by Peter M. Fonash, Acting Deputy Assistant Secretary, Office of Cybersecurity and Communications, National Protection and Programs Directorate, U.S. Department of Homeland Security (DHS)

Questions submitted by Chairman David Wu

Q1. The Cyber Space Policy Review calls for increased collaboration with the private sector. How will you improve your collaboration efforts to implement this recommendation?

A1. The National Cyber Security Division (NCSD) within the Department of Homeland Security (DHS) collaborates closely with the private sector on a wide variety of initiatives in line with the Cyberspace Policy Review, and has always engaged in a variety of activities designed to further this collaboration. Specifically, NCSD engages with public and private-sector partners through the Critical Infrastructure Partnership Advisory Council (CIPAC) within the National Infrastructure Protection Plan (NIPP) framework. Since 2007, NCSD and its private-sector partners have co-chaired the Cross-Sector Cyber Security Working Group (CSCSWG) under CIPAC. The CSCSWG's membership includes public and private-sector representatives from each of the 18 Critical Infrastructure and Key Resources (CIKR) sectors under the NIPP. The CSCSWG meets monthly and offers a mechanism for public-private collaboration on cybersecurity initiatives, such as improving information sharing, considering private-sector incentives for increased cybersecurity, and developing cybersecurity metrics that can be used by multiple CIKR sectors. The co-chairs of the CSCSWG have recently formed a Steering Committee to ensure that the agenda and work areas undertaken by the group meet the needs of all CIKR sectors.

One area of focus for the CSCSWG in the near future will be development of a Cyber Incident Response Plan. This plan will be developed in collaboration with industry and government partners and will provide a much needed overall framework to significantly improve coordination in response to cyber incidents.

Under CIPAC, NCSD will continue to expand its engagement with private-sector partners to address additional issues necessary to secure the Nation's cyber assets, networks, systems, and functions. Control systems security represents an area of cyber concern that will see a substantially increased level of collaborative efforts, including the continued expansion of the Industrial Control Systems Joint Working Group (ICSJWG) and the Industrial Control Systems Cyber Emergency Response Team (ICS–CERT). Both of these groups are based on a model of public-private partnership and represent a growing area of collaboration.

NCSD, in conjunction with the National Communications System, can also leverage the National Coordinating Center for Communications (NCC). The NCC is a joint industry-government operation. It involves the U.S. telecommunications industry and Federal Government organizations that are involved in responding to the Federal Government's National Security and Emergency Preparedness (NS/EP) communications service requirements and supports planning for a more resilient national and international communications system to satisfy those requirements.

The mission of the National Coordinating Center is to assist in the initiation, coordination, restoration and reconstitution of NS/EP telecommunications services or facilities. The NCC is the mechanism by which the Federal Government and the communications industry jointly respond to NS/EP telecommunications service requirements. It provides for the rapid exchange of information and expedites NS/EP communications responses. While the primary focus of the NCC is the NS/EP telecommunication service requirements of the Federal Government, the NCC also monitors the status of all essential telecommunication facilities including public switched networks.

In addition, DHS is partnering with the Department of Defense and the Office of the Director of National Intelligence to engage with senior leadership, at the Chief Executive Officer level, in the information technology and defense industrial base sectors, under the Enduring Security Framework. This CIPAC working group recently formed to address the risks and opportunities to the U.S. cyber infrastructure inherent in globalization.

The Office of Intelligence and Analysis (I&A) has recently increased the production rate of cyber threat intelligence products intended for use by the private sector, State and local authorities, and federal civilian departments and agencies. These products are intended to provide awareness of the cyber threats and in some cases provide warnings so that the appropriate resources and actions can be implemented to counter these cyber threats.

I&A also, in coordination with NPPD, provides cyber threat briefings (classified and unclassified) to private sector representatives. In August and September 2009, I&A has provided or is scheduled to provide cyber threat intelligence briefings to the American Petroleum Institute (API), the Oil and Natural Gas Sector Coordinating Council (SCC), the Chemical SCC, and the Nuclear SCC.

In the area of cybersecurity research and development (R&D), DHS pursues collaboration with the private sector through participation in the Networking and Information Technology Research and Development (NITRD) program. A representative from the DHS Science and Technology Directorate co-chairs the NITRD Cyber Security and Information Awareness (CSIA) interagency working group and is a member of the NITRD Senior Steering Group for Cyber Security. During the past year, these groups have issued three Requests for Information through the *Federal Register* (garnering more than 230 private-sector white paper responses) and held a National Cyber Leap Year Summit with more than 100 private-sector participants (participants reports summarizing Summit outcomes are available at *www.nitrd.gov/NCLYSummitIdeas.aspx*). The private sector will continue to be engaged in the development of a game-changing cybersecurity R&D strategy.

Finally, we continue to look for new and better ways to enhance our partnership with the private sector, on both an operational and policy level.

Q2. The Cyber Space Policy Review also recommends increased interagency coordination. How will you change your current efforts to meet this recommendation?

A2. Overall Federal interagency cybersecurity policy coordination occurs through the Interagency Policy Committee (IPC) framework under the President's National Security Council system. The Information and Communications Infrastructure IPC serves as a focal point for cybersecurity matters and several Sub-IPCs are used to consider specific topics, such as incident response and information sharing.

The National Cyber Security Division (NCSD) within the Department of Homeland Security (DHS) continually strives to identify additional methods to facilitate coordinated responses to cyber threats. NCSD maintains many, often multi-faceted, relationships with government agency partners to fulfill its cybersecurity mission, and as we add personnel to meet mission needs, we will enhance not only our effectiveness but our ability to work with other agencies. Our existing relationships include operational coordination, information sharing, and policy formulation. NCSD's United States Computer Emergency Readiness Team (US–CERT) is charged with providing response support and coordinating the defense against cyber attacks for the Federal Civil Executive Branch (.gov). US–CERT focuses on improved customer service and improved interagency coordination in a variety of ways. For example, the Joint Awareness Cyber Knowledge Exchange meets biweekly to provide a classified forum for federal departments and agencies to exchange cyber threat and defense information, with US–CERT providing regular briefings and updates on specific ongoing threats.

Other NCSD programs also offer significant opportunities to improve agency coordination, and we continue to look for new and better ways to build partnerships. Through the Trusted Internet Connection (TIC) Initiative and deployment of the National Cybersecurity Protection System (NCPS), operationally known as EINSTEIN, NCSD has the ability to work with all federal civilian departments and agencies in a coordinated approach to reduce and consolidate external connections (access points) and implement or acquire security services. DHS coordinated with departments and agencies to create and refine TIC technical requirements and architecture, bringing technical expertise and issue awareness from early deployments to bear as additional departments and agencies are added to the program. DHS also meets quarterly with the TIC Interagency Working Group to address specific implementation challenges and provide definitions and clarification, as well as formal recommendations for TIC policy to the Office of Management and Budget. NCSD will continue to work with these groups to track TIC implementation progress, lessons learned, and recommendations for improvement. In addition, planned enhancements to NCPS will improve US–CERT's ability to share information about cyber incidents across the departments and agencies, thereby increasing interagency cybersecurity situational awareness.

NCSD also engages with public and private-sector partners through the Critical Infrastructure Partnership Advisory Council (CIPAC) process within the National Infrastructure Protection Plan framework. Since 2007, NCSD and its private-sector partners have co-chaired the Cross-Sector Cyber Security Working Group (CSCSWG) under CIPAC. One area of focus for the CSCSWG in the near future will be development of a Cyber Incident Response Plan. This plan will be developed in collaboration with industry and government partners and will provide a much-needed overall framework—supported by sub-frameworks, concepts of operations, and op-

erating procedures—to enable significantly improved coordination in response to cyber incidents. Under the CIPAC engagement framework, NCSD will continue to expand its engagement with private-sector partners to address additional issues necessary to secure the Nation's cyber assets, networks, systems, and functions.

In light of the Cyber Space Policy Review recommendations for increased interagency coordination, the Office of Intelligence and Analysis (I&A) will continue to strengthen its established relationships with the members of the Intelligence Community, the cyber intelligence elements of the Department of Defense, and law enforcement entities. I&A coordinates with interagency partners on its cyber products and participates in the interagency development of national level intelligence products. In the near-term, I&A will be striving to increase our interactions with the intelligence components of the Non-Title 50 and Title 10 departments and agencies. I&A continues to participate in intelligence community interagency coordination and working groups to ensure effective intelligence information sharing on cyber threat actors and will seek out additional partnership opportunities to include embedding I&A analysts in sister intelligence community elements. I&A plays an active role in developing all-source collection requirements and information needs through interagency coordination and working groups across the community. To ensure increased coordination I&A will seek to further involve DHS component organizations Federal, State, local and Tribal (FSTL) governments and critical infrastructure and key resource (CIKR) partners both public and private with cyber or infrastructure protection missions into the requirements development process to insure information deemed relevant to the operational components is collected by the intelligence community and disseminated to FSTL and CIKR partners.

In the area of cybersecurity research and development (R&D), DHS pursues collaboration across the federal landscape through participation in the Networking and Information Technology Research and Development (NITRD) program. A representative from the DHS Science and Technology Directorate co-chairs the NITRD Cyber Security and Information Awareness (CSIA) interagency working group and is a member of the NITRD Senior Steering Group for Cyber Security.

Questions submitted by Representative Adrian Smith

Q1. You stated in your testimony that when this effort began, the Federal Government had more than 4,500 access points to the Internet. I understand that the original plan was to reduce this number to below 100 to enable manageable deployment of EINSTEIN. Is this still the objective? If not, why not, and what is the new target number of TICS? How much does a change in the target number of TICS change the expected costs of the TIC initiative?

A1. The Comprehensive National Cybersecurity Initiative's Initiative 1 (the Trusted Internet Connection [TIC] Initiative) currently has the following objectives: to reduce and consolidate external access points across the federal enterprise; to manage the security requirements for Network and Security Operations Centers (NOCs/SOCs); and to establish a compliance program to monitor department and agency (D/A) adherence to TIC policy. Working together, DHS and OMB are making progress towards meeting this initiative.

NCSD, OMB, and the other Federal Department and Agencies, are constantly assessing the appropriate number of TICS required for the .gov domain.

The primary cost driver in this initiative is the number of physical locations where sensors need to be deployed. Multiple access connections can go through a single location. Therefore, changes in the number of access connections would not greatly affect cost.

Q2. Due to the geographical distribution of existing TICS, efforts to dramatically reduce Federal Government access points to the Internet presumably require a significant re-routing of traffic, which presumably adds additional cost to agencies' Internet Service Providers (ISPs). Is this correct, and if so, how (a) how significant are re-routing costs; and (b) how will this additional expense be paid for? Are these additional costs accounted for in agency budgets and planning?

A2. The geographic distribution of Trusted Internet Connections (TICs), in general, is not a cost factor. The TIC program is a consolidation of agencies' connections to external networks, not new connections. The Internet Service Providers (ISPs) can automatically reroute traffic on their network to a designated location. Pricing for traffic on an ISP backbone is not distance sensitive. The price sensitivity is the number of connections and the bandwidth of the connection to the ISP by the agency. Consolidation has a long-term financial benefit—namely, the larger the connec-

tion bandwidth, the lower the cost per unit of traffic. In general, there are additional charges for access lines in rural or remote locations.

An agency connection to an ISP has two cost elements: the cost of the dedicated access circuit and a service enabling device (SED) at the agency location (e.g., gateway router). The TIC program introduces the following additional access costs: capital cost and maintenance costs for the TIC equipment and facilities.

There may be additional costs for rerouting traffic within an agency's enterprise network; however, those costs largely depend on how each agency chooses to implement the TIC initiative. Agencies designated as TIC Access Providers (TICAPs) that are building their own TIC locations may incur additional costs for rerouting circuits, but that will depend on the outcome of negotiation efforts with the carriers. An option for TICAP agencies is to use a "hybrid" approach combining a subscription to the Networx Managed Trusted IP Service (MTIPS) with agency-specific TICs to reduce rerouting circuit costs. Agencies not designated as TICAPs, or those considered as seeking service, may comply with the TIC mandate by subscribing to the Networx MTIPS directly.

The MTIPS pricing contains three primary elements: a local dedicated access circuit, a SED at the agency location (e.g., a router), and the MTIPS Port. Only the local dedicated access circuit cost may be distance sensitive. If agencies are already using a Networx provider, there should not be a change to the cost per unit of traffic for the local circuit. If the agency chooses separate Networx contractors or MTIPS contractors, or has other agency-specific requirements, a new local dedicated access circuit or new SEDs may be required, increasing the cost.

The guidance from the Office of Management and Budget was for agencies to cover any additional costs out of existing funding.

Q3. What performance measures are associated with EINSTEIN and how will they be used to assess effectiveness and improve performance?

A3. The National Cyber Security Division (NCSD) within the Department of Homeland Security (DHS) has created performance goals under the *Government Performance Reporting Act* (GPRA) and applies Key Performance Parameter (KPP) performance measures to the National Cybersecurity Protection System (NCPS), operationally known as EINSTEIN.

Consistent with our GPRA goals, NCSD measures the percentage of Trusted Internet Connections (TICs) covered by NCPS. This measure tracks the percentage of TICS where NCPS sensors are deployed. Tracking this coverage of approved Internet access points for the Federal Government demonstrates the extent of coverage of .gov traffic that NCPS is providing at any given time.

KPPs are developed as part of the DHS acquisition review process. KPPs demonstrate the performance capabilities that will be purchased with requested funding. The KPPs are broken out by the Block capabilities—to match NCPS deployment plans—and each builds on the previous Block's capability. Additionally, each measure contains both a threshold and objective target. The threshold is the baseline "what-must-be-achieved" measure; the objective is what the NCPS is attempting to achieve. The table below contains the Block KPPs and their thresholds and objectives:

RESPECTIVE BLOCK	KEY PERFORMANCE PARAMETER (KPP)	BASELINE	
		THRESHOLD	OBJECTIVE
BLOCK 2.0	Detect known cyber events through automated intrusion detection within one minute of event occurrence	90% of known events automatically detected < 1 minute	95% of known events automatically detected < 1 minute
	Provide automated notification within operations center that cyber event took place within one minute of event detection	95% of automated notifications provided < 1 minute	99% of automated notifications provided < 1 minute
BLOCK 2.1	Aggregate and correlate detected cyber events for known indicators within 30 minutes of event notification	90% of cyber events aggregated and correlated < 30 minutes	95% of detected cyber events aggregated and correlated < 30 minutes
	Access stored data and automatically generate reports for post-cyber event analysis within 30 minutes of report initialization	95% of reports generated < 30 minutes	95% of reports generated < 15 minutes

Q4. What if any traffic volume or throughput limitations exist associated with EINSTIEN? Are you confident that this system can provide the processing power necessary to effectively analyze traffic and ensure against significant network delays, especially as online communications (including those on government networks) increasingly transition to more data and video intensive applications? Has the system's capability been validated in practice?

A4. Capacity challenges were identified as a risk; however, a mitigation approach was built into its development. There are two steps to the mitigation approach. First, initial deployment meets immediate and near-term bandwidth requirements as reported by the Department and/or Agency receiving EINSTEIN. Second, the commercially scalable platform and collection of technologies that make up EINSTEIN, as designed, allow for the seamless expansion of available computing resources as needs arise. This flexibility is best suited to meet today's bandwidth requirements and provides the ability to rapidly accommodate future increases.

Developmental, integration, and operational testing have been successfully conducted and validated to ensure that EINSTEIN's processing power scalability meets the increasing bandwidth demands of the federal network enterprise. Such testing and evaluation are part of a continual process as the Department of Homeland Security's National Cyber Security Division implements a phased deployment of EINSTEIN.

Q5. Given that cybersecurity is a cat-and-mouse problem where network defenders and attackers are both constantly changing their technologies and methods, how confident are you that the EINSTEIN system can remain effective over the medium- and long-term? Is it possible (or plausible) that, three to four years from now, our adversaries will be employing completely different technological means of penetrating networks that could render EINSTEIN obsolete? In other words, how adaptable is the EINSTEIN system to changing threats, technologies, and methods?

A5. We agree that attackers are constantly changing their technologies and methods, and therefore network defenders must quickly evolve their capabilities through continuous technology insertion and evolution. DHS is necessarily concerned both with today's threats and those unknown threats that are certain to surface and evolve. With the goal of addressing current and future threats firmly in mind, the National Cyber Security Division (NCSD) recently issued a Request for Information to identify new capabilities from industry. NCSD's goal is to deploy and operate today's cybersecurity technology while implementing the processes to ensure that EINSTEIN can address medium and long-term threat technologies and methods. The Department's Science and Technology Directorate (S&T) has substantial efforts, coordinated with NCSD, to identify and fund research and development (R&D) that would enable NCSD's future EINSTEIN capability to adopt to changing threats, technologies and methods. Additionally, the Office of Intelligence and Analysis continues to work with its intelligence community partners to understand the tactics,

techniques and procedures of threat actors as they evolve. The Department believes we can achieve this goal and meet future cybersecurity challenges.

Q6. You note in your testimony that EINSTEIN deployment has been completed at five agencies. Is it correct that the EINSTEIN system was originally intended to be deployed at all agencies? Is this still the case? If not, how is agency participation being determined-voluntarily by agencies or through a government-wide prioritization effort? Does the lack of participation by some agencies notably increase the vulnerability of intrusions and information breeches at participating agencies?

A6. The EINSTEIN program is designed under the Comprehensive National Cybersecurity Initiative to provide coverage to the federal civil agencies. The Administration is requiring all federal civil agencies to participate. Success of the program depends upon full participation. Lack of participation by some agencies could increase risk to all the others—including those that have deployed EINSTEIN—by slowing the identification of vulnerabilities and breaches and thereby increasing the likelihood of cascading effects within the .gov space.

Q7. In response to a question about the privacy of data collected through EINSTEIN at the hearing, you stated that "we wouldn't get into the privacy or a person's e-mail unless there was some issue, a national security issue, or something like that." How is "national security" defined in this context? What agency or official is responsible for making a national security determination that would authorize inspection of content traveling across federal networks, and what is the associated process for doing so?

A7. EINSTEIN 2 supports the Department of Homeland Security's (DHS's) critical information infrastructure protection mission as established by the *Homeland Security Act*, the *Federal Information Security Management Act* (FISMA), Homeland Security Presidential Directive 7 (HSPD–7), National Security Presidential Directive 54/Homeland Security Presidential Directive 23, and related authorities. FISMA requires the Office of Management and Budget (OMB) to oversee and ensure the operation of a central federal information security incident center that provides departments and agencies with cyber detection, analysis, warning, and mitigation support. In 2004, OMB identified the United States Computer Emergency Readiness Team (US–CERT), which is the operational branch of DHS's National Cyber Security Division, to carry out these responsibilities.

Under HSPD–7, DHS is "responsible for coordinating the overall national effort to enhance the protection of the critical infrastructure and key resources of the United States." "Critical Infrastructure" is specifically defined in the USA PATRIOT Act to mean "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." Malicious cyber activity that threatens one or more of these elements establishes the context under which EINSTEIN 2 is used by US–CERT.

EINSTEIN 2 passively observes network traffic to and from participating Federal Civilian Executive Branch department and agency networks. No human being reviews any of this data via EINSTEIN 2 unless and until specific pre-defined signatures designed to detect identified patterns of network traffic that may affect the integrity, confidentiality, or availability of computer networks or information are triggered. Only if such risk factors are identified within the data will US–CERT be alerted of potential malicious network activity. Thus, US–CERT does not obtain the content of all electronic communications passing over the protected networks but rather receives the network traffic relevant to a specific signature, along with the network traffic that is reasonably related to, and associated with, the network connection that caused the alert. Moreover, when an alert does occur, US–CERT has adopted procedures for reviewing signatures and handling information collected to ensure that the privacy of individuals is protected.

As discussed in greater detail in the DHS Privacy Impact Assessment (PIA) prepared for EINSTEIN 2,[1] EINSTEIN is not programmed to specifically collect or locate PII. While future signatures might be developed in response to threats that use what appears to be PII, the purpose of these signatures is to prevent malicious activity from reaching federal networks, not to collect or locate PII. US–CERT also follows procedures to remove any personal information from its products so that only US–CERT would see the full details of any personal information in the flow records,

[1] Available at *http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_einstein2.pdf*

alerts, and related network traffic. The PIA provides additional details on the minimization process and related US–CERT analyst training.

If it comes to DHS's attention that there may be a computer network event or incident that has "national security" implications, the proper entity with responsibility over that event would be notified in accordance with laws and policies.

Q8. What oversight and accountability mechanisms are in place to ensure that only data traveling to and from federal networks is routed off of Internet Service Provider (ISP) systems and through to EINSTEIN?

A8. Internet traffic flows to an EINSTEIN sensor either through the use of a Managed Trusted Internet Protocol Service (MTIPS) provided by an Internet Service Provider (ISP) or to the EINSTEIN sensor located at a department or agency's Internet access point, referred to as a Trusted Internet Connection (TIC). Safety mechanisms are in place under either EINSTEIN option to ensure that only data traveling to and from federal networks is routed off of ISP systems and through to EINSTEIN. Both options require the relevant department or agency to work with its ISP to ensure that only data traveling to and from federal networks is routed through to EINSTEIN based on Internet Protocol (IP) ranges assigned to the department or agency. Because federal networks do not allow non-agency, commercial traffic to traverse their infrastructure, the restriction of EINSTEIN monitoring to these IP ranges should limit monitoring to traffic directed to or originating from government systems.

MTIPS

With respect to a department or agency that contracts with an ISP for MTIPS, the contract contains a provision requiring the ISP to ensure that only data routed to or from the department or agency's IP addresses is routed to the EINSTEIN sensor. Specifically, the ISP's General Services Administration Networx MTIPS Statement of Work provides that:

> traffic collection and distribution supports the transport of government-only IP traffic between Agency Enterprise WANs [Wide Area Networks] and TIC Portals . . .. The TIC Portal . . . monitoring and management systems shall be dedicated to the management and monitoring of the subscribing agencies hosted by the contractor's portal and shall be isolated from commercial customers.

The ISP further confirms its responsibility to isolate government traffic from that of its commercial customers through a memorandum of agreement (MOA) executed with the Department of Homeland Security (DHS), which references the Statement of Work provisions. A department or agency that is using MTIPS also executes an MOA with DHS. Pursuant to this MOA, the department or agency is responsible for ensuring, in conjunction with the MTIPS provider, that only department or agency IP traffic is routed through the TIC portal where the EINSTEIN sensor is located.

TIC

A department or agency using a TIC would already have a contractual relationship in place with its ISP. Pursuant to that relationship, the ISP, in its ordinary course of business, would use routing tables to ensure that only traffic intended for the department or agency's IP addresses is routed to the department or agency's networks. In addition, a department or agency with an EINSTEIN sensor placed at a TIC also must sign an MOA with DHS. Pursuant to that MOA, the department or agency is responsible for ensuring that only traffic intended for, or originating from, that department or agency is routed through the EINSTEIN sensor.

Because EINSTEIN collects net flow information for all traffic traversing a sensor, in the rare case that the contractual routing protections fail, net flow information would be collected. A US–CERT analyst may detect the error by doing flow analysis, but the volumes of traffic make this unlikely. EINSTEIN's intrusion detection system (IDS) would only alert an analyst if the mis-routed traffic triggers an EINSTEIN signature. In the event of an IDS alert, and upon further inspection and investigation with the department or agency receiving the incorrectly routed traffic, a US–CERT analyst would be able to identify an incorrectly routed traffic error. US–CERT would then work with the National Cyber Security Division's Network Security Deployment and Federal Network Security branches, the relevant department or agency, the ISP and, if necessary, the MTIPS vendor to remedy the routing problem. In the unlikely event that an ISP's routing tables mistakenly assign a government IP address to a commercial client, a routing loop would result and would

be detected by the ISP in its ordinary course of business. This would signal to the ISP a need to correct the routing table.

Q9. What performance measures or other assessment tools have been developed for the CNCI? What are the primary risks to the success of the initiative going forward?

A9. The Department of Homeland Security's (DHS's) National Cyber Security Division (NCSD) is the lead or co-lead for six of the 12 initiatives within the Comprehensive National Cybersecurity Initiative (CNCI).

Currently, DHS reports both weekly and quarterly to the Joint Interagency Cybersecurity Taskforce. This reporting includes both activities and performance metrics. Performance information is reported quarterly to the Executive Office of the President. In addition, we work closely with the Office of Management and Budget on Initiatives 1–3.

Q10. Some organizations are calling for using liability protection (such as that provided by the SAFETY Act) as a tool for incentivizing greater private efforts to address cybersecurity. Is this being discussed and considered as part of your effort to collaborate with the private sector?

A10. Yes, the National Cyber Security Division (NCSD) within the Department of Homeland Security (DHS) collaborates closely with the private sector on a wide variety of initiatives and has always engaged in a variety of activities designed to further this collaboration. Specifically with respect to incentives, NCSD has engaged with public and private-sector partners through the Critical Infrastructure Partnership Advisory Council (CIPAC) process within the National Infrastructure Protection Plan (NIPP) partnership framework. Since 2007, NCSD and its private-sector partners have co-chaired the Cross-Sector Cyber Security Working Group (CSCSWG) under CIPAC. The CSCSWG's membership includes public and private-sector representatives from each of the 18 critical infrastructure and key resources (CIKR) sectors under the NIPP. The CSCSWG, which meets monthly, offers a mechanism for public-private collaboration on cybersecurity initiatives, such as improving information sharing, considering private-sector incentives for increased cybersecurity, and developing cybersecurity metrics that can be used by multiple CIKR sectors. The co-chairs of the CSCSWG have recently formed a steering committee to ensure that the agenda and work areas undertaken by the group meet the needs of all CIKR sectors.

Leveraging this public-private partnership, DHS solicited recommendations and advice from industry partners on a wide range of incentives—from leveraging federal procurement power, to cyber insurance, to ensuring inclusion of cyber investments in the utility rate base—for increased cybersecurity. One incentive considered by the working group concerns increased use of the SAFETY Act to address cybersecurity, including the issue of liability protection. The SAFETY Act Office is receiving and approving applications for cybersecurity technologies. These recommendations will be reviewed and considered by the appropriate members of the interagency and taken into consideration in light of the significant differences in business models and perspectives across the sectors.

Q11. As an alternative to regulatory- or liability-based tools to address private sector critical infrastructure, some have proposed simply taking critical infrastructure "off the Internet grid"—that is making the networks necessary for managing infrastructure such as the electricity grid completely closed, similar to how we operate our classified networks. Is this something the administration is looking at, and do you think it could help to eliminate the security vulnerabilities inherent to being connected to the Internet?

A11. The strategy of taking critical infrastructure "off the Internet grid" is not an option the Department of Homeland Security is pursuing due to the inherent complexities and feasibility problems associated with the concept. The Nation's critical infrastructure and related information technology systems and networks are interconnected, diverse, and unique, such that taking them off of the global Internet grid would generate a wide range of problems that make the task unfeasible on both strategic and practical levels. Many critical infrastructure networks were built with a specific architecture designed for Internet access. Their day-to-day communications and business operations require this access for functions ranging from inventory management to customer communications. Sequestering these networks behind barriers, in a manner similar to how classified networks operate, would result in multiple problems and logistical difficulties. This would require a complete revision of the design and function of critical infrastructure and key resources (CIKR) sector networks, as well as changes to the operations and business models of CIKR sector

members. An example of this is the Financial Services Sector, which depends on the Internet to provide real-time communications and transfer of electronic payments and account information. Additionally, several other government agencies outside of the Department of Homeland Security have responsibilities or regulatory authorities related to CIKR sectors and would have their own views on this subject.

○