AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

PROTECTING INFORMATION IN THE DIGITAL AGE: FEDERAL CYBERSECURITY RESEARCH AND DEVELOPMENT EFFORTS

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY AND INNOVATION

AND THE

SUBCOMMITTEE ON RESEARCH AND SCIENCE EDUCATION

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

WEDNESDAY, MAY 25, 2011

Serial No. 112–19

Printed for the use of the Committee on Science, Space, and Technology

Available via the World Wide Web: http://science.house.gov

U.S. GOVERNMENT PRINTING OFFICE

66–560PDF WASHINGTON : 2011

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, SPACE, AND TECHNOLOGY

HON. RALPH M. HALL, Texas, *Chair*

F. JAMES SENSENBRENNER, JR., Wisconsin
LAMAR S. SMITH, Texas
DANA ROHRABACHER, California
ROSCOE G. BARTLETT, Maryland
FRANK D. LUCAS, Oklahoma
JUDY BIGGERT, Illinois
W. TODD AKIN, Missouri
RANDY NEUGEBAUER, Texas
MICHAEL T. McCAUL, Texas
PAUL C. BROUN, Georgia
SANDY ADAMS, Florida
BENJAMIN QUAYLE, Arizona
CHARLES J. "CHUCK" FLEISCHMANN, Tennessee
E. SCOTT RIGELL, Virginia
STEVEN M. PALAZZO, Mississippi
MO BROOKS, Alabama
ANDY HARRIS, Maryland
RANDY HULTGREN, Illinois
CHIP CRAVAACK, Minnesota
LARRY BUCSHON, Indiana
DAN BENISHEK, Michigan
VACANCY

EDDIE BERNICE JOHNSON, Texas
JERRY F. COSTELLO, Illinois
LYNN C. WOOLSEY, California
ZOE LOFGREN, California
DAVID WU, Oregon
BRAD MILLER, North Carolina
DANIEL LIPINSKI, Illinois
GABRIELLE GIFFORDS, Arizona
DONNA F. EDWARDS, Maryland
MARCIA L. FUDGE, Ohio
BEN R. LUJÁN, New Mexico
PAUL D. TONKO, New York
JERRY McNERNEY, California
JOHN P. SARBANES, Maryland
TERRI A. SEWELL, Alabama
FREDERICA S. WILSON, Florida
HANSEN CLARKE, Michigan

SUBCOMMITTEE ON TECHNOLOGY AND INNOVATION

HON. BENJAMIN QUAYLE, Arizona, *Chair*

LAMAR S. SMITH, Texas
JUDY BIGGERT, Illinois
RANDY NEUGEBAUER, Texas
MICHAEL T. McCAUL, Texas
CHARLES J. "CHUCK" FLEISCHMANN, Tennessee
E. SCOTT RIGELL, Virginia
RANDY HULTGREN, Illinois
CHIP CRAVAACK, Minnesota
RALPH M. HALL, Texas

DAVID WU, Oregon
JOHN P. SARBANES, Maryland
FREDERICA S. WILSON, Florida
DANIEL LIPINSKI, Illinois
GABRIELLE GIFFORDS, Arizona
BEN R. LUJÁN, New Mexico

EDDIE BERNICE JOHNSON, Texas

SUBCOMMITTEE ON RESEARCH AND SCIENCE EDUCATION

HON. MO BROOKS, Alabama, *Chair*

ROSCOE G. BARTLETT, Maryland
BENJAMIN QUAYLE, Arizona
STEVEN M. PALAZZO, Mississippi
ANDY HARRIS, Maryland
RANDY HULTGREN, Illinois
LARRY BUCSHON, Indiana
DAN BENISHEK, Michigan
RALPH M. HALL, Texas

DANIEL LIPINSKI, Illinois
HANSEN CLARKE, Michigan
PAUL D. TONKO, New York
JOHN P. SARBANES, Maryland
TERRI A. SEWELL, Alabama

EDDIE BERNICE JOHNSON, Texas

CONTENTS

Wednesday, May 25, 2011

	Page
Witness List	2
Hearing Charter	3

Opening Statements

Statement by Representative Benjamin Quayle, Chairman, Subcommittee on Technology and Innovation, Committee on Science, Space, and Technology, U.S. House of Representatives	8
Written Statement	9
Statement by Representative David Wu, Ranking Minority Member, Subcommittee on Technology and Innovation, Committee on Science, Space, and Technology, U.S. House of Representatives	10
Written Statement	11
Statement by Representative Mo Brooks, Chairman, Subcommittee on Research and Science Education, Committee on Science, Space, and Technology, U.S. House of Representatives	12
Written Statement	13
Statement by Representative Daniel Lipinsky, Ranking Minority Member, Subcommittee on Research and Science Education, Committee on Science, Space, and Technology, U.S. House of Representatives	13
Written Statement	15

Witnesses:

Dr. George Strawn, Director, National Coordination Office, Networking and Information Technology Research and Development Program	
Oral Statement	16
Written Statement	18
Biography	22
Dr. Farnam Jahanian, Assistant Director, Directorate for Computer and Information Science and Engineering, National Science Foundation	
Oral Statement	22
Written Statement	24
Biography	34
Ms. Cita Furlani, Director, Information Technology Laboratory, National Institute of Standards and Technology	
Oral Statement	35
Written Statement	36
Biography	42
Rear Admiral Michael A. Brown, Director, Cybersecurity Coordination, Department of Homeland Security	
Oral Statement	43
Written Statement	44
Biography	52

Appendix: Answers to Post-Hearing Questions

Dr. George Strawn, Director, National Coordination Office, Networking and Information Technology Research and Development Program	68

Page

Dr. Farnam Jahanian, Assistant Director, Directorate for Computer and Information Science and Engineering, National Science Foundation 73

Ms. Cita Furlani, Director, Information Technology Laboratory, National Institute of Standards and Technology 76

Rear Admiral Michael A. Brown, Director, Cybersecurity Coordination, Department of Homeland Security 80

PROTECTING INFORMATION IN THE DIGITAL AGE: FEDERAL CYBERSECURITY RESEARCH AND DEVELOPMENT EFFORTS

WEDNESDAY, MAY 25, 2011

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

The Subcommittees met, pursuant to call, at 10:05 a.m., in Room 2318 of the Rayburn House Office Building, Hon. Benjamin Quayle [Chairman of the Subcommittee on Technology and Innovation] presiding.

RALPH M. HALL, TEXAS
CHAIRMAN

EDDIE BERNICE JOHNSON, TEXAS
RANKING MEMBER

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
2321 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6301
(202) 225–6371
www.science.house.gov

Subcommittee on Technology and Innovation &
Subcommittee on Research and Science Education – Joint Hearing
Protecting Information in the Digital Age: Federal Cybersecurity Research and Development Efforts
Wednesday, May 25, 2011
10:00 a.m.-12:00 p.m.
2318 Rayburn House Office Building

Witnesses

Dr. George Strawn
Director, National Coordination Office, Networking and Information Technology Research and Development Program

Dr. Farnam Jahanian
Assistant Director, Directorate for Computer and Information Science and Engineering, National Science Foundation

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

Rear Admiral Michael A. Brown
Director, Cybersecurity Coordination, Department of Homeland Security

HEARING CHARTER

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

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

WEDNESDAY, MAY 25, 2011
10:00 A.M.—12:00 P.M.
2318 RAYBURN HOUSE OFFICE BUILDING

I. Purpose

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

II. Witnesses

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

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

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

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

III. Overview

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

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

view also called for increased public awareness, improved education and expansion of the number of information technology professionals.

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

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

IV. Legislation

In June 2009, GAO found that the Federal agencies responsible for protecting the U.S. Information Technology (IT) infrastructure were not satisfying their responsibilities, leaving the Nation's IT infrastructure vulnerable to attack. In an effort to strengthen the work of those Federal agencies, the U.S. House of Representatives passed the Cybersecurity Enhancement Act of 2010 (H.R. 4061) in the 111th Congress. H.R. 4061 required increased coordination and prioritization of Federal cybersecurity research and development activities, and the development of cybersecurity technical standards. It also strengthened cybersecurity education and talent development and industry partnership initiatives. The Senate did not act on the legislation.

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

V. Issues and Concerns

Research and Development

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

Research and development provides a greater understanding of weaknesses in systems and networks and of how to protect those systems and networks. The Subcommittees will examine the integration of research and development activities within the Federal Government's cybersecurity efforts given its importance in increasing security over the long term. The hearing will explore current government research and development investments to ensure they are properly focused to pro-

---

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

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

vide effective and lasting cybersecurity, and will assess the challenges to establishing a prioritized national research and development agenda that strategically includes near-term, mid-term, and long-term goals.

Education and the Development of Cybersecurity Professionals

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

Standards Development

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

Agency Coordination

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

VI. Background

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

Networking and Information Technology Research and Development Program

The Networking and Information Technology Research and Development (NITRD) program coordinates unclassified cybersecurity research and development across 14 Federal agencies (additional agencies informally participate in NITRD).

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

In December 2010, the President's Council of Advisors on Science and Technology (PCAST) completed a legislatively required report on NITRD. The report, entitled Designing a Digital Future: Federally Funded Research and Development in Networking and Information Technology, found that "NITRD is well coordinated and that the U.S. computing research community, coupled with a vibrant Networking and Information Technology (NIT) industry, has made seminal discoveries and ad-

vanced new technologies that are helping meet many societal challenges."[3] The PCAST report included several recommendations, including increasing investments in long-term, multi-agency research initiatives in security and cyberinfrastructure, and enhancing the effectiveness of government coordination of NIT research and development.

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

National Science Foundation

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

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

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

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

National Institute of Standards and Technology

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

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

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

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

---

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

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

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

Department of Homeland Security

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

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

Housed within the National Protection and Programs Directorate (NPPD) the National Cyber Security Division (NCSD) is the operational arm of DHS's Office of Cybersecurity and Communications (CS&C). NCSD works collaboratively with public, private, and international entities to secure cyberspace and America's cyber assets, and protect cyber infrastructure through two overarching objectives: building and maintaining an effective national cyberspace response system, and implementing a cyber-risk management program for the protection of critical infrastructure. Numerous programs housed within NPPD work on cybersecurity related issues. The total FY 2012 budget request, as related to cyber programs, totals more than $500 million.

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

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

---

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

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

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

baseline security postures across individual agencies and the Federal enterprise as a whole.

Chairman QUAYLE. The Subcommittee on Technology and Innovation and the Subcommittee on Research and Science Education will come to order.

Good morning, everybody. Welcome to today's hearing entitled "Protecting Information in the Digital Age: Federal Cybersecurity Research and Development." In front of you are packets containing the written testimony, biographies and truth in testimony disclosures for today's witness panel.

Before we get started, since this is a joint hearing involving two Subcommittees, I want to explain how we will operate procedurally so all Members understand how the question-and-answer period will be handled. As always, we will alternate between the majority and the minority Members, and allow all Members an opportunity for questioning before recognizing a Member for a second round of questions. We will recognize those Members of either Subcommittee present at the gavel in order of seniority on the Full Committee, and those coming in after the gavel will be recognized in order of arrival. I now recognize myself for five minutes for an opening statement.

It is next to impossible to ignore the relevance of cybersecurity these days. News coverage has increasingly focused on cyber vulnerabilities covering stories such as companies losing personnel information or customers' financial data, or a government database being compromised by a malicious hacker. Perhaps most unsettling is that most stakeholders agree that our national cybersecurity response has not kept pace with the threats.

In early 2008, the need to increase network security was brought to the forefront when President Bush formally established the Comprehensive National Cybersecurity Initiative (CNCI) to deal with widespread cyberattacks on federal networks. Early in his administration, President Obama committed to continue this effort, and expanded it through the 2009 Cyberspace Policy Review, which identified a number of problems to be addressed through both near-term and mid-term actions. At that time, the Committee on Science, Space, and Technology held a series of hearings evaluating the state of cybersecurity research and development and the recommendations contained within the review.

Security efforts are often focused on the past and designed to respond to the most recently faced attack. However, the technology sector is exceptionally dynamic, and where possible, we need to attempt to anticipate vulnerabilities and future threats. This is where research and development and proper coordination can make a contribution.

It has now been a number of years since the review identified vulnerabilities across federal agencies. We are here today in part to evaluate what progress has been made. Additionally, as new threats emerge, we must assess whether we are staying ahead with research and development. Finally, we must make sure that we are appropriately tracking federally funded research and development initiatives. Since multiple agencies have cybersecurity responsibilities, and federal efforts in this area are growing, I am concerned that agencies may compete with each other for cyber ownership.

Congress must ensure that agencies are working collaboratively to prevent work from being duplicated at the cost of precious taxpayer funds.

Several agencies before us today have an important role in the development of cybersecurity standards. We should not underestimate the value of standards, whether they are minimum security measures for use by federal government agencies to protect information, or a framework to address cybersecurity risks for critical infrastructure. The lead responsibility for working closely with industry to develop successful standards has historically fallen to NIST. We would like to ensure that any comprehensive cybersecurity legislation effectively leverages the expertise of all federal assets.

I should also note that today's hearing is focused on federal cybersecurity stakeholders. Notably absent are those who design, build, own and operate the majority of the digital infrastructure in our nation. To that end, I intend to hold further discussions related to cybersecurity issues through future hearings of the Technology and Innovation Subcommittee that will include voices from the private sector.

I would like to thank my co-Chairman, Congressman Brooks, for sharing leadership on this important hearing. I also thank the witnesses for being here today and I look forward to a productive discussion.

[The prepared statement of Mr. Quayle follows:].

PREPARED STATEMENT OF CHAIRMAN BENJAMIN QUAYLE

It is next to impossible to ignore the relevance of cybersecurity these days. News coverage has increasingly focused on cyber vulnerabilities covering stories such as a company losing personnel information or customers' financial data, or a government database being compromised by a malicious hacker. Perhaps most unsettling, is that most stakeholders agree that our national cybersecurity response has not kept pace with the threats.

In early 2008, the need to increase network security was brought to the forefront when President Bush formally established the Comprehensive National Cybersecurity Initiative (CNCI) to deal with widespread cyberattacks on Federal networks.

Early in his administration, President Obama committed to continue this effort, and expanded it through the 2009 Cyberspace Policy Review, which identified a number of problems to be addressed through both near-term and mid-term actions. At that time, the Committee on Science, Space and Technology held a series of hearings evaluating the state of cybersecurity research and development and the recommendations contained within the Review.

Security efforts are often focused on the past, and designed to respond to the most recently faced attack. However, the technology sector is exceptionally dynamic, and where possible, we need to attempt to anticipate vulnerabilities and future threats. This is where research and development and proper coordination can make a contribution.

It has now been a number of years since the Review identified vulnerabilities across federal agencies. We are here today in part to evaluate what progress has been made.

Additionally, as new threats emerge, we must assess whether we are staying ahead with research and development. Finally, we must make sure that we are appropriately tracking federally funded research and development initiatives. Since multiple agencies have cybersecurity responsibilities, and federal efforts in this area are growing, I am concerned that agencies may compete with each other for cyber ownership. Congress must ensure that agencies are working collaboratively to prevent work from being duplicated at the cost of precious taxpayer funds.

Several agencies before us today have an important role in the development of cybersecurity standards. We should not underestimate the value of standards - whether they are minimum security measures for use by federal government agen-

cies to protect information, or a framework to address cybersecurity risks for critical infrastructure. The lead responsibility for working closely with industry to develop successful standards has historically fallen to NIST.

We would like to ensure that any comprehensive cybersecurity legislation effectively leverages the expertise of all federal assets.

I should also note that today's hearing is focused on federal cybersecurity stakeholders. Notably absent are those who design, build, own, and operate the majority of the digital infrastructure in our nation. To that end, I intend to further the discussion of related cybersecurity issues through future hearings of the Technology and Innovation Subcommittee that will include voices from the private sector.

I would like to thank my co-Chairman, Congressman Brooks, for sharing leadership on this important hearing. I also thank the witnesses for being here today and I look forward to a productive discussion.

Chairman QUAYLE. I would now like to recognize the gentleman from Oregon, Mr. Wu, for his opening statement.

Mr. WU. Thank you, Mr. Chairman, for calling this very, very important hearing, and thanks to all the witnesses for being with us today.

More and more of our personal information is making its way online and our Nation's entire infrastructure from traffic systems to the electricity grid to manufacturing to our health information is becoming increasingly dependent on secure and reliable access to the Internet, and I can think of few topics more important to this Committee to address than cybersecurity, and in the last Administration it was referred to as the greatest threat to our national security standing today, and I agree with that assessment.

Anyone following the headlines recently knows that cybercrimes are becoming more frequent. Sony's PlayStation network has been repeatedly targeted, exposing the personal information of over 100 million users. A server at NASA was recently targeted, revealing satellite data, and social media sites like Facebook are constantly targeted by phishing scams and other cyberattacks.

I am pleased that this Administration has provided Congress with the legislative framework to consider ways to address various vulnerabilities. The proposal focuses primarily on the role and authority of the Department of Homeland Security in securing nondefense systems. I look forward to working with Chairman Quayle and the other Members of the Subcommittee and the Full Committee to ensure that NIST's expertise in information security is maintained, especially in the development of technical standards and as a facilitator of private sector collaboration.

I am also interested in ensuring that any comprehensive House bill advances cybersecurity research and development and lays out a clear strategy for building a highly skilled federal cyber workforce.

According to OMB, last year federal agencies spent $12 billion on cybersecurity to protect the $80 billion federal information technology infrastructure. Additionally, the Federal Government funds about $400 million in cybersecurity research each year.

Despite this considerable funding and many federal employee hours spent on this issue, the assessment remains the same: Our cybersecurity is insufficient. We need to use existing resources more efficiently and with specific achievable goals in mind.

Previously, federal efforts have been output-oriented, focusing on metrics such as the number of programs, funds spent and the number of interagency working groups rather than outcome-driven. I

am pleased that the current Administration is focusing its efforts on achieving outcomes such as reducing breaches of federal systems and cases of identity theft as well as ensuring the security of smart grid and health IT systems.

It is true that the Administration's Cyberspace Policy Review reemphasized recommendations from previous reports including improving information sharing, bolstering cross-sector coordination, modernizing the research agenda, and enhancing public cybersecurity awareness. But the review was also successful in outlining a concrete vision and set of objectives that have been steadily addressed by the Administration over the last two years. For example, the creation of a national initiative for cybersecurity education to educate consumers about online risks and to provide training to build a skilled cybersecurity workforce—I am fond of saying that some aspects of cybersecurity are rocket science but others are relatively simple like wearing your seat belt or washing your hands—the development of the National Strategy for Trusted Identities in Cyberspace to combat online fraud and strengthen privacy, and the recent release of an international strategy for cyberspace that calls for the development of international standards aimed at preventing barriers to trade, commerce, and an open environment that fosters free expression and innovation around the world. By addressing these recommendations, we are laying the building blocks for a new outcome-based approach to federal cybersecurity.

The 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 has progressed toward meeting the goals and objectives outlined in the Administration's review, the agency's plans going forward, and the impact of the Administration's legislative proposal on their current roles and authorities. This information will help guide the Committee's ongoing efforts to protect our Nation from cyberattacks.

Again, I would like to thank the witnesses for being here today and I look forward to your testimony.

Thank you, Mr. Chairman. I yield back the balance of my time.

[The prepared statement of Mr. Wu follows:]

PREPARED STATEMENT OF RANKING MEMBER DAVID WU

Thank you, Chairman Quayle, for calling this hearing. And thank you to our witnesses for being here today.

More and more of our personal information is making its way online, and our nation's entire infrastructure-from traffic systems and the electricity grid to manufacturing-is becoming increasingly dependent on secure and reliable access to the internet. I can think of few topics more important for this Committee to address than cybersecurity.

Anyone following the headlines recently knows that cybercrimes are becoming more frequent- Sony's PlayStation network has been repeatedly targeted by hackers, exposing the personal information of over 100 million users; a server at NASA was recently targeted revealing satellite data; and social media sites like Facebook are consistently targeted by phishing scams and other cyber attacks.

I'm pleased that the Administration has provided Congress with a legislative framework to consider ways to address various vulnerabilities. The proposal focuses primarily on the role and authority of the Department of Homeland Security in securing non-defense systems.

I look forward to working with Chairman Quayle and the other members of this Subcommittee to ensure that NIST's expertise in information security is maintained-especially in the development of technical standards and as a facilitator of

private-sector collaboration. I am also interested in ensuring that any comprehensive House bill advances cybersecurity research and development and lays out a clear strategy for building a highly-skilled federal cyberworkforce.

According to OMB, last year Federal agencies spent $12 billion on cybersecurity to protect the $80 billion dollar federal information technology infrastructure. Additionally, the Federal government funds about $400 million in cybersecurity research each year.

Despite this considerable funding and many federal employee hours spent on this issue, the assessment remains the same: our cybersecurity is insufficient. We need to use existing resources more efficiently and with specific achievable goals in mind.

Previously, federal efforts have been output oriented-focusing on metrics such as the number of programs, funds spent, and the number of inter-agency working groups-rather than outcome driven. I am pleased that the current Administration is focusing its efforts on achieving outcomes—such as reducing breaches of federal systems and cases of identity theft, as well as ensuring the security of smart grid and health IT systems.

It's true that the Administration's Cyberspace Policy Review re-emphasized recommendations from previous reports—including improving information sharing, bolstering cross-sector coordination, modernizing the research agenda, and enhancing public cybersecurity awareness. But the review was also successful in outlining a concrete vision and set of objectives that have been steadily addressed by the Administration over the last two years. For example:

- the creation of a National Initiative for Cybersecurity Education to educate consumers about online risks and provide training to build a skilled cybersecurity workforce;
- the development of the National Strategy for Trusted Identities in Cyberspace to combat online fraud and strengthen privacy;
- and the recent release of an International Strategy for Cyberspace that calls for the development of international standards aimed at preventing barriers to trade, commerce, and an open environment that fosters free expression and innovation around the world.

By addressing these recommendations, we are laying the building blocks for a new, outcome-based approach to federal cybersecurity. The 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 has progressed toward meeting the goals and objectives outlined in the Administration's review, the agencies' plans going forward, and the impact of the Administration's legislative proposal on their current roles and authorities. This information will help guide the Committee's ongoing efforts to protect our nation from cyber attacks.

I'd like to again thank the witnesses for being here today and I look forward to your testimony. Thank you, Mr. Chairman. I yield back the balance of my time.

Chairman QUAYLE. Thank you, Mr. Wu.

I now recognize the Chairman of the Subcommittee on Research and Science Education, Mr. Brooks, for his opening statement.

Mr. BROOKS. Thank you, Chairman Quayle.

Good morning and welcome to each of our witnesses. As my fellow Chairman already pointed out, our hearing topic today, cybersecurity, is a dynamic issue that plays a role in a myriad of fields from our Nation's infrastructure to our private lives. It is an issue that is not only of interest to the government and industry, but also affects each of us personally.

The Research and Science Education Subcommittee, of which I am the Chairman, shares jurisdiction of this issue with the Technology and Innovation Subcommittee for a number of reasons. In large part, this is due to the essential basic research taking place on cyber-related issues, conducted in large part through the National Science Foundation's Directorate for Computer and Information Science and Engineering (CISE). Likewise, NSF has an important role to fill regarding the cybersecurity workforce pipeline and education.

In addition, the Subcommittee also authorizes and has oversight over the cyber-related work of the interagency Networking and Information Technology Research and Development program, also known as NITRD, which coordinates the Nation's unclassified federal research development efforts in cybersecurity.

Today our witnesses include a number of federal agency representatives who will be able to discuss specific agency priorities related to cybersecurity research and development, as well as the larger issue of collaboration and coordination across the Federal Government.

While I recognize and understand the essential functions of cybersecurity research and development, I am looking forward to an earnest discussion on the recent fiscal year 2012 budget requests. NSF's CISE Directorate requested over $728 million for fiscal year 2012, a 17.7 percent increase over fiscal year 2010. The fiscal year 2012 budget request for the NITRD program is $3.866 billion, a $73 million increase over fiscal year 2010 expenditures. Our role in Congress is to ensure that federal investments are made wisely, and once made, investments must produce significant value for the Nation.

I look forward to our discussion today. Thank you for joining us.

[The prepared statement of Mr. Brooks follows:]

PREPARED STATEMENT OF CHAIRMAN MO BROOKS

Thank you Chairman Quayle. Good morning, and welcome to each of our witnesses. As my fellow Chairman already pointed out, our hearing topic today, cybersecurity, is a dynamic issue area that plays a role in a myriad of fields from our Nation's infrastructure to our private lives. It is an issue that is not only of interest to the government and industry, but also affects each of us personally.

The Research and Science Education Subcommittee, of which I am the Chairman, shares jurisdiction of this issue with the Technology and Innovation Subcommittee for a number of reasons. In large part, this is due to the essential basic research taking place on cyber-related issues, conducted in large part through the National Science Foundation's Directorate for Computer and Information Science and Engineering (CISE). Likewise, NSF has an important role to fill regarding the cybersecurity workforce pipeline and education.

In addition, the Subcommittee also authorizes and has oversight over the cyber-related work of the interagency Networking and Information Technology Research and Development program (NITRD). NITRD (Niter-dee) coordinates the Nation's unclassified federal research development efforts in cybersecurity.

Today our witnesses include a number of Federal agency representatives who will be able to discuss specific agency priorities related to cybersecurity research and development, as well as the larger issue of collaboration and coordination across the Federal government.

While I recognize and understand the essential functions of cybersecurity research and development, I am looking forward to an earnest discussion on the recent FY12 budget requests. NSF's CISE Directorate requested over $728 million for FY12, a 17.7 percent increase from FY10. The FY12 budget request for the NITRD Program is $3.866 billion, a $73 million dollar increase over FY10 expenditures.

Our role in Congress is to ensure that Federal investments are made wisely, and once made, investments must produce significant value for the Nation. I look forward to our discussion today.

Thank you for joining us.

Chairman QUAYLE. Thank you, Mr. Brooks.

The Chair now recognizes Mr. Lipinski for an opening statement.

Mr. LIPINSKI. Good morning. I want to thank you, Chairman Quayle, and also Chairman Brooks for holding this hearing.

I agree with my colleagues' remarks on the nature and severity of the challenges we face in cybersecurity in both the public and

private sectors. Cybercrime is a problem for our national security, for businesses large and small, and for every single American. Like Mr. Wu, I can think of no more important topic for this Committee to address.

While there are several other agencies not here today who also play a significant role in cybersecurity, the three agencies that are represented here are all central to these efforts. I know some of my colleagues will address the cyber efforts of NIST and DHS, so I would like to highlight those of the National Science Foundation.

NSF is the agency overseen by the Research and Science Education Subcommittee and is second only to the Department of Defense in its support for cybersecurity research. In addition, NSF uniquely funds research across the entire range of science and engineering disciplines that are relevant to cybersecurity, and joins only DARPA in supporting truly game-changing research. It is also significant that the Director of the interagency NITRD program is here today since all of the civilian agencies coordinate their cybersecurity R&D activities through NITRD.

I want to highlight one particular area that is often left out of discussions on cybersecurity research needs, and that is the human element of cybersecurity. People are perhaps the most important part of our IT infrastructure, and according to experts, they are also the weakest link in many systems. Better cybersecurity education for both the general public and for current and future IT professionals is vital. However, there is still a lot we don't understand about how humans interact with technology. Therefore, more research into the social and behavioral sciences has the potential to significantly improve the security of our IT systems. I am happy to see that the social, behavioral, and economic sciences directorate at NSF now has a more explicit role in the agency's Trustworthy Computing initiative. In the end, our cybersecurity efforts can only be as strong as our weakest link. I look forward to hearing more from Dr. Jahanian about that.

We last held a series of hearings on cybersecurity in 2009, when I was Chair of the Research and Science Education Subcommittee. We learned at that time about the respective roles of different agencies and we received extensive outside expert testimony. We also learned that a lot had changed since Congress, led by this Committee, enacted the 2002 Cybersecurity R&D Act. That is why last Congress I introduced the Cybersecurity Enhancement Act of 2010, building on the 2002 Act. That bill, like today's hearing, was a joint effort between my Subcommittee and T&I, then chaired by my friend Mr. Wu. Mr. McCaul, who has been a strong leader on cybersecurity issues, joined me as the lead Republican cosponsor, and the bill passed the House by a margin of 422 to 5. Since our bill, like so many others, never made it through the Senate in the last Congress, I am now joining Mr. McCaul in introducing an updated version. We are still making some small modifications, but I am hoping we can introduce the bill soon, perhaps as early as this week. I know the witnesses were asked about this legislation, and I look forward to hearing your thoughts and feedback today.

We are anticipating that our R&D bill will be part of a bigger, bipartisan cybersecurity bill in both the House and Senate. The efforts to move a larger bill have stalled for some time over disagree-

ments about how to assign leadership and coordination responsibilities across the government. I am glad that the President is taking an active role in this discussion, and I hope that the proposal the White House sent up to Congress two weeks ago will help to move efforts along in both chambers. I look forward to working with both my colleagues and the Administration to ensure the development of a strong cyber security strategy.

I want to thank all of our witnesses for being here this morning and I look forward to hearing your testimonies, and I yield back.

[The prepared statement of Mr. Lipinski follows:]

PREPARED STATEMENT OF RANKING MEMBER DANIEL LIPINSKI

Ranking Member, Subcommittee on Research & Science Education

Good morning. I want to thank both Chairman Quayle and Chairman Brooks for holding this hearing. I agree with my colleagues' remarks on the nature and severity of the challenges we face in cybersecurity in both the public and private sectors. Cybercrime is a problem for our national security, for businesses large and small, and for every single American. Like Mr. Wu, I can think of no more important topic for this committee to address.

While there are several other agencies not here today who also play a significant role in cybersecurity, the three agencies that are represented here are all central to these efforts. I know some of my colleagues will address the cyber efforts of NIST and DHS, so I'd like to highlight those of the National Science Foundation. NSF is the agency overseen by the Research and Science Education Subcommittee and is second only to the Department of Defense in its support for cybersecurity research. In addition, NSF uniquely funds research across the entire range of science and engineering disciplines that are relevant to cybersecurity, and joins only DARPA in supporting truly game-changing research. It is also significant that the Director of the interagency NITRD program is here today since all of the civilian agencies coordinate their cybersecurity R&D activities through NITRD.

I want to highlight one particular area that is often left out of discussions on cybersecurity research needs, and that is the human element of cybersecurity. People are perhaps the most important part of our IT infrastructure, and according to experts, they are also the 'weakest link' in many systems. Better cyber security education for both the general public and for current and future IT professionals is vital. However, there's still a lot we don't understand about how humans interact with technology; therefore, more research into the social and behavioral sciences has the potential to significantly improve the security of our IT systems. I am happy to see that the social, behavioral, and economic sciences directorate at NSF now has a more explicit role in the agency's trustworthy computing initiative. In the end, our cybersecurity efforts can only be as strong as our 'weakest link'. I look forward to hearing more from Dr. Jahanian about that.

We last held a series of hearings on cybersecurity in 2009, when I was chair of the Research and Science Education Subcommittee. We learned at that time about the respective roles of different agencies and we received extensive outside expert testimony. We also learned that a lot had changed since Congress, led by this committee, enacted the 2002 Cybersecurity R&D Act. That is why last Congress I introduced the Cybersecurity Enhancement Act of 2010, building on the 2002 Act. That bill, like today's hearing, was a joint effort between my subcommittee and T&I, then chaired by my friend Mr. Wu. Mr. McCaul, who has been a strong leader on cybersecurity issues, joined me as the lead Republican cosponsor, and the bill passed the House by a margin of 422–5. Since our bill, like so many others, never made it through the Senate in the last Congress, I am now joining Mr. McCaul in introducing an updated version. We are still making some small modifications, but I'm hoping we can introduce the bill soon, perhaps as early as this week. I know the witnesses were asked about this legislation, and I look forward to hearing your thoughts and feedback today.

We are anticipating that our R&D bill will be part of a bigger, bipartisan cybersecurity bill in both the House and Senate. The efforts to move a larger bill have stalled for some time over disagreements about how to assign leadership and coordination responsibilities across the government. I am glad that the President is taking an active role in this discussion, and I hope that the proposal the White House sent up to Congress two weeks ago will help to move efforts along in both chambers. I look forward to working with both my colleagues and the Administration to ensure the development of a strong cyber security strategy.

I want to thank all of our witnesses for being here this morning, and I look forward to hearing your testimonies.

Chairman QUAYLE. Thank you, Mr. Lipinski.

If there are Members who wish to submit additional opening statements, your statements will be added to the record at this point.

At this time I would like to introduce our witness panel. Our first witness is Dr. George Strawn, the Director of the National Coordination Office for the Networking and Information Technology Research and Development program. Prior to his appointment as Director at NITRD, Dr. Strawn served as the Chief Information Officer at the National Science Foundation.

Next is Dr. Farnam Jahanian, Assistant Director of the Directorate for Computer and Information Science and Engineering at the National Science Foundation. Prior to joining NSF, Dr. Jahanian served as Chair of Computer Science and Engineering at the University of Michigan.

Next is Ms. Cita Furlani, the Director of the Information Technology Laboratory at the National Institute of Standards and Technology. Previously, Ms. Furlani has served as Director of the National Coordination Office for Information Technology, Research and Development.

Finally, we will hear from Rear Admiral Michael A. Brown, Director of Cybersecurity Coordination at the Department of Homeland Security. Rear Admiral Brown is also assigned as the DHS Senior Cybersecurity Representative to the United States Cyber Command.

As our witnesses should know, spoken testimony is limited to five minutes each after which the Members of the Committee will have five minutes each to ask questions.

I now recognize our first witness, Dr. George Strawn, the Director of the National Coordination Office for the Networking and Information Technology Research and Development program.

STATEMENT OF DR. GEORGE STRAWN, DIRECTOR, NATIONAL COORDINATION OFFICE, NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT PROGRAM

Dr. STRAWN. Thank you, and good morning. As you say, I am George Strawn, Director of what we call the NCO, National Coordinating Office, of Networking and Information Technology Research and Development, called both NITRD or NITRD, as the case may be. I will use those shorthands, NCO and NITRD, in the rest of my comments in the interest of brevity.

With Dr. Farnam Jahanian of NSF, I also co-Chair the NITRD Subcommittee of the National Science and Technology Council. I would like to thank Chairman Brooks, Chairman Quayle, Ranking Members Lipinski and Wu, and the Members of the Subcommittee for this opportunity to come before you today to discuss protecting information in the digital age and NITRD's role in federal efforts to improve cybersecurity.

The NITRD program provides for the coordination of research and development in networking and information technology across 14 federal agencies and many other partners. Their combined efforts represent America's primary investment in research and de-

velopment for IT-related technologies in general and cybersecurity in particular. The NCO supports the coordination of the activities of the NITRD program.

My written testimony responds to each of the five questions posed by the Subcommittees. In my oral comments today, I just want to highlight three points.

First, the NITRD community strongly believes that this Nation's cybersecurity infrastructure must be made more secure and trustworthy than it is today if we are to sustain our technological and economic leadership role in the global information age. Indeed, the agency developed NITRD's strategic plan. One of the most significant tests of technological leadership will be the ability to engineer and build IT systems that inspire high levels of confidence because they function as intended: safely, securely, reliably and cost-effectively. The agencies added that fundamental research to ensure that digital networks, systems, devices, applications and communication processes earn and deserve the trust and confidence of society, thus constitutes an essential foundation for the Nation's future. Advancing our IT capabilities with radically improving cybersecurity technologies directly supports such U.S. priorities as national and homeland security, economic innovation, global competitiveness, health care reform and job creation.

My second point is that because cyberspace interconnects us all, both the problems and solutions of cybersecurity transcend any one federal agency, any one sector or even any one nation. They involve not just a small number of discrete technologies but global scale interdependencies among a vast array of technologies. The scope and complexity of these cybersecurity challenges absolutely requires effective coordination of research and development between the federal agencies themselves as well as collaboration with our private sector partners, and this is the central role of the NITRD program. This coordination process is exemplified by NITRD's two cybersecurity and information assurance groups, one called a Senior Steering Group, the other called an interagency working group, which have responded to the Cyberspace Policy Review with innovative conceptual framework for R&D intended to radically change the game of cybersecurity in favor of the defendants.

NITRD's recently developed strategic plan for federal R&D and cybersecurity brings me to my third point. Visionary federal R&D in cybersecurity is necessary but not sufficient. Much of cybersecurity infrastructure is in the private sector and much of it is overseas. Federal strategic plan for R&D in cybersecurity expressly calls for new forms of federal outreach and partnerships with the private sector and international stakeholders to accelerate the deployment of promising research into commercial applications and adoption. This transition to practice is currently exemplified in a variety of interagency projects of NITRD members and within several of the NITRD working groups.

Thank you for your interest in cybersecurity and the opportunity to appear before you today. The NITRD community looks forward to working with you to realize the goal of a cyberspace in which we can all have trust and confidence.

[The prepared statement of Mr. Strawn follows:]

PREPARED STATEMENT OF DR. GEORGE O. STRAWN, DIRECTOR, NATIONAL COORDINATION OFFICE FOR NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT

Good morning. I am George Strawn, Director of the National Coordination Office (NCO) for Networking and Information Technology Research and Development (NITRD). With my colleague, Dr. Farnam Jahanian of the National Science Foundation (NSF), I co-chair the NITRD Subcommittee of the National Science and Technology Council's (NSTC) Committee on Technology. I want to thank Chairman Brooks and Chairman Quayle, Ranking Members Lipinski and Wu, and members of the Subcommittees for the opportunity to come before you today to discuss protecting information in the digital age and NITRD's role in Federal efforts to improve cybersecurity.

The NITRD Program—now in its 20th year—provides a coordinated view of the Government's portfolio of unclassified investments in fundamental, long-term research and development (R&D) in advanced networking and information technology (IT), including cybersecurity and information assurance. All of the research reported in this portfolio is managed, selected, and funded by one or more of the 14 member agencies under their own individual appropriations. In addition to cybersecurity, the Program's current research areas are high-end computing, large-scale networking, human-computer interaction and information management, high-confidence software and systems, software design and productivity, and socioeconomic, education, and workforce implications of IT. Advances in these areas further our nation's goals for national defense and national security, economic competitiveness, energy and the environment, health care, and science and engineering leadership.

Response to the Committee Request

Your invitation to testify here today asked me to address five specific questions. But I would like to preface my comments with the general statement that the NITRD agencies strongly concur that improving the overall security of our cyber infrastructure—including computing systems, mobile devices, networks, digitally controlled critical infrastructures, and the vast quantities of information that now flow through cyberspace—is a critical national challenge. It is imperative that we successfully address this challenge, not only to strengthen our national security but also to sustain the technological leadership that drives our economic innovation, global competitiveness, and science and engineering preeminence, and supports our quality of life as Americans.

The 2010 strategic plan for NITRD developed by the Program's 14 member agencies (and now awaiting White House sign-off) describes "trust and confidence" in our systems, networks, and information as one of three fundamental prerequisites for a bright U.S. future. The NITRD Plan states:

"The perspective of the NITRD agencies is that one of the most significant tests of technological leadership in the years ahead will be the ability to engineer and build IT systems that inspire high levels of confidence because they function as intended—safely, securely, reliably, and cost-effectively. Fundamental research to ensure that digital networks, systems, devices, applications, and communications processes earn and deserve the trust and confidence of society thus constitutes an essential foundation for the Nation's future."

The 14 NITRD member agencies and some two dozen other participating agencies represent the broad spectrum of Federal interests in networking and information technology R&D related to cybersecurity—such as national defense and intelligence capabilities; health records privacy and confidentiality; the security of the national power grid; the reliability and functionality of the air-traffic-control system; the integrity and persistence of scientific research data; and the maintenance of secure real-time communications systems in emergency response, weather forecasting, and the financial markets; and many other key national purposes. The role of the NITRD Program in advancing the Government's cybersecurity efforts is to identify the technologically hard but critical problems and coordinate effective research and development to address them.

The Program's framework of regular and ongoing interagency coordination enables the varied agencies to identify significant leverage, target common critical needs, avoid duplication of effort, maximize resource sharing, and partner in investments to pursue higher-level goals. Moreover, because NITRD research is performed in universities, Federal research centers and laboratories, Federally funded R&D centers, and in partnerships with private companies and nonprofit organizations across the country, continuous interaction, information exchange, and feedback takes place, providing new perspectives and insights to both Federal and private-sector stakeholders.

Initiatives #4 and 9 of the Comprehensive National Cybersecurity Initiative (CNCI) called for coordinating R&D efforts and developing enduring "leap-ahead" technology, strategies, and programs. The President's Cyberspace Policy Review builds on these goals to include developing a framework for research and development strategies that focus on game-changing technologies. The NITRD program has a key role in pursuing these goals. Research coordination has been strengthened through the establishment of a Cybersecurity and Information Assurance (CSIA) Senior Steering Group (SSG; made up of budget-level officials). The SSG, in close cooperation with the Special Cyber Operations Research and Engineering group (SCORE: convened by the Office of Science and Technology Policy and the Office of the Director of National Intelligence) enables effective coordination between the classified and unclassified Federal IT security R&D portfolios. This strong framework for coordination and the partnerships it has engendered enabled a comprehensive response to the near- and mid-term action items of the Cyberspace Policy Review as described in my answer to question #2 below.

While individual members of the NITRD community are likely to be involved in multiple elements of the near- and mid-term action plans, I would like to focus on three of these in which NITRD, supported by the NCO, has a prominent role:

Near-term Action Plan #9: Develop a framework for research and development strategies that focus on game-changing technologies that have the potential to enhance the security, reliability, resilience, and trustworthiness of digital infrastructure; provide the research community with access to event data to facilitate developing tools, testing theories, and identifying workable solutions.

Over the last two years, NITRD's CSIA IWG and SSG have engaged in an intensive round of public discussions, brainstorming, and thorough technical examinations of cybersecurity issues in order to develop just such a game-changing R&D framework. The result is the soon-to-be-released Federal cybersecurity R&D strategic plan, "Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program." The strategic plan provides game-changing themes to direct R&D efforts towards understanding the underlying root causes of known current threats with the goal of disrupting the status quo with radically different approaches. The four themes serve as a framework to unify cybersecurity R&D activities. The themes are: Designed-In Security (DIS), Tailored Trustworthy Spaces (TTS), Moving Target (MT), and Cyber Economic Incentives (CEI), with focus areas on wireless mobile networks in the TTS theme and nature-inspired solutions and a deep understanding of cyberspace in the MT theme.

The process of building the R&D strategic plan began with a Leap-Ahead Initiative, developed by the White House Office of Science and Technology Policy (OSTP) and the CSIA SSG. The initiative solicited public inputs and received more than 200 responses on ideas for how to change the cybersecurity landscape. These ideas were distilled into five fundamentally game-changing concepts in cybersecurity and provided as inputs to the National Cyber Leap Year Summit held August 17–19, 2009, in Arlington, Virginia. The summit gathered innovators from the academic and commercial sectors to explore these concepts. The outcomes of the summit were distilled into the three game-changing R&D themes. In FY 2010, the themes were provided as inputs to the Administration's cybersecurity R&D agenda and introduced to the research community as strategies for public-private actions to secure the Nation's digital future. Since the Summit, as the understanding of cyberspace has evolved, a new theme—Designed-In Security (DIS)—has been added to the Federal cybersecurity R&D plan. The next phase in this effort will be to develop, with private-sector input, a roadmap to implement the strategic plan.

An important new strategic thrust introduced in the Federal cybersecurity R&D plan is to develop a science of security. A science of security is needed to ground research efforts and would have the potential of producing hypotheses subject to experimental validation and universal concepts that are predictive and transcend specific systems, attacks, and defenses. Within 10 years, the aim is to develop a scientific framework that applies to real-world settings and provides explanatory value. The CSIA agencies are working with private-sector stakeholders to identify real-world data sets that can be used for research experimentation and testing without compromising privacy or proprietary and sensitive information.

Mid-term Action Plan #3: Expand support for key education programs and research and development to ensure the Nation's continued ability to compete in the information age economy.

The portfolio of research and development activities sponsored by the NITRD agencies constitutes this country's only full-spectrum IT R&D enterprise, and thus these activities represent a unique resource for seeding U.S. innovation of all kinds. In addition, NITRD funding represents the single largest source of support for the education and training of new generations not only of U.S. IT research leaders but

of IT entrepreneurs and technical experts in many fields of endeavor. Our Nation's investments in this NITRD portfolio in general, and in its cybersecurity-related components in particular, have increased along with the critical roles that these technologies play in our information age economy. NITRD agencies now support multiple NCO-coordinated activities impacting research and development, education, and workforce readiness for cybersecurity and the protection of our Nation's critical infrastructure and its entire economy. Nevertheless, all recognize that the challenge remains large and growing.

Mid-term Action Plan #11: Encourage collaboration between academic and industrial laboratories to develop migration paths and incentives for the rapid adoption of research and technology development innovations.

The forthcoming Federal cybersecurity R&D plan specifically addresses the need to accelerate the transition of R&D to practice. It states that an explicit, coordinated process that transitions the fruits of research into practice is essential if Federal cybersecurity R&D investments are to have significant, long-lasting impact. As part of the transition to practice activities, the Federal cybersecurity research community plans to participate in activities related to technology discovery; test and evaluation; and transition, adoption, and commercialization. Planned activities in technology discovery include, for example, participation in the Information Technology Security Entrepreneurs' Forum (ITSEF) and Defense Venture Catalyst Initiative (DeVenCI). In test and evaluation, NITRD agencies plan to leverage available operational and next-generation networked environments to support experimental deployment, test, and evaluation of novel security technologies in realistic settings in both public- and private-sector environments. For transition, adoption, and commercialization, NITRD agencies plan to participate in the System Integrator Forum (SIF) and Small Business Innovative Research (SBIR) Conferences.

As part of their activities to engage with the cybersecurity research community, senior Federal agency cybersecurity officials are presenting the framework for R&D strategies and themes articulated in the strategic plan to researchers attending the annual IEEE Security and Privacy Symposium, May 22–25, 2011 in Oakland, California.

I would like to note here that the transition to practice is also being addressed by NITRD's Large Scale Networking (LSN) agencies. They have developed an innovative network-performance monitoring technology called perfSONAR, which provides network managers with unprecedented capabilities to evaluate how well their networks are functioning, to find problems, and to recognize anomalies in network security. The LSN agencies are now working with private-sector networks and international research network partners to implement deployment of this powerful new tool. The LSN teams, JET (Joint Engineering Team) and MAGIC (Middleware and Grid Infrastructure Coordination), are also closely involved in transition to practice through their testing and implementation in advanced research networks of security-enhancing technologies such as federated identity management, IPv6, and DNSSec.

NITRD activities are supported by the NCO, which provides logistics as well as expert technical coordinators to support the operations of the Subcommittee and an evolving collection of working groups (such as the CSIA IWG) in which the agencies participate to coordinate their own research and development activities and to plan and oversee joint activities when appropriate. They regularly share plans and developments, host workshops, author papers, and interact with the academic and private sectors as a means of defining and operating the most effective programs of research and development attainable in their subject areas.

The following snapshot examples illustrate how such interagency collaboration can lead to substantially better results in research and development as well as education:

- Partnership for Cyberspace Innovation—a partnership of NIST, the Science and Technology Directorate of DHS, and the Financial Services Sector Coordinating Council (FSSCC), with the goal of speeding the commercialization of cybersecurity research innovations that support our Nation's critical infrastructures. This agreement will accelerate the deployment of network testbeds for specific use cases that strengthen the resiliency, security, integrity, and usability of financial services and other critical infrastructures such as online health services, the Smart Grid, water, and transportation.
- Middleware And Grid Infrastructure Coordination (MAGIC) Team—a partnership of agencies and Federal laboratories including ANL, DHS, DOE/SC, FNAL, LANL, LBL, NASA, NIH, NIST, NOAA, NSF, PNNL, and UCAR, and their industry partners, which improves the Nation's cybersecurity and pri-

vacy environment through research, development, and promotion of Identity Management best practices, standards, and community outreach.

- Joint Engineering Team (JET)—a partnership of agency and research networks including DoD, DOE, NASA, NSF, Internet2, and National Lambda Rail that seeks to improve performance as well as security by coordinating networking testbeds (for optical, cloud, architecture, and networking research) and promoting the deployment in advanced networks of more secure technologies such as IPv6 and DNSSec.
- National Initiative for Cybersecurity Education (NICE)—a partnership led by NIST and including DHS, DoD, NSF, ED, OPM, NSA, DOJ, NSA, ODNI, and others, with the goal of establishing an operational, sustainable, and continually improving cybersecurity education program to foster sound cyber practices that will enhance the Nation's security.
- The SEW–Education subgroup of the NITRD SEW Coordinating Group, with a focus on raising the national profile of computing-related knowledge through fundamental changes in K–12 computer science education. This new group, one of whose co-chairs leads the NIST cybersecurity education initiative, is a participant in the NICE program and is now developing its plan of action.

As Director of the NCO for NITRD, it is always a pleasure for me to describe how, by facilitating the collaborative efforts of representatives from many agencies—by arranging meetings and teleconferences, hosting/supporting workshops and conferences, preparing "zero-th" drafts of brainstorming documents, communicating regularly with NITRD participants, and the like—the NCO helps empower the collective intelligence of the NITRD community to accomplish together far more than any single agency could on its own. I believe the NITRD model of cooperation among very disparate agencies truly works, and has led to significant improvements in research and development as well as strategic planning and for cybersecurity.

As is described above, the NITRD Program currently supports an extensive process of coordination and planning across the Federal agencies involved in research and development. This process has led to the development of the Federal cybersecurity R&D strategic plan, Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program, which defines a set of interrelated priorities for the agencies of the U.S. government that conduct or sponsor R&D in cybersecurity. This plan aligns well with the planning objectives noted in H.R. 4061, and is to be followed by coordinated development of a roadmap of steps guiding its implementation. In this process, NITRD and its agency members have hosted workshops for the exchange of information with academia and the private sector and have requested comments from a wide range of stakeholders including the public. NITRD member agencies are beginning to use language and direction from this coordinated plan in agency research and development activities. We greatly appreciate the interest of the Committee and the Subcommittees represented here today and share your commitment to research and development for better cybersecurity. We look forward to continuing to work closely with you on this shared goal with or without any additional legislation.

The proposed legislation directly promotes greater cybersecurity research and development, education, and workforce needs as one of five parts of its basic approach as outlined in SEC 243 (b). The same section promotes the development and implementation of technical capabilities in support of national cybersecurity goals. Many such technical capabilities of the future will represent the practical implementations of the results of ongoing Federal research and development coordinated in the NITRD Program.

The legislation also calls for research and development in cybersecurity in SEC 243 (c) as an important component of a multifaceted program to foster the development, in conjunction with other governmental entities and the private sector, of essential information security technologies and capabilities for protecting Federal systems and critical information infrastructure, including comprehensive protective capabilities and other technological solutions. Such research and development will be essential not only to better meet existing threats, but to provide the technical and scientific foundation for capabilities to meet emerging threats and developments. The coordination of such research and development, and the transition to practice of its successful results, are key components of the NITRD contributions to improving cybersecurity. The proposed legislation for cybersecurity research and development, as outlined in Sections 243 (c) and (d), thus is consistent and aligns with the R&D coordination in which the NITRD Program engages.

BIOGRAPHY FOR DR. GEORGE O. STRAWN, DIRECTOR, NATIONAL COORDINATION OFFICE, NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT PROGRAM

Dr. George O. Strawn is the Director of the National Coordination Office (NCO) for the Networking and Information Technology Research and Development (NITRD) interagency program. He also serves as the Co-Chair of the Subcommittee on NITRD. The NCO reports to the Office of Science and Technology Policy (OSTP) within the Executive Office of the President.

Dr. Strawn is on assignment to the NCO from the National Science Foundation (NSF), where he most recently served as Chief Information Officer (CIO). As the CIO for NSF, he guided the agency in the development and design of innovative information technology, working to enable the NSF staff and the international community of scientists, engineers, and educators to improve business practices and pursue new methods of scientific communication, collaboration, and decision-making.

Prior to his appointment as NSF CIO, Dr. Strawn served as the executive officer of the NSF Directorate for Computer and Information Science and Engineering (CISE) and as Acting Assistant Director for CISE. Previously, Dr. Strawn had served as the Director of the CISE Division of Advanced Networking Infrastructure and Research, where he led NSF's efforts in the Presidential Next Generation Internet Initiative.

Prior to coming to NSF, Dr. Strawn was a Computer Science faculty member at Iowa State University (ISU) for a number of years. He also served there as Director of the ISU Computation Center and Chair of the ISU Computer Science Department. Under his leadership, ISU became a charter member of MIDNET, a regional NSFNET network; he also lead the creation of a thousand-workstation academic system based on an extension of the MIT Athena system; and under his leadership, the ISU Computer Science department was accredited by the then-new Computer Science Accreditation Board.

Dr. Strawn received his Ph.D. in Mathematics from Iowa State University and his BA Magna Cum Laude in Mathematics and Physics from Cornell College.

Chairman QUAYLE. Thank you very much.

I now recognize our second witness, Dr. Farnam Jahanian, for five minutes.

STATEMENT OF DR. FARNAM JAHANIAN, ASSISTANT DIRECTOR, DIRECTORATE FOR COMPUTER AND INFORMATION SCIENCE AND ENGINEERING, NATIONAL SCIENCE FOUNDATION

Mr. JAHANIAN. Good morning. Chairmen Quayle and Brooks, Ranking Members Wu and Lipinski, and Members of the Subcommittees, I am Farnam Jahanian, Assistant Director for the Computer and Information Science and Engineering Directorate at the National Science Foundation.

As you know, NSF is dedicated to the support of fundamental research in all disciplines to the advancement of science and engineering and to educating a new generation of innovative leaders. I welcome this opportunity to present NSF's investments in cybersecurity research and education this morning.

Investments in unclassified long-term research are critical to an effective national strategy of achieving trustworthy cyberspace. It is important to note that many powerful information technologies deployed today capitalize on fundamental research outcomes generated decades ago. NSF brings the problem-solving capabilities of the Nation's best minds to bear on these challenges. It also promotes connections between academia and industry which help to protect the cyberspace, secure the Nation's critical infrastructure and fuel job growth.

In fiscal year 2011, NSF will invest up to $130 million in cybersecurity research including $55 million in the cross-cutting Trustworthy Computing program at NSF. Its projects range from security at the microscopic level, detecting whether a silicon chip contains a malicious circuit, to the macroscopic level, determining strategies for securing the next generation electrical power grid.

Fundamental research in cryptography, formal specification, verification techniques and security testing all contribute to improved methods for building systems that perform as intended, even in the face of threats. Research in secure programming languages and methodologies, secure operating systems and specialty virtualization mechanisms on which many of the security of cloud computing depends are also prominent in NSF's portfolio. Cybersecurity investments are also made in the subdisciplines of computing and information sciences, for example, in the physical cybersystems, algorithmic foundations and networking programs in my directorate.

Center-scale activities play an important role in NSF's portfolio. The Trust Center, a multidisciplinary collaborative research effort, is focused on science and technology for developing and using secure information systems with almost 30 industrial partners. Four cybertrust centers and two industry-university cooperative centers also focus on a number of foundational challenges. Research outcomes and innovations developed with the funding from NSF and other federal partners are now being used by the private sector and government agencies to protect the Nation's cyber infrastructure. In recent years, research outcomes have led to the formation of numerous startup companies in the IT sector that bring innovative solutions to the marketplace.

Education is embedded in all these projects through the training of graduate students, many of whom will join the cybersecurity workforce. CAREER NSF, most prestigious program for junior faculty, carries specific requirements for the integration of research and education. Research experiences for undergraduates, another NSF program, gives students opportunities to do cybersecurity research. Scholarship for Service program provides tuition at academic institutions in exchange for government service following graduation. To date, this program has provided 1,400 scholarships at 34 institutions and has placed graduates in 30 federal agencies. Advanced technology innovation education program educates technicians and has three regional centers: Cyber Watch in Maryland with 35 community colleges, 15 universities from 20 States and an enrollment of 1,800 students; the CSSIA Center in Illinois, eight institutions from five States with more than 1,400 enrolled; and a third regional center, the CSEC Center in Oklahoma with 45 institutions from eight states and almost 2,000 students enrolled.

NSF has been actively responding to the near-term and midterm action plans outlined in the Cyberspace Review Policy. NSF also participates in the interagency NITRD program, which ensures the coordination of cybersecurity investment across 14 government agencies.

To conclude, the Internet plays a critical role in tightly integrating the economic, political and social fabric of our global society. These interdependencies leave the Nation vulnerable to a wide

range of threats that challenge the security, reliability, availability and overall trustworthiness of all IT resources. In my testimony today, I have emphasized that NSF's investment in cybersecurity research and education allows our society to benefit from a robust, secure, dependable infrastructure that supports all application sectors including those on which our lives depend.

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

[The prepared statement of Mr. Jahanian follows:]

PREPARED STATEMENT OF FARNAM JAHANIAN, PH.D., ASSISTANT DIRECTOR, COMPUTER AND INFORMATION SCIENCE AND ENGINEERING DIRECTORATE

Good afternoon, Chairman Quayle and Chairman Brooks, Ranking Members Wu and Lipinski, and members of the Subcommittees. My name is Farnam Jahanian and I am the Assistant Director of the Computer and Information Science and Engineering Directorate at the National Science Foundation.

I welcome this opportunity to highlight NSF's investments in cyber security research and education. NSF aims to fund cyber security research at the frontiers of knowledge, to capitalize on the intellectual capacity of both young and experienced investigators in our Nation's academic and research institutions, and to partner with other U.S. government agencies and private sector and international organizations to meet the challenges of securing cyberspace. It is important to note that the many powerful information technologies (IT) deployed today around the world capitalize on fundamental research outcomes generated decades ago. An effective national strategy for achieving a cyberspace that is deemed "trustworthy" must include investments in fundamental, unclassified, long-term research. These investments will allow our society to continue to benefit from a robust, secure, dependable cyber infrastructure that supports all application sectors, including those on which our lives depend.

Allow me to share with you some examples of the important contributions made to date by the research community with both NSF and other Federal support. They include:

- Cryptographic schemes and cryptographic-based authentication, enabling today's Internet commerce, supporting secure digital signatures and online credit card transactions;
- Program analyses and verification techniques, enabling the early detection of software vulnerabilities and flaws, which can prevent cyber attacks, such as phishing, worms and botnets;
- New approaches to prevent and mitigate distributed denial of service attacks have helped secure Internet's underlying infrastructure;
- Approaches to identify exploitable flaws in cyber-enabled systems, including automotive control software and medical device software, that have alerted industry to the need for secure software and system development practices;
- Technology to detect and defeat "drive-by downloads" from malicious websites makes web browsing safer for the public;
- Innovative machine learning and data mining approaches used in spam filtering, and methods for detecting attacks, such as those involving credit card fraud;
- CAPTCHAs, the distorted text that only humans—not machines or bots—can decipher, to ensure that it is indeed a human, and not a bot, who is buying a ticket on-line or setting up an email account;
- Open source tools that enable rapid analysis of malware allow for quick detection and mitigation and new methods to study botnets reveal the structure of the underground economy, allowing investigators to make attribution and prevent future attacks from the same sources;
- Better understanding of how humans respond to software security warnings gives designers new models for designing usable and secure systems; and
- The underpinnings for fully homomorphic encryption, which means that we may eventually be able to perform encrypted computations on untrusted platforms (such as on a distributed "cloud" platform), just as today we can send encrypted communications over untrusted networks.

The research contributions listed above and other research outcomes and innovations developed with funding from NSF and other Federal partners are now being used by the private sector and government agencies to protect the nation's cyber infrastructure. Moreover, in recent years, NSF-funded research activities have led to the formation of start-up companies in the IT sector that bring innovative solutions and technologies to the marketplace, fueling job growth, and helping to protect cyber space. By promoting a healthy connection between academia and companies, NSF further enhances its research portfolio in trustworthy computing with foundational concepts and new ideas that are directly relevant to the commercial sector.

While the advances in cyber security research and development (R&D) are many, including those mentioned above, the Nation needs to continue its investments in long-term, game-changing research if our cyber systems are to be trustworthy. As you know, every day, we learn about more sophisticated and dangerous attacks. Why is the cyber security challenge so hard? The general answer is that attacks and defenses co-evolve: a system that was secure yesterday might no longer be secure tomorrow. More specific responses to this question include:

- The technology base of our systems is frequently updated to improve functionality, availability, and/or performance. New systems introduce new vulnerabilities that need new defenses.
- The settings in which our computing systems are deployed and the functionality they provide are not static. With new computing models/platforms, like cloud computing and smart phones, come new content and function, which in turn creates new incentives for attack and disruption.
- The sophistication of attackers is increasing as well as their sheer number and the specificity of their targets.
- Achieving system trustworthiness is not purely a technology problem. System developers, purchasers, operators and users all have a role to play in system security, and ways to incentivize them are required. Security mechanisms that are not convenient will be ignored or circumvented; security mechanisms that are difficult to understand will be ignored.
- Humans can be tricked into performing insecure actions or divulging confidential information through various ruses of clever adversaries.

Emerging Threats

The Internet plays a critical role in tightly integrating the economic, political, and social fabric of global society. These interdependencies leave the Nation vulnerable to a wide range of threats that challenge the security, reliability, availability, and overall trustworthiness of all information technology resources.

An evolution of means and motives. In retrospect, early threats, such as first-generation viruses and worms, while costly and dangerous, did not seriously challenge the availability or security of the Internet. In practice, many attackers simply engaged in acts of vandalism. Quickly, however, global Internet threats underwent a profound transformation—from attacks designed solely to disable all or part of the Internet to those that specifically targeted people and organizations. Driven in large part by financial incentives, attackers learned that these systems offered a valuable resource, both in terms of the personal data they contained and as a resource that could be used for future attacks. Networks of these compromised machines, or botnets, have become the delivery platform of choice and fuel a variety of threats, such as SPAM, identity theft, phishing, and Distributed Denial of Service Attacks (DDoS).

These threats continue to evolve both in the motives of the attackers and the means they employ to achieve their goals. Today, exclusively economic motivations have given way to a wide range of goals, including the desire to project political will into cyber-space, such as the denial of service attacks that shadowed the clashes between Russia and Georgia over the region of South Ossetia in 2008, and the Ghostnet cyber spying operation that infiltrated the computers of embassies, foreign ministries, and the offices of the Dalai Lama in 2009. Both instances serve to highlight the scope of this problem and the difficulty in discovering the persons or nations that launched the attacks. With these changing motivations, attackers continue to innovate with new methods. Attacks continue to increase in size. They are more targeted, sophisticated, and stealthy. Furthermore, these attacks are more effective, propagating through high-level applications and through social engineering.

Future security challenges will follow Internet adoption patterns. While Internet threats are likely to continue along the trajectory outlined above, I believe new security challenges will emerge as attackers shadow Internet adoption patterns.

Mobile Internet use is growing quickly: it will become the predominant global Internet access method by 2014. Tens of thousands of applications available today

support banking, ecommerce, highway navigation, health and wellbeing, and social networking, for example; the future will only bring more varied applications used in all facets of daily life. The current culture that encourages application downloading makes mobile devices especially vulnerable to malware. For example, in 2010, a smart phone weather application downloaded by mobile phone users demonstrated how a malicious attack could quickly co-opt a cohort of smart phones around the globe. Today, we lack the understanding and technology to enforce security policies in these situations.

Machine rooms and data centers have long been a mainstay of commercial information technology support. But new technology now enables the unprecedented aggregation of hardware and software, which is then provided in a comprehensive, highly-elastic service that we call "cloud computing." Cloud providers are adding infrastructure at a rapid rate to support this new model. These opportunities bring new risks. A new trust model is required. Users of cloud computing must place their trust in a third party that could well be sharing its resources with competitors and adversaries. Moreover, the cloud—because it concentrates value—is especially attractive to attackers. The ramifications of these changes require continued research and development; new approaches for protecting cloud infrastructure will be key to its long-term success. For more information on the strengths and weaknesses of cloud computing, see the NIST draft recommendations for information technology policy makers: http://csrc.nist.gov/publications/drafts/800–146/Draft-NIST–SP800–146.pdf.

The trend toward increasingly cyber-enabled systems, i.e., the integration of computation, communication, and control into physical systems, offers new challenges. Healthcare, education, and finance have been at risk of attack for a long time, and physical infrastructure—manufacturing, energy production, and transportation—are now at risk. Recent attacks demonstrate that even facilities not directly connected to the Internet can be targeted.

The Nation's researchers must start building systems whose trustworthiness derives from first principles, i.e., proven assumptions. To do that, NSF is formulating and developing a comprehensive research portfolio around a view of systems that are deemed *trustworthy*, i.e., systems that people can depend on day after day and year after year to operate correctly and safely—from our avionics, mass transit and automobile systems to medical devices operated remotely to save lives on battlefields. Included in this notion of trustworthiness are a number of critical concepts: *reliability* (does it work as intended?); *security* (how vulnerable is it to attack?); *privacy* (does it protect a person's information?); and *usability* (can a human easily use it?). Research needs to be game-changing and forward-looking; new policies and continued focus on cyber security education, public awareness and workforce development are critical to our success.

Given this summary of the emerging threats in cybersecurity and NSF's contributions to these challenges, let me now turn to the issues that were raised by the Subcommittees in the invitation to this hearing.

(1) Please provide a brief overview of the National Science Foundation's (NSF) cybersecurity activities and how research and development is integrated into your agency's mission.

The National Science Foundation funds a broad range of activities to advance cybersecurity research, develop a well-educated and capable workforce, and to keep all citizens informed and aware. Investments in these activities include the Trustworthy Computing program in the Directorate for Computer and Information Science and Engineering, the Scholarships for Service program in the Directorate for Education and Human Resources, the TRUST Science and Technology Center, and many related research projects across Engineering, Mathematical and Physical Sciences, and Office of Cyberinfrastructure programs. As stated in its organic act, NSF's mission is "to promote the progress of science; to advance the national health, prosperity, and welfare; to secure the national defense." Support for basic and applied research is integral to NSF's mission. NSF also supports development activities beyond the stage of research prototypes through its Small Business Innovative Research (SBIR) and Small Business Technology Transfer (STTR) programs and in its support of science and engineering computing infrastructure through its Office of Cyberinfrastructure.

Cybersecurity Research

NSF has been investing in cyber security research for many years. In FY 2011, NSF will invest almost $117 million in fundamental research in the science of trustworthiness and related trustworthy systems and technologies. Approximately one half of this $117 million is allocated to the cross-cutting Trustworthy Computing program, which in FY 2011 is funded at a level of $55 million dollars. Currently,

there are about 500 projects that are active. About a third of these projects includes more than one faculty researcher and all include graduate students. Active awards in the Trustworthy Computing program include $1.2M for support of 19 post-doctoral students as well. In addition to the Trustworthy Computing program, NSF continues to make cyber security investments in the core scientific sub-disciplines of the computing and information sciences, including the foundations of algorithms and information and communications, cyber physical systems, smart health and wellbeing, future internet architectures, networking technology and systems, information integration and informatics, and in the social and economic implications of developing secure, trustworthy systems.

NSF continues to cast a wide net and let the best ideas surface, rather than pursuing a prescriptive research agenda. It engages the cyber security research community in developing new fundamental ideas, which are then evaluated by the best researchers through the peer review process. This process, which supports the vast majority of unclassified cyber security research in the United States, has led to innovative and transformative results. Today, NSF's cyber security research portfolio includes projects addressing security from the microscopic level, detecting whether a silicon chip may contain a malicious circuit, to the macroscopic level, determining strategies for securing the next generation electrical power grid, as well as at the human level, studying online privacy and security behaviors of both adolescents and senior citizens. Fundamental research in cryptography, cryptographic protocol analysis, formal specification and verification techniques, static and dynamic program analysis, security testing methods, all contribute to improved methods for building systems that perform as intended, even in the face of threats. Research in secure programming languages and methodologies, in securing operating systems and especially the virtualization mechanisms and hypervisors on which much of the security of cloud computing architectures depends is also prominent in NSF's portfolio. NSF's researchers are investigating novel methods for detecting when security measures have failed, when intrusions have occurred, and when information may have been altered or stolen. NSF's portfolio includes projects studying security in human-centric systems and in a variety of web application contexts as well as in smart phones, medical devices, and automotive systems.

Aside from single investigator and team awards, NSF also invests in center-scale activities. In FY 2012, NSF will provide the eighth year of funding for the *Team for Research in Ubiquitous Secure Technology* (TRUST) Science and Technology Center (STC). This center, which includes University of California (UC), Berkeley, Carnegie Mellon University, Cornell University, San Jose State University, Stanford University, and Vanderbilt University and many industrial partners, is focused on the development of cybersecurity science and technology that will radically transform the ability of organizations to design, build, and operate trustworthy information systems for the Nation's critical infrastructure by addressing the technical, operational, legal, policy, and economic issues affecting security, privacy, and data protection as well as the challenges of developing, deploying, and using trustworthy systems.

Since 2004, the Trustworthy Computing program has funded four centers. All of these centers are coming to an end this year or next:

- *Trustworthy Cyber Infrastructure for the Power Grid* led by University of Illinois Urbana-Champaign, now transitioned to Department of Energy (DoE) and Department of Homeland Security (DHS) for continued funding

This research creates infrastructure technology that will convey critical information to grid system operators despite partially successful cyber attacks and accidental failures. Security and trust validation techniques are developed that can quantify the trustworthiness of a proposed design with respect to critical properties. An interactive simulator created by the project will allow users to experiment with new power grid cyber-infrastructure design approaches.

- *Cybertrust Center for Internet Epidemiology and Defenses* led by UC San Diego and UC Berkeley

Understanding the scope and emergent behavior of Internet-scale worms seen in the wild constitutes a new science termed Internet epidemiology. To gain visibility into pathogens propagating across the global Internet, the Center has developed and operated an Internet pathogen detection service of unprecedented scale. With this service, the Center has demonstrated the speed and coverage over which such pathogens can spread, and has developed mechanisms for deriving "signatures" of a worm's activity and disseminating these to worm suppression devices deployed throughout the global network.

- *Situational Awareness for Everyone* led by Carnegie Mellon University and University of North Carolina, Chapel Hill

This center focuses on how to make both users and organizations more aware of their cybersecurity situation—the risks they face and how they can deal with them in practice. For organizations, the center has developed tools and techniques focused on network security awareness and management. Some of these tools are now operating in California's inter-campus network as well as Berkeley's and Carnegie Mellon's internal campus networks; industry is also showing concrete interest. The center has also focused on educating children and adults, reaching children through a novel game that educates users about security issues and tailors its behavior for the age and background of the player. It has been tested in Pittsburgh regional school districts and is now available on the Internet.

- ACCURATE led by Johns Hopkins University

The voting system integrity problem is a paradigmatic hard cyber trust problem, requiring trustworthy system architectures, security, integrity, privacy, anonymity, high assurance, and human-machine interfaces. Voting systems must preserve a voter's privacy and anonymity, while also being auditable and transparent. This center has generated new understanding of voting systems and has participated in the California Secretary of State's "Top to Bottom Review" of voting systems.

NSF has also invested in two active industry/university cooperative research centers:

- CITeR: Center for Identification Technology Research (Biometrics) at West Virginia University and the University of Arizona

CITeR focuses on identification of people that includes iris, fingerprint and face recognition and will significantly enhance the research database available for the disciplines involved with security biometrics technologies. Research is needed in large-scale, fully-automated, distributed systems in several applications, ranging from drivers license to passports and visas, for example.

- S2ERC: Security and Software Engineering at Ball State and other universities

S2ERC investigates integrated methods of engineering practical software systems that are able to meet emerging security requirements. This goal is of great importance to both industry and government in order for them to confidently deploy real-world software systems that meet their mission goals in the face of a broad range of security attacks. Participants in S2ERC include Ball State University, DePaul University, Indiana University- Purdue University Fort Wayne, Indiana University—Purdue University Indianapolis, Iowa State University, James Madison University, Pennsylvania State University, Purdue University, University of Illinois at Chicago, University of West Florida, Virginia Polytechnic Institute and State University, and West Virginia University.

Cybersecurity Education

Investments in cybersecurity research are accompanied by investments in cybersecurity education and workforce development. Research undertaken in academia not only engages some of our nation's best and brightest researchers, but because these researchers are also teachers, new generations of students are exposed to the latest thinking from the people who understand it best. And when these students graduate and move into the workplace, they will bring this knowledge and understanding with them. Moreover, faculty members in this dual role of researchers and teachers have incentives to write textbooks and prepare other teaching materials that allow dissemination of their work to a wide audience, including teachers and students nationwide.

Over the years, the Trustworthy Computing program has supplemented its awards by giving small amounts of additional funding to researchers who were willing to bring undergraduates into their labs through the Research Experiences for Undergraduates (REU) program. This program gives many undergraduate students their first hands-on experiences with real science and engineering research projects. In addition, the Trustworthy Computing program has funded up and coming young investigators through the CAREER program that offers NSF's most prestigious awards in support of junior faculty who exemplify the role of teacher-scholars through outstanding research, excellent education and the integration of education and research within the context of the mission of their organizations.

	FY08	FY09	FY10	FY11
TC CAREER awards	15	19	15	17
TC REUs	29	58	23	41

The NSF Directorate for Education and Human Resources (EHR) has focused on increasing the number of professionals with degrees in cybersecurity. An overwhelming majority of these EHR developed professionals were supported by the **Federal Cyber Service: Scholarship for Service (SFS)** and **Advanced Technological Education (ATE)** programs.

The SFS program seeks to increase the number of qualified students entering the field of cybersecurity and to increase the capacity of United States higher education enterprise to produce cybersecurity professionals. The SFS program is an interagency program administered by NSF in collaboration with the Office of Personnel Management (OPM), the Department of Homeland Security (DHS), and the National Security Agency (NSA), among other agencies. SFS was established as a result of a January 2000 Presidential Executive Order that defined the National Plan for Information Systems Protection. The SFS program supports two tracks.

The first track, the **SFS Scholarship Track**, provides funding to colleges and universities to award scholarships to students in the information assurance and computer security fields. A recipient must be a U.S. citizen, a full-time student within two years of graduation, demonstrate academic talent, meet selection criteria for Federal employment, be willing to undergo a background investigation for security clearance and must agree to work for at least two years in the Federal government. To date, the SFS program has provided scholarships to 1400 students with 1100 of them successfully placed in the Federal government. The SFS graduates were employed by more than 30 Federal agencies, including National Security Agency, Department of Homeland Security, Central Intelligence Agency, and Department of Justice.

From 2007 to 2010, twenty-eight awards were made totaling $46.75 million dollars. Currently, SFS Scholarships are offered at 34 institutions, with the largest enrollments at the University of Tulsa, Carnegie Mellon University, Mississippi State, and University of North Carolina.

Calendar Years	SFS Graduates
2002	9
2003	75
2004	152
2005	179
2006	172
2007	157
2008	121
2009	86
2010	116
Total	1067

Students enrolled FY2007-10	
University of Tulsa	107
Carnegie Mellon University	75
Mississippi State	48
University of North Carolina	46
Naval Postgraduate School	44
Idaho State University	42
Syracuse University	35
New Mexico Tech	31
Stoney Brook University	31
Polytechnic University of NY	30
AFIT	28
North Carolina A&T	28
George Washington University	27
Iowa State University	26
Georgia Tech	22
Johns Hopkins University	22

Agency Placement FY 2007-10	
National Security Agency	105
US Navy	51
Department Of Defense	28
Mitre Corporation	27
US Army	26
US Air Force	22
Central Intelligence Agency	19
Sandia Laboratory	19
Department Of Treasury	18
Department Of Commerce	17
Department Of Justice	17
Department Of Homeland Security	13
Federal Reserve System	13
Software Engineering Institute	12
Other	90
Total	477

The second track, the **SFS Capacity Building Track**, provides funds to colleges and universities to improve the quality and increase the production of information assurance and computer security professionals. Examples of projects include: developing faculty expertise in information cybersecurity, creating learning materials and strategies, outreach activities, or other innovative and creative projects, which lead to an increase in the national cyber security workforce. Proposing organizations must demonstrate expertise in cybersecurity education or research. From 2007 to 2010, twenty-four awards were made totaling $5.73 million dollars and covering every region of the country.

With an emphasis on two-year colleges, the **Advanced Technological Education (ATE) program** focuses on the education of technicians for the high-tech-

nology fields, including cybersecurity. Activities may have either a national or a regional focus, but not a purely local one. The ATE program supports projects, centers, and targeted research in technician education. Currently, there are 14 active ATE awards in cybersecurity for a total of $17.1M, including $3M awarded in FY10. Three of these projects have been funded under the Regional ATE Center track, providing $3M for four years for each of the centers.

- **CyberWatch** (Maryland)—The CyberWatch Center is headquartered at Prince George's Community College. The mission of the center is to "increase the quantity and quality of the cybersecurity workforce." It sponsors a K–12 program, college-level model programs and courses, lab resources, articulation agreements, and resources for faculty development. CyberWatch has 50 institutional members, including 35 community colleges and 15 universities from 20 states. More than 1800 students were enrolled in cybersecurity courses at partnering community colleges in 2009.
- **Center for Systems Security and Information Assurance (CSSIA)** (Illinois)—The CSSIA center has developed an associate's degree program in information technology security, and is providing professional development opportunities and curricular materials. CSSIA has 8 institutional members, including 6 community colleges and 2 universities from 5 states—Illinois, Indiana, Michigan, Minnesota, and Wisconsin. Their community college partner institutions enrolled more than 1400 students in cybersecurity courses in 2009.
- **Cyber Security Education Consortium (CSEC)** (Oklahoma)—The CSEC center is "dedicated to building a cybersecurity workforce who will play a critical role in implementing the national strategy to secure cyberspace." The center provides regional training workshops as well as internships in SCADA security and digital forensics. CSEC has 45 institutional members, including 42 community colleges and 3 universities from 8 states—Arkansas, Colorado, Kansas, Louisiana, Missouri, Oklahoma, Tennessee, and Texas. Almost 2000 students enrolled in cybersecurity courses at partnering community colleges in 2009.

(2) Describe NSF's role in meeting the objectives outlined in the near-term and mid-term action plans included in the Cyberspace Policy Review, and detail past progress and future plans for meeting the objectives outlined in the Review.

NSF supported the development of the Cyberspace Policy Review, providing the task force that prepared the review with direct access to an extensive group of academic cyber security researchers. The Cyberspace Policy Review Near-Term Action Plan lists ten items and the Mid-Term Action Plan lists fourteen. The actions most concerned with NSF's mission are discussed below.

Near-term Action Plan #9 calls for (a) developing a framework for research and development strategies that focus on game-changing technologies that can enhance the trustworthiness of the digital infrastructure and (b) providing the research community with access to event data to facilitate developing tools, testing theories, and identifying workable solutions.

(a)Specifically, over the past two years, NSF has participated in a set of activities designed to develop research themes related to game-changing technologies, including the announcement of three such themes last year: Moving Target, intended to raise the costs for attackers; Tailored Trustworthy Spaces, intended to support the creation of trustworthy computing environments that can respond to a range of trust requirements; and Cyber Economic Incentives, intended to help understand how to motivate adoption of trustworthy technologies. NSF has collaborated with its partner agencies in publicizing these themes to the research community and has incorporated them into related research solicitations. In the succeeding year, NSF has participated actively in a working group organized under the Networking Information Technology R&D (NITRD) program's Cyber security and Information Insurance (CSIA) Interagency Working Group (IWG) to develop a strategic plan for the Federal cyber security research and development program. This plan is expected to be released officially before the end of May.

(b)NSF has also actively promoted research access to event data. Although NSF itself does not possess any datasets appropriate for this purpose, it convened a workshop on cyber security data for experimentation in August 2010 that brought companies and organizations that possess such data together with members of the research community who would like to study the data. Several companies have agreed to make data available on their premises, and NSF has invited its researchers to request supplementary funds to support visits to data repositories that are not available for remote access.

Mid-Term Action Plan #3: Expand support for key education programs and research and development to ensure the Nation's continued ability to compete in the information age economy.

As already described above, NSF supports a broad range of cyber security research; in FY2011 NSF will invest almost $117 million in this area; approximately half of this is in the Trustworthy Computing program. The balance of NSF's cyber security investments are made in the many core scientific sub-disciplines of the computing and information sciences. In addition to single and multiple-investigator research grants, NSF has funded a Science and Technology Center, four Center-Scale Activities, and Industry/University Cooperative Research Centers. Education is embedded in virtually all of these research grants through the training of graduate students, many of whom will join the industry or university workforce in cyber security research. NSF CAREER awards, among NSF's most prestigious grants, carry specific requirements for integration of research and education. Cyber security research funds also support the Research Experience for Undergraduates (REU) program to grow student interest in cyber security research. The Scholarships for Service (SFS) program ($52.5 million from 2007–2010) provides tuition scholarships for students enrolled in cyber security programs at a wide range of institutions across the nation in exchange for a commitment to a period of service in a government post following graduation. A component of the SFS program is also devoted to building additional teaching capacity through curriculum and faculty development. The Advanced Technological Education (ATE) program supports cyber security education in fourteen projects.

Mid-Term Action Plan #4: Develop a strategy to expand and train the workforce, including attracting and retaining cyber security expertise in the Federal government.

As described earlier, NSF's Scholarships for Service program, including capacity building grants to support expansion of the educational resources available to train students in cyber security, is a fundamental part of the national strategy to train and expand the workforce in this key area; scholarships under this program carry a commitment for service in the Federal government. Last fall, NSF sponsored a Summit on Education in Secure Software to help identify how to teach students to write programs that cannot easily be subverted. NSF is also participating in the National Initiative for Cyber security Education (NICE) as co-lead with the Department of Education for Formal Cyber security Education. This activity encompasses development of education programs for K–12, higher education, vocational and other discipline-related programs in order to help provide a pipeline of skilled workers for private sector and government.

Mid-Term Action Plan #11: Encourage collaboration between academic and industrial laboratories to develop migration paths and incentives for rapid adoption of research and technology development innovations.

NSF's Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) programs aim to support the transition of successful research projects into the marketplace. These programs have funded several projects related to cyber security in recent years. Of the current active projects, eight have direct linkage to cyber security; these have been awarded about $4.5M to date.

CISE also participates in the Grant Opportunities for Academic Liaison with Industry (GOALI) program, which aims to promote academic-industry partnerships on high risk, transformational research projects. CISE plans to supplement its regular Advisory Committee with a new panel of industry leaders to further promote the adoption of research results by industry.

CISE also encourages academic industry partnerships. For example, as mentioned above, 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 Broadcom, Cisco, eBay, Google, HP, IBM, Intel, Juniper, Microsoft, Oracle/Sun, Qualcom, Raytheon, Symantec, United Technologies, and Yahoo. CISE has similar active engagement with industry across its portfolio, including in four Trustworthy Computing Centers and two Industry & University Cooperative Research Centers.

The following areas—as stated in the Cyberspace Policy Review—are not directly addressable by NSF; however, the Trustworthy Computing Program has invested in foundational research that can facilitate progress.

Mid-Term Action Plan #8: Develop mechanisms for cyber security-related information sharing that address concerns about privacy and proprietary information and make information sharing mutually beneficial.

Example research areas include methods for specifying and enforcing privacy policies, applying new cryptographic schemes to support access control, developing techniques for anonymizing sensitive data, and secure multiparty computation techniques.

Mid-Term Action Plan #9: Develop solutions for emergency communications capabilities during a time of natural disaster, crisis, or conflict while ensuring network neutrality.

Example research areas include communication patterns during emergencies; efficient, robust mesh networks that can operate through disasters; and network architectures for first-responder communications.

Mid-Term Action Plan #13: Implement, for high-value activities (e.g., the Smart Grid), an opt-in array of interoperable identity management systems to build trust for online transactions and to enhance privacy.

Example research areas include biometrics, cryptographic means for securing identities, and access management based on identity and experience.

(3) Please discuss how cybersecurity research and development, education and workforce training, and standards development are coordinated with other relevant agencies;

NSF coordinates its cyber security 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 cyber security research investments.
- In January 2008, President Bush initiated the Comprehensive National Cybersecurity Initiative (CNCI). The current Administration supports and has continued efforts on this initiative. One of the goals of the CNCI is to develop "leap-ahead" technologies that would achieve orders-of-magnitude improvements in cybersecurity. Based on this directive, a NITRD Senior Steering Group (SSG) for Cybersecurity R&D was established to provide a responsive and robust conduit for cybersecurity R&D information across the policy, fiscal, and research levels of the Government. The SSG is composed of senior representatives of agencies with national cybersecurity leadership positions, including: DoD, ODNI, DHS, NSA, NSF, NIST, OSTP, and OMB. A principal responsibility of the SSG is to define, coordinate, and recommend strategic Federal R&D objectives in cybersecurity, and to communicate research needs and proposed budget priorities to policy makers and budget officials, including recommendations to OSTP, OMB, and the Joint Inter-Agency Cyber Task Force (JIACTF). One of CISE's Division Directors is the co-chair of this group.
- The NITRD CyberSecurity and Information Assurance Interagency Working Group (CSIA IWG) coordinates cyber security and information assurance research and development across the thirteen member agencies, including DoD, the Department of Energy (DOE) and the National Security Agency (NSA).
- To facilitate cross conversation between classified and unclassified programs in the Federal government, a coordinating group called Special Cyber Operations Research and Engineering (SCORE) was established, which includes members from the SSG. NSF research is reported in this forum. In the past year, SCORE has organized a series of workshops questioning some commonly held assumptions about technical approaches to cybersecurity; NSF investigators have been active participants.
- Under the auspices of the NITRD program and the CSIA SSG and IWG, NSF and the other member agencies have co-funded and co-sponsored a number of workshops:
  - Science of Security Workshop, co-funded by NSF, NSA, and IARPA (November 16–18, 2008): To discuss the foundations of making security into a science.
  - Usability, Security, Privacy Workshop, hosted by the National Academies' Computer Science and Telecommunications Board (July 21–22, 2009): To advance the study of usability and ways to embed usability considerations into the research, design and development of secure systems.
  - Workshop on Clean-Slate Security Architectures, co-funded by NSF and DARPA (July 28, 2009): To frame a new security architecture that could be the basis of clean-slate networks.

- Workshop on Security Research for the Financial Infrastructure, co-supported by Treasury, DHS and NSF (October 28–29, 2009): To gain a better understanding of the security problems faced by the financial sector and how the research community might help solve those problems.
- Workshop on Cyber Security Data for Experimentation (August 26–27, 2010): To explore options for research access to event data.
- Summit on Education in Secure Software (October 18–19, 2010): To develop a comprehensive agenda focused on the challenges of secure software education.
- NSF Workshop on the Future of Trustworthy Computing (October 27–29, 2010): To provide context and direction for researchers interested in Trustworthy Computing.
- NSF/Microsoft Research Workshop on Usable Verification (November 15–16, 2010): To stimulate advances in the usability of tools for formal verification.
- Workshop on Fundamental Research Challenges for Trustworthy Biometrics (November 8–9, 2010): To identify underlying biometrics research challenges.

• A number of projects have received their seed or beginning funding at NSF and then have been picked up by other agencies as they see the value of applying basic research to their mission challenges. NSF has also encouraged its researchers to take advantage of research assets created by its partner agencies. For example,

- NSF funded the Trustworthy Cyber Infrastructure for the Power Grid Center at UIUC; it has now transitioned to DoE/DHS for continued funding.
- NSF funded the DETER testbed in its early years; it is now wholly funded by DHS.
- NSF encourages its Principal Investigator (PI) community to use the data available from the DHS-funded PREDICT repository to validate and test their ideas.

(4) Please provide feedback on H.R. 4061, the Cybersecurity Enhancement Act of 2009, from the 111th Congress, by commenting on the merits of that bill and any areas that you see room for improvement or changes.

The Cyber Security Research and Development Act of 2002 has been an important asset in stimulating innovative research and development. NSF's activities are well-aligned with the provisions of the existing Act and its proposed enhancement. NSF has been working with the National Coordinating Office (NCO) on a national strategy for research and development, which is one of the key points in the new draft legislation. The addition of usability and social and behavioral factors as areas of research interest is consistent with the path that NSF is currently pursuing, as is the focus on fostering curriculum development on principles and techniques of designing secure software. Calling out investments in center-scale activities is also consistent with the importance that NSF places on funding centers to create visibility and activity around important national challenges. As mentioned above, NSF actively encourages interaction across government, academic, and commercial sectors. CISE plans to supplement its regular Advisory Committee with a new panel of industry leaders to further promote the adoption of research results by industry. In summary, NSF's investments in cybersecurity research, education and workforce development are consistent with the provisions of H.R. 4061.

(5) How would the Administration's proposed cybersecurity legislation impact NSF's cyber security activities?

The National Science Foundation is the Nation's premier agency for advancing fundamental research and education in science and engineering. NSF's mission is to "to promote the progress of science; to advance the national health, prosperity, and welfare; to secure the national defense."

The Administration's proposal is offering a carefully tailored and measured approach that relies on private sector innovation. This proposal will enable cyber infrastructure owners and operators to adopt new strategies and techniques to deal with cyber threats. NSF's R&D investments enable scientific discovery and engineering advances that continuously fuel that innovation.

Conclusions

In my testimony today, I've tried to show that the pace and scope of today's cyber threats pose grand challenges to our national critical infrastructure. I have outlined the investments in NSF's cyber security research and education portfolio, which show progress and significant advances over the years. Nonetheless, the Nation needs to invest in long-term, fundamental and game-changing research if our cybersystems are to remain secure in the future. I have indicated NSF's role in ad-

dressing the Near- and Mid-Term Action Plans included in the Cyberspace Policy Review and have detailed our progress in meeting those objectives. I have also discussed how NSF partners with other agencies and have given examples of many cross-agency activities. Finally, I have provided feedback on H.R. 4061, The Cybersecurity Enhancement Act of 2009, as well as on the Administration's proposed cybersecurity legislation. I appreciate the opportunity to have this dialogue with members of your Subcommittees on these very important topics. With robust sustained support for cyber security research and development in both the executive and legislative branches, there is a unique opportunity to protect our national security and enhance our economic prosperity for decades to come. This concludes my remarks. I would be happy to answer any questions at this time.

BIOGRAPHY FOR DR. FARNAM JAHANIAN, ASSISTANT DIRECTOR, DIRECTORATE FOR COMPUTER AND INFORMATION SCIENCE AND ENGINEERING, NATIONAL SCIENCE FOUNDATION

Farnam Jahanian is the Assistant Director of the Computer and Information Science and Engineering (CISE) Directorate at the National Science Foundation. Prior to joining NSF, he held the Edward S. Davidson Collegiate Professorship in Electrical Engineering and Computer Science at the University of Michigan, where he served as Chair for Computer Science and Engineering from 2007—2011 and as Director of Software Systems Laboratory from 1997—2000. Dr. Jahanian also serves as co-chair of the Networking and Information Technology Research and Development (NITRD) Subcommittee of the NSTC Committee on Technology, providing overall coordination for activities of 14 government agencies.

At CISE, Dr. Jahanian guides the directorate in its mission to uphold the nation's leadership in computer and information science and engineering through its support for fundamental and transformative advances that are a key driver of economic competitiveness and crucial to achieving our major national priorities. With a budget of approximately $618 million, CISE supports ambitious long-term research and innovation, the creation of cutting-edge facilities and tools, broad interdisciplinary collaborations, and education and training of the next generation of computer scientists and information technology professionals with skills essential to success in the increasingly competitive, global market.

Over the last two decades at the University of Michigan, Dr. Jahanian led several large-scale research projects that studied the growth and scalability of the Internet infrastructure and which ultimately transformed how cyber threats are addressed by Internet Service Providers. His work on Internet routing stability and convergence has been highly influential within both the network research and the Internet operational communities. This work was recently recognized with an ACM SIGCOMM Test of Time Award in 2008. His research on Internet infrastructure security formed the basis for the successful Internet security services company Arbor Networks, which he co-founded in 2001. He served as Chairman of Arbor Networks until its acquisition by Tektronix Communications, a division of Danaher Corporation, in 2010.

The author of over 100 published research papers, Dr. Jahanian has served on dozens of national advisory boards and government panels. He has received numerous awards for his research, teaching, and technology commercialization activities. He has been an active advocate for economic development efforts over the last decade, working with entrepreneurs, and frequently lecturing on how basic research can be uniquely central to an innovation ecosystem that drives economic growth and global competitiveness. In 2009, he was named Distinguished University Innovator at the University of Michigan.

Dr. Jahanian holds a master's degree and a Ph.D. in Computer Science from the University of Texas at Austin. He is a Fellow of the American Association for the Advancement of Science (AAAS), the Association for Computing Machinery (ACM), and the Institute of Electrical and Electronic Engineers (IEEE).

Chairman QUAYLE. Thank you very much.

The Chair now recognizes our next witness, Ms. Furlani, for five minutes.

STATEMENT OF MS. CITA FURLANI, DIRECTOR, INFORMATION TECHNOLOGY LABORATORY, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Ms. FURLANI. Thank you very much, Chairmen Quayle and Brooks, Ranking Members Wu and Lipinski, and Members of the Subcommittee. I am Cita Furlani, the Director of the Information Technology Laboratory at the Department of Commerce's National Institute of Standards and Technology. Thank you for the opportunity to appear before you today to discuss NIST's role in protecting information in the digital age.

Since the early 1970s, NIST has developed standards to support federal agencies' information assurance requirements. Through FISMA, Congress 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. The responsibility for the development of FIPS rests with NIST.

NIST works with federal agencies, industry and academic to research, develop and deploy information security standards and the technology that is necessary to protect information systems against threats to the confidentiality, integrity and availability of information and services. Consistent with its mission and with the recommendations of the President's Cyberspace Policy Review, NIST is actively engaged with private sector, academia, non-national security federal departments and agencies, the intelligence community and other elements of the law enforcement and national security communities to coordinate and prioritize cybersecurity research, standards development, standards conformance demonstration, and cybersecurity education and outreach.

Our research activities range from innovations in identity management and verification, to metrics for complex systems, to development of practical and secure cryptography and quantum computing environments, 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 is actively contributing to the objectives of several of the near- and midterm action plan activities from the Cyberspace Policy review.

The National Initiative for Cybersecurity Education represents the evolution of the comprehensive National Cybersecurity Initiative, the work on cybersecurity education, moving it from a federal focus to a broader national focus. NIST has assumed the overall coordination role for this effort and is finalizing a strategic framework and a tactical plan of operation.

NIST and the National Security Agency lead an interagency activity to establish strategic objectives in pursuing the development of timely, technically sound, international voluntary consensus cybersecurity standards including a commitment to the development of an international standards framework. NIST is an active member in each of the groups coordinating cybersecurity R&D among federal agencies including the NITRD CSIA, the SCORE and the Senior Steering Group, all designed to actively share

cybersecurity R&D information across the policy, fiscal and research levels of the government.

NIST participated in the creation of the National Strategy for Trusted Identifies in Cyberspace, which calls for a national program office to coordinate needed federal activities. This office will be led by NIST and will have full access to NIST technical expertise as NIST has been actively involved in the development and interoperability of secure identity management for many years.

NIST believes that effective cybersecurity legislation requires an appropriate balance between short- and long-term goals as well as providing motivation for strong collaborations between federal agencies, industry, academia, state and local governments, and other interested stakeholders. Indeed, the legislation proposed by the Administration is focused on improving cybersecurity for the American people and our Nation's critical infrastructure. NIST looks forward to leveraging its legacy of research, development and standards in this area with other federal and private sector partners.

Thank you for the opportunity today, and I will answer any questions you may have.

[The prepared statement of Ms. Furlani follows:]

PREPARED STATEMENT OF CITA M. FURLANI, DIRECTOR, INFORMATION TECHNOLOGY LABORATORY, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, UNITED STATES DEPARTMENT OF COMMERCE

Chairmen Quayle and Brooks, Ranking Members Wu and Lipinski and Members of the Subcommittees, I am Cita M. Furlani, Director of the Information Technology Laboratory 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 protecting information in the digital age.

As Secretary of Commerce Gary Locke said at the White House during the launch of the U.S. International Strategy for Cyberspace: "To preserve and even improve on people's confidence in cyberspace, we need an environment that not only rewards innovation and empowers entrepreneurs, but one that also is constantly improving upon the integrity of the interactions that take place online." NIST's mission to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life is well positioned to support that goal.

As one of the major research components of NIST, the Information Technology Laboratory (ITL) accelerates, through standards, tests and metrics, the development, deployment and use of secure, usable, interoperable and reliable information systems that enable American businesses to be more innovative competitive. ITL enables world-class measurement and testing through research innovations in the areas of computer science and systems engineering, mathematics, and statistics. We balance our research portfolio to be responsive to pressing national priorities while pursuing research necessary to meet future challenges in measurement science and technology. Our R&D agenda focuses on the following broad program areas: cloud computing, complex systems, cybersecurity, biometrics, health information technology, National Initiative for Cybersecurity Education (NICE), National Strategy for Trusted Identities in Cyberspace (NSTIC), quantum information, pervasive information technology, security automation, smart grid, virtual measurement systems, and voting standards.

ITL addresses technical challenges through an integrated, multidisciplinary and systems approach that emphasizes collaboration with other NIST organizations, the Department of Commerce, other government agencies, the U.S. private sector, standards development organizations, and other national and international stakeholders. Our rich programmatic diversity derives from our mission and mandates like the Federal Information Security Management Act (FISMA), which charges ITL to develop cybersecurity standards, guidelines, and associated methods and techniques. Charged under other legislation, such as the USA PATRIOT Act, the HITECH Act and the Help America Vote Act, we are addressing major challenges

faced by the nation in the areas of homeland security, health IT and electronic voting.

Overview of NIST Cybersecurity Activities

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. 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 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, 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 standards conformance 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 Information Technology, the Smart Grid, biometrics/face authentication, cybersecurity education and training beyond the federal government, 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.

Recognizing the importance of security-related standards beyond the federal government, NIST leads national and international consensus standards activities in cryptography, identity management, biometrics, electronic credentialing, secure network protocols, software and systems reliability, and security conformance testing.

Included in the scope of NIST cybersecurity activities are the usability of systems such as voting machines, electronic health records and software interfaces; network security, including standards and tests for Internet Protocol version 6, Domain Network Security (DNSSec), and wireless network protocols; research in mathematical foundations to determine the security of information systems; the National Software Reference Library, computer forensics tool testing, and mobile device forensics; 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 measurements to achieve end-to-end security over heterogeneous, multi-domain networks; biometrics evaluation, usability, and standards (fingerprint, face, iris, voice/speaker,

multimodal biometrics) and an international competition for a next generation Secure Hash Algorithm (SHA–3).

NIST Role in Cyberspace Policy Review Activities

NIST is actively participating in meeting the objectives of several of the near- and mid-term action plan activities from the Cyberspace Policy review.

National Initiative for Cybersecurity Education

Cyberspace Policy Review Near-Term Action Item 6: Initiate a national public awareness and education campaign to promote cybersecurity

Cyberspace Policy Review Mid-Term Action Item 3: Expand support for key education programs and research and development to ensure the Nation's continued ability to compete in the information age economy

Cyberspace Policy Review Mid-Term Action Item 4: Develop a strategy to expand and train the workforce, including attracting and retaining cybersecurity expertise in the Federal government.

The National Initiative for Cybersecurity Education (NICE) represents the evolution of the Comprehensive National Cybersecurity Initiative (CNCI) work on cybersecurity education. The scope of the initiative has been expanded from a federal focus to a broader national focus. NIST has assumed the overall coordination role for the effort, and is finalizing a strategic framework and a tactical plan of operation to support that framework. This expansion and the overall coordination role by NIST are in response to the President's priorities as expressed in Chapter II, Building Capacity for a Digital Nation, of the President's Cyberspace Policy Review.

NIST is currently readying the NICE strategic plan for public review, which should be available this summer. The strategic plan describes the goals and objectives that support the NICE Vision: *a secure digital nation capable of advancing America's economic prosperity and national security in the 21st century through innovative cybersecurity education, training, and awareness on a grand scale.*

NIST's NICE Team is working to unify and coordinate federal resources to enable the larger national effort to improve cybersecurity awareness, education, and training for the entire country. This effort is targeted to all U.S. citizens of all ages, and all types of professions whether it be academia, federal/state/local government, business partners (small-medium to large size businesses/companies), and local community groups. NICE is comprised of four components.

- Component 1: National Cybersecurity Awareness Campaign, encouraging a national culture of security in cyberspace; lead agency Department of Homeland Security (DHS), supported by Department of Education (ED), National Science Foundation (NSF),
- Department of Defense (DoD), Office of the Director of National Intelligence (ODNI) and others as identified.
- Component 2: Formal Cybersecurity Education, enabling a broader pool of skilled workers for a cyber-secure nation; lead agencies DoED and NSF, supported by Office of Personnel Management (OPM), DHS, National Security Agency (NSA) and others as identified (e.g., Department of Labor)
- Component 3: Cybersecurity Workforce Structure, defining cybersecurity jobs, attraction, recruitment, retention, and career path strategies; lead agency DHS and supported by OPM.
- Component 4: Cybersecurity Workforce Training and Development, enabling the development and maintenance of an unrivaled cyber workforce; lead agencies DHS, DoD and ODNI, supported by OPM, DoED, NSF, and others as identified.

In addition, NIST co-chairs the Networking and Information Technology Research and Development (NITRD) Social, Economic, and Workforce Implications of IT and IT Workforce Development (SEW) Coordinating Group Education Team. The NITRD SEW Education Team was recently established to focus on workforce development, training, and education needs arising from the growing demand for productive information technology-skilled workers and the role of innovative IT applications in education and training. The group is currently developing a draft set of priority federal research areas in education and IT.

International Cybersecurity Policy Framework

Cyberspace Policy Review Near-Term Action Item 7: Develop U.S. Government positions for an international cybersecurity policy framework and strengthen our international partnerships to create initiatives that address the full range of activities, policies, and opportunities associated with cybersecurity.

Cyberspace Policy Review Mid-Term Action Item 12: Use the infrastructure objectives and the research and development framework to define goals for national and international standards bodies

To support the U.S. Government's international cybersecurity policy framework and strengthen our international partnerships, NIST and the National Security Agency lead an interagency activity to establish strategic objectives in pursuing the development of timely, technically sound international voluntary consensus cybersecurity standards. This includes commitment to the development of an international standards framework that:

- Ensures the availability of standards that promote security and resiliency for all U.S. information systems;
- Specifies performance criteria rather than detailed design criteria;
- Is open to innovation; and
- Discourages barriers to international trade.

Game Changing Technologies

Cyberspace Policy Review Near-Term Action Item 9: In collaboration with other EOP entities, develop a framework for research and development strategies that focus on game-changing technologies that have the potential to enhance the security, reliability, resilience, and trustworthiness of digital infrastructure; provide the research community access to event data to facilitate developing tools, testing theories, and identifying workable solutions.

NIST is an active member in the groups that coordinate the cybersecurity research and development agenda for federal agencies. The NITRD Cyber Security and Information Assurance Interagency Working Group (CSIA IWG), co-chaired by NIST, coordinates 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. The Special Cyber Operations Research and Engineering (SCORE) Interagency Working Group works in parallel to the CSIA IWG to coordinate classified cybersecurity R&D. Representatives from both of these groups participate together in the Senior Steering Group (SSG) for CSIA R&D, to actively share cybersecurity R&D information across the policy, fiscal, and research levels of the Government.

In May 2010, the CSIA IWG released its "Cybersecurity Game-Change Research & Development Recommendations," [1] identifying three primary R&D themes to motivate future Federal cybersecurity research activities: (a) Moving Target, (b) Tailored Trustworthy Spaces, and (c) Cyber Economic Incentives. These themes are designed to inspire Federal and private cybersecurity researchers to discover novel solutions to increase the nation's cybersecurity protections. The NITRD CSIA IWG is currently developing a "Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program."

Many of NIST's research activities include standards and technologies that will address the three R&D themes recommended by the CSIA IWG, including, but not limited to,

Multi-Factor Authentication methods

- NIST has successfully initiated an international standards project on anti-spoofing/liveness detection within ISO/IEC JTC 1 SC 37 (Biometrics). This is the first standards projects in this field, with the goal of strengthening the security of biometrics as an authentication factor for unattended applications. NIST is leading an international "team" of co-editors and has completed the first official working draft.
- On March 31, NIST released results from the latest in its series of tests of fingerprint minutiae match-on-card (MOC) implementations. The report, NIST Interagency Report 7477, Revision II, details results for 17 MOC implementations submitted by 12 fingerprint-provider card-provider teams. The study shows that there are now five implementation providers that can meet the error rate requirements for Homeland Security Presidential Directive/HSPD–12 Personal Identify Verification (for biometric matching off card) while being able to process the comparison on a smartcard. This is a great example of successful standards and testing work to provide multi-factor authentication that is a privacy-enhancing solution.

[1] The full document is available at http:1//nitrd.gov/PUBS/CSIA__IWG__%20Cybersecurity__%20GameChange__RD__%20Recommendations__20100513.pdf

- NIST is collaborating with OASIS, ANSI/INCITS M1 and ISO JTC 1 SC 37 in developing web services protocols to enable the use of biometrics as a second factor for remote authentication of users for applications requiring higher levels of assurance. Biometrics and Web services may be combined to enhance mobile identification and remote authentication capabilities.

Foundations of Measurement Science for Information Systems

- Developing measurement and modeling techniques needed to enable the characterization, prediction, and control of the security of dynamic, large-scale interconnected information systems

Emerging Virtual Technologies

- Implementing a cloud computing and virtualization test environment to evaluate the security of virtualization techniques and the cloud computing systems and to develop ideas to mitigate security vulnerabilities in virtualized and cloud systems.
- Leverage the test environment to support some of the Standards Acceleration to Jumpstart Adoption of Cloud Computing (SAJACC) use cases by implementing a proof of concept for supporting the NIST 800–53 security control requirements for low and moderate impact baseline to a cloud computing service model such as infrastructure as a service reference implementation, which includes typical virtual workloads running on commercial hypervisors.
- Define some typical use cases involving migrating virtual workloads from a private cloud to a public or community cloud while demonstrating compliance with the security and audit requirements.

Usability of Security

- Developed an in-depth interview instrument to explore users' perception of online risk, trust, privacy, and their knowledge of computer security terms and mechanisms. The goal of this effort is to understand user's mental models in order to assist in computer security education and training.
- Completed the analysis of the password survey that was performed at NIST. Now analyzing the survey results from all of the Bureaus with the Department of Commerce; the survey closed at the end of April 2011.
- Preparing to implement a second usability pilot based on the lessons learned with the Homeland Security Presidential Directive/HSPD–12 Personal Identify Verification (PIV) pilot at NIST.
- Planning studies to evaluate the tradeoff of error rates in the human limitation between memory and typing and the complexity of the password.

Quantum Computing

- Researching cryptographic algorithms for public key-based key agreement and digital signatures that are not susceptible to cryptanalysis by quantum algorithms. Results are expected to be submitted to relevant standards development organizations.

Mobile Handheld Device Security and Forensics

- Developing tests and methodologies that will improve the security of mobile devices and enable the advancement of the state of the art in mobile device forensics.

Security for Pervasive Systems and Grid Computing

- Investigating trust management frameworks, protocols, and application programming interfaces for generalized pervasive systems security functions.

National Strategy for Trusted Identities in Cyberspace

Cyberspace Policy Review Near-Term Action Item 10: Build a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties interests, leveraging privacy-enhancing technologies for the Nation.

Cyberspace Policy Review Mid-Term Action Item 13: Implement, for high-value activities (e.g., the Smart Grid), an opt-in array of interoperable identity management systems to build trust for online transactions and to enhance privacy.

Under the leadership of the National Cybersecurity Coordinator, a multi-agency team, of which NIST was a substantial partner, created "The National Strategy for Trusted Identities in Cyberspace," which laid out the vision for individuals and organizations to be able to utilize secure, efficient, easy-to-use, and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation. The Strategy calls for a National Program Office to facilitate the carrying out of the Strategy and the development of interoperable tech-

nology standards and policies—an "Identity Ecosystem"—where individuals, organizations, and underlying infrastructure—such as routers and servers—can be authoritatively authenticated. The goals of the Strategy are to promote private sector capabilities for protecting individuals, businesses, and public agencies from the high costs of cyber crimes like identity theft and fraud, while simultaneously helping to ensure that the Internet continues to support innovation and a thriving marketplace of products and ideas in a privacy enhancing manner.

The National Program Office (NPO), to be established within the Department of Commerce, will coordinate the federal activities—including coordination of cooperative public/private efforts—needed to implement NSTIC. The office will be led by NIST with activities involving public policy development and privacy protections to be led by the National Telecommunications and Information Administration. The NPO will have full access to NIST technical expertise, both in the development and acceptance of broad consensus-based standards. NIST has been actively involved in the development and interoperability of secure identity management for many years and recently initiated research into how to make such identity schemes easy to use and hard to misuse.

NIST has hired an internationally recognized expert in identity management to manage the establishment of the NSTIC NPO. NIST has also announced the first in a series of workshops to collect public comments on possible private-sector led governance structures for the Identity Ecosystem. This first workshop will be held June 9–10, 2011 in Washington, D.C. Finally, NIST is working with others in the Department of Commerce to develop and release a Notice of Inquiry to achieve even greater public comment on the issue of governance.

Risk Management Framework

Cyberspace Policy Review Mid-Term Action Item 6: Develop a set of threat scenarios and metrics that can be used for risk management decisions, recovery planning, and prioritization of R&D.

NIST has produced Special Publication 800–34 "Contingency Planning Guide for Federal Information Systems" to assist with planning for system recovery and is currently working on

Special Publication 800–30 revision 1, "Risk Management Guide," which will provide guidance to agencies in threat identification, threat modeling, and threat metrics for use in risk management decisions. The current set of NIST Security Automation specifications includes the Common Vulnerability Scoring System which is a metric-based score for known vulnerabilities in the National Vulnerability Database. This information is used by federal agencies, industry, and internationally as an input to threat metrics for risk based decision making. NIST plans to extend these specifications into additional information areas to further facilitate threat discovery, identification, and measurement.

NIST Cybersecurity Coordination with Other Government Agencies

As mentioned above, NIST is actively engaged with private industry, academia, and other Federal agencies, including those in the NITRD community, in coordination of cybersecurity research and development.

In addition, under the provisions of the National Technology Transfer and Advancement Act (PL 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), the Organization for the Advancement of Structured Information Standards (OASIS), 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 interoperable multi-vendor fingerprint minutia capture and verification;

- Development and demonstration of quantum key distribution;
- Establishment of a national cyber vulnerability database;
- Establishment of U.S. Government IPv6 Test Program;
- Assisting the General Services Administration in deploying DNSSec on the .gov Top Level Domain; and Establishment and oversight of an international cryptographic algorithm and module validation program. (Over 1,440 cryptographic module validation certificates have been issued, representing over 3,100 modules. These modules have been developed by more than 335 domestic and international vendors.)

Cybersecurity Legislation

The President made cybersecurity an Administration priority upon taking office. During the release of his *Cyberspace Policy Review* in 2009, the President declared that the "cyber threat is one of the most serious economic and national security challenges we face as a nation."

Over the past two years, the Administration has taken significant steps to ensure that Americans, our businesses, and our government are building better protections against cyber threats. Departments and agencies have implemented programs to enhance their risk management with regard to federal systems.

NIST believes that effective cybersecurity legislation requires an appropriate balance between short and long term goals, as well as providing motivation for strong collaborations between federal agencies, industry, academia, state and local governments and other interested stakeholders. The proposed legislation is focused on improving cybersecurity for the American people, our Nation's critical infrastructure, and the Federal Government's own networks and computers. NIST looks forward to playing its part, leveraging its legacy of research, development, and standards in this area with other federal and private sector partners.

Conclusion

NIST is actively involved with other federal agencies, industry and academia to address the highest priority cybersecurity research and development needs. NIST's expertise and mission provide the best environment for performing the research necessary to enable the innovative cybersecurity specifications, standards, assurance processes, and training needed for securing U.S. Government and critical infrastructure information systems as well as many other elements of the Nation's digital infrastructure to mitigate the growing threat. Finally, consistent with the NIST 3–Year Planning Report, NIST plans to expand its focus on cybersecurity challenges associated with healthcare IT, the Smart Grid, automation of federal systems security conformance, and cybersecurity game-changing research.

Thank you for the opportunity to testify today on NIST's Federal cybersecurity research and development efforts. I would be happy to answer any questions that you may have.

BIOGRAPHY FOR MS. CITA FURLANI, DIRECTOR, INFORMATION TECHNOLOGY LABORATORY, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Cita M. Furlani is Director of the Information Technology Laboratory (ITL). ITL is one of six research Laboratories within the National Institute of Standards and Technology (NIST) with an annual budget of $120 million, 367 employees, and about 160 guest researchers from industry, universities, and foreign laboratories.

Furlani oversees a research program designed to promote U.S. innovation and industrial competitiveness by developing and disseminating standards, measurements, and testing for interoperability, security, usability, and reliability of information systems, including cybersecurity standards and guidelines for Federal agencies and U.S. industry, supporting these and measurement science at NIST through fundamental and applied research in computer science, mathematics, and statistics. Through its efforts, ITL seeks to enhance productivity and public safety, facilitate trade, and improve the quality of life.

Within NIST's traditional role as the overseer of the National Measurement System, ITL is addressing the hard problems in IT Measurement Research. ITL's research results in metrics, tests, and tools for a wide range of subjects such as complex systems, pervasive information technologies, and virtual measurements, as well as issues of information and software quality, integrity, and usability.

ITL has been charged with leading the nation in utilizing existing and emerging IT to meet national priorities that reflect the broad-based social, economic, and political values and goals of the country. Under the Federal Information Security Management Act, ITL is charged with developing cybersecurity standards, guidelines,

and associated methods and techniques. Under other legislation, such as the USA PATRIOT Act, the Help America Vote Act, and the American

Recovery and Reinvestment Act, ITL is addressing the major challenges faced by the nation in the areas of homeland security, electronic voting, and health information technology.

Furlani has served as the Acting Director of the NIST Advanced Technology Program and as Chief Information Officer for NIST. She previously 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 Networking and Information Technology Research and Development Program.

She has been awarded the Department of Commerce Silver and Bronze Medal Awards.

Chairman QUAYLE. Thank you, Ms. Furlani.

The Chair now recognizes our final witness, Rear Admiral Brown, for five minutes.

STATEMENT OF REAR ADMIRAL MICHAEL A. BROWN, DIRECTOR, CYBERSECURITY COORDINATION, DEPARTMENT OF HOMELAND SECURITY

Admiral BROWN. Good morning, Chairmen Quayle and Brooks, Ranking Members Wu and Lipinski, and distinguished Members of the Committee. It is a pleasure for me to be here today to discuss the important issue of cybersecurity.

My testimony will provide an overview of the current cybersecurity environment, the cybersecurity mission carried out by the National Protection and Programs Directorate, and the coordination of this mission with our public and private sector partners.

As you well know, these operational missions benefit from and drive many of the requirements for the research and development work of the DHS Science and Technology Directorate. We also coordinate closely with our interagency partners such as the National Institute of Standards and Technology in the development and application of cybersecurity standards that are relevant across our mission set. Of note, the legislative proposal recently introduced by the Administration would, if enacted, provide a single statutory authorization which would enable DHS to better fulfill our critical infrastructure and civilian government cybersecurity responsibilities.

As you stated, we are very dependent in digital networks as part of our day-to-day lives. Without a secure cyberspace, many aspects of modern life, our economies, our health care systems and our transportation and communications networks would grind to a halt. DHS's roles and missions reflect a bipartisan agreement as established under the previous Administration and expanded upon under the current Administration. We have several specific roles in cybersecurity.

The first is protecting the federal Executive Branch civilian agencies, in other words, the dot-gov world. The second is leading the protection of critical infrastructure such as power plants, financial markets, communication systems and major transportation hubs. Thirdly, DHS must lead the national response to major cyber incidents. Finally, we lead the educational efforts to raise public awareness about the need for cyber hygiene and responsible use of computers. These missions require a full range of partners includ-

ing other government agencies, the private sector and individual users of the Internet.

At the Department, we believe cyberspace is fundamentally a vibrant civilian space similar to a neighborhood, a library, a marketplace or a workshop. We also know that it can facilitate conflict, exploitation and criminal activity. Just last year, a leading cybersecurity firm reported a 93 percent increase in cyberattacks compared with the year before. DHS's role within that space which constitutes both the dot-gov and the dot-com environments results in unique technical, legal and policy challenges. Our responsibilities cover distributed networks with vastly different ownership, configuration and legal considerations as compared to DOD networks that are relatively closed and owned by DOD.

We have accomplishments. We are moving on several fronts. The Department is deploying an intrusion detection system known as EINSTEIN to protect the dot-gov world and we are providing the latest tools and information to our infrastructure partners to support the financial services, transportation, energy and defense industries, to name a few. We have also deployed fly-away teams to assist private companies as they seek to prevent and combat cyber attacks against their networks. In addition, the Department has spearheaded the development and testing of the first-ever National Cyber Incident Response Plan, which enables us to coordinate the response at all levels. This is not a standalone document. It has been used to respond to significant real-world events this year. We are focused on building a world-class cybersecurity team of professionals, computer engineers, scientists, analysts to secure the Nation's digital assets and critical infrastructure.

From the National Cyber Security Division, we have coordinated with the Science and Technology Directorate for many years on research and development requirements for cybersecurity. Our NCSD's Research and Standards Integration Team communicates regularly our R&D requirements for inclusion in S&T's broad area announcements and Small Business Innovation Research information. The NCSD research is currently working with the S&T to identify and pursue specialized technologies that could be integrated into our operational posture. In the past, while some adopted technologies did not work well, we have worked to prevent this problem in the future, and NCSD is finalizing a technology transition process to ensure these new technologies will deliver the desired functionalities and be compatible. In addition, we have regular, ongoing efforts with NIST in developing standards related to software assurance, smart grid technologies and supply chain risk management.

Thank you, and I look forward to your questions.

[The prepared statement of Admiral Brown follows:]

PREPARED STATEMENT OF RADM MICHAEL BROWN, DIRECTOR, CYBERSECURITY COORDINATION, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, DEPARTMENT OF HOMELAND SECURITY

Chairmen Quayle and Brooks, Ranking Members Wu and Lipinski, and distinguished Members of the Committee, it is a pleasure to appear before you today to discuss the important issue of cybersecurity. My testimony will provide an overview of the current cybersecurity environment, the cybersecurity mission carried out by the National Protection and Programs Directorate (NPPD), and the coordination of this mission with our public and private sector partners. As you well know, these

operational missions benefit from, and drive the requirements for, the research and development work of the DHS Science and Technology directorate. We also coordinate closely with our interagency partners, such as the National Institute of Standards and Technology, in the development and application of cybersecurity standards that are relevant across our mission set.

I look forward to exploring how we might work collaboratively with the Committee, and I applaud the Committee for holding this hearing as a step toward such important cooperation.

Moving forward, we would like to work more closely with you to convey the relevance of cybersecurity to average Americans. Increasingly, the services we rely on for daily life, such as water distribution and treatment, electricity generation and transmission, healthcare, transportation, and financial transactions depend on an underlying information technology and communications infrastructure. Cyber threats put the availability and security of these and other services at risk.

The Current Cybersecurity Environment

The United States confronts a combination of known and unknown vulnerabilities, strong and rapidly expanding adversary capabilities, and a lack of comprehensive threat and vulnerability awareness. Within this dynamic environment, we are confronted with threats that are more targeted, more sophisticated, and more serious.

Sensitive information is routinely stolen from both government and private sector networks, undermining confidence in our information systems, the information collection and sharing process and, as bad as the loss of precious national intellectual capital is, we increasingly face threats that are even greater. We currently cannot be certain that our information infrastructure will remain accessible and reliable during a time of crisis.

We face persistent, unauthorized, and often unattributed intrusions into Federal Executive Branch civilian networks. These intruders span a spectrum of malicious actors, including nation states, terrorist networks, organized criminal groups, or individuals located here in the United States. They have varying levels of access and technical sophistication, but all have nefarious intent. Several are capable of targeting elements of the U.S. information infrastructure to disrupt, dismantle, or destroy systems upon which we depend. Motives include intelligence collection, intellectual property or monetary theft, or disruption of commercial activities, among others. Criminal elements continue to show increasing levels of sophistication in their technical and targeting capabilities and have shown a willingness to sell these capabilities on the underground market. In addition, terrorist groups and their sympathizers have expressed interest in using cyberspace to target and harm the United States and its citizens. While some have commented on terrorists' own lack of technical abilities, the availability of technical tools for purchase and use remains a potential threat.

In the virtual world of cyberspace, malicious cyber activity can instantaneously result in virtual or physical consequences that threaten national and economic security, critical infrastructure, public health and welfare, and confidence in government. Similarly, stealthy intruders can lay a hidden foundation for future exploitation or attack, which they can then execute at their leisure- and at their time of greatest advantage. Securing cyberspace requires a layered security approach. Moreover, securing cyberspace is also critical to accomplishing nearly all of DHS's other missions successfully.

In cyberspace, we need to ensure that the federal environments are secure and that legitimate traffic is allowed to flow freely while malicious traffic is prevented from penetrating our defenses. Similarly, we need to support our state and local government and private sector partners as they secure themselves against malicious activity. Collaboratively, public and private sector partners must use our knowledge of these systems and their interdependencies to prepare to respond should our defensive efforts fail. This is a serious challenge, and DHS is continually making strides to improve the nation's overall operational posture and policy efforts.

The DHS Cybersecurity Mission

The Department of Homeland Security is responsible for helping Federal Executive Branch civilian agencies secure their unclassified networks. DHS also works with owners and operators of critical infrastructure and key resources (CIKR) sectors-whether private sector, state, or municipality-owned-to bolster their cybersecurity preparedness, risk assessment and mitigation, and incident response capabilities. The Department has a number of foundational and forwardlooking efforts under way, many of which stem from the 2008 Comprehensive National Cybersecurity Initiative (CNCI). We are reducing and consolidating the number of external connections federal agencies have to the Internet through the Trusted

Internet Connections (TIC) initiative. Further, DHS continues to deploy its intrusion detection capability, known as EINSTEIN 2, to improve the security of communications entering or leaving the federal government through those TICs. In addition, through the United States Computer Emergency Readiness Team (US–CERT), we are working more closely than ever with our public and private sector partners to share what we learn from EINSTEIN 2 and to deepen our collective understanding, identify threats collaboratively, and develop effective security responses.

In a reflection of the bipartisan nature with which the federal government continues to approach cybersecurity, President Obama determined that the CNCI and its associated activities should evolve to become key elements of the broader national cybersecurity efforts. These CNCI initiatives play a central role in achieving many of the key recommendations of the President's Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure. Following the publication of those recommendations in May 2009, DHS and its components developed a long-range vision of cybersecurity for the Department and the nation's homeland security enterprise, which is encapsulated in the Quadrennial Homeland Security Review (QHSR). The QHSR provides an overarching framework for the Department and defines our key priorities and goals. One of the five priority areas detailed in the QHSR is safeguarding and securing cyberspace. Within the cybersecurity mission area, the QHSR identifies two overarching goals: to help create a safe, secure and resilient cyber environment; and to promote cybersecurity knowledge and innovation.

In alignment with the QHSR, Secretary Napolitano consolidated many of the Department's cybersecurity efforts under the National Protection and Programs Directorate (NPPD). The Office of Cybersecurity and Communications (CS&C), a component of NPPD, focuses on reducing risk to the nation's communications and information technology infrastructures and the sectors that depend upon them, as well as enabling timely response and recovery of these infrastructures under all circumstances. The functions and mission of the National Cybersecurity Center (NCSC) are now supported by CS&C. These functions include coordinating operations among the six largest federal cyber centers. CS&C also coordinates national security and emergency preparedness communications planning and provisioning for the federal government and other stakeholders. CS&C comprises three divisions: the National Cyber Security Division (NCSD), the Office of Emergency Communications, and the National Communications System.

Teamwork-ranging from intra-agency to international collaboration-is essential to securing cyberspace. Simply put, the cybersecurity mission cannot be accomplished by any one agency; it requires teamwork and coordination. Together, we can leverage resources, personnel, and skill/sets that are needed to accomplish the cybersecurity mission.

NCSD collaborates with federal government stakeholders, including civilian agencies, law enforcement, the military, the intelligence community, state and local partners, and private sector stakeholders, to conduct risk assessments and mitigate vulnerabilities and threats to information technology assets and activities affecting the operation of civilian government and private sector critical infrastructures. NCSD also provides cyber threat and vulnerability analysis, early warning, and incident response assistance for public and private sector constituents. To that end, NCSD carries out the majority of DHS' non-law enforcement cybersecurity responsibilities.

National Cyber Incident Response

The President's *Cyberspace Policy Review* called for "a comprehensive framework to facilitate coordinated responses by government, the private sector, and allies to a significant cyber incident." DHS coordinated the interagency, state and local government, and private sector working group that developed the National Cyber Incident Response Plan. The plan provides a framework for effective incident response capabilities and coordination among federal agencies, state and local governments, the private sector, and international partners during significant cyber incidents. It is designed to be flexible and adaptable to allow synchronization of response activities across jurisdictional lines. In September 2010, DHS hosted Cyber Storm III, a response exercise in which members of the domestic and international cyber incident response community addressed the scenario of a coordinated cyber event. During the event, the National Cyber Incident Response Plan was activated and its incident response framework was tested. Based on observations from the exercise, the plan is in its final stages of revision prior to publication.

Cyber Storm III also tested the National Cybersecurity and Communications Integration Center (NCCIC)-DHS' 24-hour cyber watch and warning center-and the federal government's full suite of cybersecurity response capabilities. The NCCIC works

closely with government at all levels and with the private sector to coordinate the integrated and unified response to cyber and communications incidents impacting homeland security.

Numerous DHS components, including US–CERT, the Industrial Control Systems Cyber Emergency Response Team (ICS–CERT), and the National Coordinating Center for Telecommunications (NCC), are collocated into the NCCIC. Also present in the NCCIC are other federal partners, such as the Department of Defense (DoD) and members of the law enforcement and intelligence communities. The NCCIC also physically collocates federal staff with private sector and non-governmental partners.

By leveraging the integrated operational capabilities of its member organizations, the NCCIC serves as an "always on" cyber incident response and management center, providing indications and warning of imminent incidents, and maintaining a national cyber "common operating picture." This facilitates situational awareness among all partner organizations, and also creates a repository of all vulnerability, intrusion, incident, and mitigation activities. The NCCIC also serves as a national point of integration for cyber expertise and collaboration, particularly when developing guidance to mitigate risks and resolve incidents. Finally, the unique and integrated nature of the NCCIC allows for a scalable and flexible coordination with all interagency and private sector staff during steady-state operations, in order to strengthen relationships and solidify procedures as well as effectively incorporate partners as needed during incidents.

Providing Technical Expertise to the Private Sector and Critical Infrastructure

US–CERT provides remote and onsite response support and defense against malicious cyber activity for the Federal Executive Branch civilian networks. US–CERT also collaborates and shares information with state and local government, industry, critical infrastructure owners and operators, and international partners to address cyber threats and develop effective security responses.

In addition to specific mitigation work we conduct with individual companies and sectors, DHS looks at the interdependencies across critical infrastructure sectors for a holistic approach to providing our cyber expertise. For example, the electric, nuclear, water, transportation, and communications sectors support functions across all levels of government including federal, state, local, and tribal governments. Government bodies and organizations do not inherently produce these services and must rely on private sector organizations, just as other businesses and private citizens do. Therefore, an event impacting control systems has potential implications at all these levels, and could also have cascading effects upon all 18 sectors. For example, water and wastewater treatment, chemical, and transportation depend on the energy sector, and failure in one of these sectors could subsequently affect the operations of state, local, or even federal government.

NCCIC's operations are complemented in the arena of industrial control systems by ICS–CERT. The term "control system" encompasses several types of systems, including Supervisory Control and Data Acquisition (SCADA), process control, and other automated systems that are found in the industrial sectors and critical infrastructure. These systems are used to operate physical processes that produce the goods and services that we rely upon, such as energy, drinking water, emergency services, transportation, postal and shipping, and public health. Control systems security is particularly important because of the inherent interconnectedness of the CIKR sectors and their dependence on one another.

As such, assessing risk and effectively securing industrial control systems are vital to maintaining our nation's strategic interests, public safety, and economic well-being. A successful cyber attack on a control system could result in physical damage, loss of life, and cascading effects that could disrupt services. DHS recognizes that the protection and security of control systems is essential to the nation's overarching security and economy. In this context, as an example of the many related initiatives/activities, DHS-in coordination with the Department of Commerce's National Institute of Standards and Technology (NIST), the Department of Energy, and DoD-has provided a forum for researchers, subject matter experts and practitioners dealing with cyber-physical systems security to assess the current state of the art, identify challenges, and provide input to developing strategies for addressing these challenges. Specific infrastructure sectors considered include energy, chemical, transportation, water and wastewater treatment, healthcare and public health, and commercial facilities. A 2010 published report of findings and recommendations is available upon request.

ICS–CERT provides onsite support to owners and operators of critical infrastructure for protection against and response to cyber threats, including incident re-

sponse, forensic analysis, and site assessments. ICS–CERT also provides tools and training to increase stakeholder awareness of evolving threats to industrial control systems.

A real-world threat emerged last year that significantly changed the landscape of targeted cyber attacks on industrial control systems. Malicious code, dubbed Stuxnet, was detected in July 2010. DHS analysis concluded that this highly complex computer worm was the first of its kind, written to specifically target mission-critical control systems running a specific combination of software and hardware.

ICS–CERT analyzed the code and coordinated actions with critical infrastructure asset owners and operators, federal partners, and Information Sharing and Analysis Centers. Our analysis quickly uncovered that this sophisticated malware has the ability to gain access to, steal detailed proprietary information from, and manipulate the systems that operate mission-critical processes within the nation's infrastructure. In other words, this code can automatically enter a system, steal the formula for the product being manufactured, alter the ingredients being mixed in the product, and indicate to the operator and the operator's anti-virus software that everything is functioning normally.

To combat this threat, ICS–CERT has been actively analyzing and reporting on Stuxnet since it was first detected in July 2010. To date, ICS–CERT has briefed dozens of government and industry organizations and released multiple advisories and updates to the industrial control systems community describing steps for detecting an infection and mitigating the threat. As always, we attempt to balance the need for public information sharing while limiting the information that malicious actors may exploit.

Looking ahead, the Department is concerned that attackers could use the increasingly public information about the code to develop variants targeted at broader installations of programmable equipment in control systems. Copies of the Stuxnet code, in various different iterations, have been publicly available for some time now. ICS–CERT and the NCCIC remain vigilant and continue analysis and mitigation efforts of any derivative malware.

ICS–CERT will continue to work with the industrial control systems community to investigate these and other threats through malicious code and digital media analysis, onsite incident response activities, and information sharing and partnerships.

Protecting Federal Civilian Government Networks

In addition to its support of private sector owners and operators of infrastructure, DHS also collaborates with its partners to increase the security of Federal Executive Branch civilian agency networks. As part of the CNCI, DHS works with the Office of Management and Budget (OMB) to reduce and consolidate the number of external connections that federal agencies have to the Internet through the TIC initiative. This initiative reduces the number of potential vulnerabilities to government networks and allows DHS to focus monitoring efforts on limited and known avenues through which Internet traffic must travel. DHS conducts onsite evaluations of agencies' progress toward implementing TIC goals.

In conjunction with the TIC initiative, the EINSTEIN system is designed to provide the U.S. government with an early warning system for intrusions to Federal Executive Branch civilian networks, near real-time identification of malicious activity, and automated disruption of that malicious activity. The first iteration of EINSTEIN was developed in 2003 and automates the collection and analysis of computer network security information from participating agency and government networks to help analysts identify and combat malicious cyber activity that may threaten government network systems, data protection and federal communications infrastructure. The second phase of EINSTEIN, developed in 2008 as part of the CNCI, incorporates intrusion detection capabilities into the original EINSTEIN system. DHS is currently deploying EINSTEIN 2 to Federal Executive Branch civilian agency TIC locations and Networx Managed Trusted Internet Protocol Services (MTIPS) providers, which are private internet service providers that serve federal agencies, to assist them with protecting their computers, networks and information. EINSTEIN 2 has now been deployed at 15 of the 19 large departments and agencies who maintain their own TIC locations. Also, the four MTIPS providers currently provide service to seven additional federal agencies. In 2010, EINSTEIN 2 sensors registered 5.4 million "hits," an average of more than 450,000 hits per month or nearly 15,000 hits per day. A hit is an alert triggered by a predetermined intrusion detection signature that corresponds to a known threat. Each hit represents potential malicious activity for further assessment by US–CERT.

DHS is currently developing the third phase of the EINSTEIN system-an intrusion prevention capability which will provide DHS with the ability to automatically

detect and disrupt malicious activity before harm is done to critical networks and systems. In advance of this development, DHS, in coordination with the National Security Agency (NSA), conducted the CNCI Initiative 3 Exercise. US–CERT successfully met the objectives of the CNCI Initiative 3 Exercise, including the successful deployment of one signature, scenario and countermeasure, and the demonstrated ability to share alert data with DoD. As a result of the countermeasures deployed during the exercise, US–CERT was successful in denying the entry of more than 36,473 potentially malicious threats into the federal agency customer's network infrastructure. The CNCI Initiative 3 Exercise advanced the potential capabilities of the EINSTEIN system by demonstrating defensive technology, sharing near real-time threat information with DoD for enhanced situational awareness, and providing a platform upon which an oversight and compliance process can be implemented for the evolving set of EINSTEIN capabilities. The Department's Privacy Office and its Office for Civil Rights and Civil Liberties carefully reviewed the exercise concept of operations, and the Privacy Office worked with US–CERT to publicly release a detailed Privacy Impact Assessment evaluating the exercise. US–CERT also briefed the exercise to the cyber subcommittee of the independent DHS Data Privacy and Integrity Committee.

Beyond the TIC initiative and the EINSTEIN system, DHS, OMB, and the National Institute for Standards and Technology work cooperatively with agencies across the federal government to coordinate the protection of the nation's federal information systems through compliance with the Federal Information Security Management Act of 2002 (FISMA). US–CERT monitors EINSTEIN 2 sensors for intrusion activity and receives self-reported incident information from federal agencies. This information is reported to OMB for use in its FISMA oversight capacity. In 2010, DHS also began to administer oversight of the CyberScope system, which was developed by the Department of Justice. This system collects agency information regarding FISMA compliance and, as DHS, OMB and their agency partners move toward automated reporting, the system will enable real-time assessments of baseline security postures across individual agencies and the federal enterprise as a whole. This activity complements the development of reference architectures that DHS designs for federal agency stakeholders that are interested in implementing security solutions based on standards and best practices. DHS also works with the General Services Administration to create Blanket Purchase Agreements that address various security solutions for federal agencies.

The DHS Cybersecurity Workforce

As DHS continues to make progress on initiatives such as TIC and EINSTEIN, the Department is also mindful that the cybersecurity challenge will not be solved by a single technology solution. Multiple innovative technical tools are necessary and indeed, technology alone is insufficient. The mission requires a larger cybersecurity professional workforce, governance structures for enhanced partnerships, more robust information sharing and identity protection, and increased cybersecurity awareness among the general public. Responsibility for these solutions is, and will remain, distributed across public and private sector partners.

DHS is focused on building a world-class cybersecurity team by hiring a diverse group of cybersecurity professionals-computer engineers, scientists, and analysts-to secure the nation's digital assets and protect against cyber threats to our critical infrastructure and key resources. NCSD continues to hire cybersecurity and information technology professionals, nearly tripling its cybersecurity workforce in FY 2009 and nearly doubling that number again in FY 2010. NCSD currently has more than 230 cybersecurity professionals on board, with dozens more in the hiring pipeline.

Several initiatives are designed to increase the nation's number of highly qualified cybersecurity professionals. DHS and NSA co-sponsor the Centers of Academic Excellence in Information Assurance Education and Research programs, the goal of which is to produce a growing number of professionals with information assurance expertise in various disciplines. DHS and the Department of State co-hosted Operation Cyber Threat (OCT1.0), the first in a series of government-wide experiential and interactive cybersecurity training pilots designed to apply learning concepts and share best practices in a secure, simulated environment to build capacity within the federal workforce. In December 2010, the Institute of Electrical and Electronics Engineers Computer Society, the world's leading organization of computing professionals, formally recognized the Master of Software Assurance (MSwA) Reference Curriculum, which DHS sponsored through its Software Assurance (SwA) Curriculum Project. The MSwA program is the first curriculum of its kind to focus on assuring the functionality, dependability, and security of software and systems. Finally, DHS co-sponsored the annual Colloquium for Information Systems Security

Education and the Scholarship for Services (SFS) Job Fair/Symposium, which brought together 55 federal agencies and more than 200 SFS students.

The National Initiative for Cybersecurity Education (NICE) has the dual goals of a cyber-savvy citizenry and a cyber-capable workforce. Working with NIST, which is the overall interagency lead, DHS heads the NICE awareness elements and co-leads the training and professional development components with DoD and the Office of the Director of National Intelligence.

Interagency and Public-Private Coordination

Overcoming new cybersecurity challenges requires a coordinated and focused approach to better secure the nation's information and communications infrastructures. President Obama's *Cyberspace Policy Review* reaffirms cybersecurity's significance to the nation's economy and security. Establishment of a White House Cybersecurity Coordinator position solidifies the priority the Administration places on improving cybersecurity.

No single agency controls cyberspace and the success of our cybersecurity mission relies on effective communication and critical partnerships. Many government players have complementary roles-including DHS, the Intelligence Community, DoD, the Department of Justice, the Department of State, and other federal agencies-and they require coordination and leadership to ensure effective and efficient execution of our collective cyber missions. The creation of a senior-level cyber position within the White House ensures coordination and collaboration across government agencies.

DHS works closely with its federal, state and local partners to protect government cyber networks. In September 2010, DHS and DoD signed a memorandum of agreement that aligns and enhances America's capabilities to protect against threats to our critical civilian and military computer systems and networks, including deploying a National Security Agency support team to the NCCIC to enhance the National Cyber Incident Response Plan and sending a full-time senior DHS leader and support team to the National Security Agency.

This initiative builds upon pre-existing liaison exchanges DHS has with the National Security Agency/Central Security Service Threat Operation Center (NTOC), United States Cyber Command and United States Northern Command. Liaisons to DHS operate out of US–CERT and the NCCIC. The initiative also further supports DHS' already active partnership with DoD. The partnerships ensure that agile coordination and technical capabilities support any cyber contingency.

In November 2010, the Multi-State Information Sharing and Analysis Center (MS–ISAC) opened its Cyber Security Operations Center, a 24-hour watch and warning facility, which will both enhance situational awareness at the state and local level for the NCCIC and allow the federal government to quickly and efficiently provide critical cyber risk, vulnerability, and mitigation data to state and local governments. An MS–ISAC analyst/liaison is collocated in the NCCIC.

Private industry owns and operates the vast majority of the nation's critical infrastructure and cyber networks. Consequently, the private sector plays an important role in cybersecurity, andDHS has initiated several pilot programs to promote public-private sector collaboration. In its engagement with the private sector, DHS recognizes the need to avoid technology prescription and to support innovation that enhances critical infrastructure cybersecurity.

In February 2010, DHS, DoD, and the Financial Services Information Sharing and Analysis Center (FS–ISAC) launched a pilot designed to help protect key critical networks and infrastructure within the financial services sector by sharing actionable, sensitive information. In June 2010, DHS implemented the Cybersecurity Partner Local Access Plan, which allows security-cleared owners and operators of CIKR, as well as state technology officials and law enforcement officials, to access secret-level cybersecurity information and video teleconference calls via state and local fusion centers. In November 2010, DHS signed an agreement with the Information Technology Information Sharing and Analysis Center (IT–ISAC) to embed a fulltime IT–ISAC analyst and liaison to DHS at the NCCIC, part of an ongoing effort to collocate private sector representatives alongside federal and state government counterparts. The IT–ISAC consists of information technology stakeholders from the private sector and facilitates cooperation among members to identify sector-specific vulnerabilities and risk mitigation strategies.

In December 2010, DHS and NIST signed a Memorandum of Understanding with the Financial Services Sector Coordinating Council. The goal of the agreement is to speed the commercialization of cybersecurity research innovations that support our nation's critical infrastructures. This agreement will accelerate the deployment of network testbeds for specific use cases that strengthen the resiliency, security, integrity, and usability of financial services and other critical infrastructures.

In July 2010, DHS worked extensively with the White House on the publication of a draft National Strategy for Trusted Identities in Cyberspace, which seeks to secure the digital identities of individuals, organizations, services and devices during online transactions, as well as the infrastructure supporting the transaction. This fulfills one of the near-term action items of the President's Cyberspace Policy Review. The strategy is based on public-private partnerships and supports the protection of privacy and civil liberties by enabling only the minimum necessary amount of personal information to be transferred in any particular transaction. Its implementation will be led by the Department of Commerce.

Public Education and Outreach

While considerable activity is focused on public and private sector critical infrastructure protection, DHS is committed to developing innovative ways to enhance the general public's awareness about the importance of safeguarding America's computer systems and networks from attacks. Every October, DHS and its public and private sector partners promote efforts to educate citizens about guarding against cyber threats as part of National Cybersecurity Awareness Month. In March 2010, Secretary Napolitano launched the National Cybersecurity Awareness Challenge, which called on the general public and private sector companies to develop creative and innovative ways to enhance cybersecurity awareness. In July 2010, seven of the more than 80 proposals were selected and recognized at a White House ceremony. The winning proposals helped inform the development of the National Cybersecurity Awareness Campaign, *Stop. Think. Connect.*, which DHS launched in conjunction with private sector partners during the October 2010 National Cybersecurity Awareness Month. *Stop. Think.Connect*, a message developed with the private sector, has evolved into an ongoing national public education campaign designed to increase public understanding of cyber threats and how individual citizens can develop safer cyber habits that will help make networks more secure. The campaign fulfills a key element of President Obama's *Cyberspace Policy Review*, which tasked DHS with developing a public awareness campaign to inform Americans about ways to use technology safely. The campaign is a component of the NIST National Initiative for Cyber Education (NICE).

Throughout its public and private sector activities, DHS is committed to supporting the public's privacy, civil rights and civil liberties. Accordingly, the Department has implemented strong privacy and civil rights and civil liberties standards into all of its cybersecurity programs and initiatives from the outset. To support this, DHS established an Oversight and Compliance Officer within NPPD, and key cybersecurity personnel receive specific training on the protection of privacy and other civil liberties as they relate to computer network security activities. In an effort to increase transparency, DHS also publishes privacy impact assessments on its website, www.dhs.gov, for all of its cybersecurity systems.

Conclusion

Set within an environment characterized by a combination of known and unknown vulnerabilities, strong and rapidly expanding adversary capabilities, and a lack of comprehensive threat and vulnerability awareness, the cybersecurity mission is truly a national one requiring collaboration across the homeland security enterprise. The Department of Homeland Security is committed to creating a safe, secure and resilient cyber environment while promoting cybersecurity knowledge and innovation. We must continue to secure today's infrastructure as we prepare for tomorrow's challenges and opportunities. It is important to recognize that we do not undertake cybersecurity for the sake of security itself, but rather to ensure that government, business and critical societal functions can continue to use the information technology and communications infrastructure on which they depend. We are confident that the cyber legislative proposal put forward by the Administration will, if enacted, enhance our ability to more effectively execute our cybersecurity missions.

Distinguished Members of the Committee, let me end by reiterating that I look forward to exploring opportunities to advance this mission in collaboration with the Committee and my colleagues in the public and private sectors. Thank you again for this opportunity to testify. I would be happy to answer your questions.

Rear Admiral Michael A. Brown
Director, Cybersecurity Coordination

Rear Admiral Michael A. Brown serves as director, Cybersecurity Coordination (DCC) in the National Protection and Programs Directorate (NPPD) for the Department of Homeland Security (DHS). In this position, he is responsible for increasing interdepartmental collaboration in strategic planning for the Nation's cybersecurity, mutual support for cybersecurity capabilities development, and synchronization of current operational cybersecurity mission activities for the Departments of Homeland Security and Defense. He is also assigned as the DHS senior cybersecurity representative to the United States Cyber Command. Brown previously served as the DHS deputy assistant secretary, Cybersecurity and Communications and as assistant deputy director Joint Interagency Task Force, Office of the Director of National Intelligence.

Brown has assisted and led the Navy's efforts and development in Information Operations (IO) and cyberspace. Prior to his assignment to DHS, Brown served as director, Information Operations Division (OPNAV N3IO) and deputy director for Cryptology Division (N2C), at the Navy Staff in Washington, DC. Additionally, he was designated as the special assistant for Signals Intelligence (SIGINT) and IO to commander, Naval Network Warfare Command. In this position he led the Navy's expansion of its operational role in cyberspace.

In 2005, Brown served as deputy commander and chief of staff for the Commander, Naval Security Group Command where he was selected to the Flag rank.

Brown has served in several key roles in Naval Information Warfare and Intelligence including commanding officer, Naval Information Warfare Activity (NIWA) in Suitland, Md., where the command revolutionized tactical naval IO capabilities across the fleet, assuring naval commanders were equipped and prepared to operate around the world. He has held various fleet, joint and national positions throughout his career.

He graduated from the U.S. Naval Academy in 1980 with a Bachelor of Science in Mathematics and holds a Master of Science in Systems Engineering (Electronic Warfare) from the Naval Postgraduate School, a Master of Arts in National and Strategic Studies for the Naval War College, and is designated an Acquisition Professional.

Brown is authorized to wear the Legion of Merit (four awards), the Defense Meritorious Service Medal, the Meritorious Service Medal (two awards), the Navy and Marine Corps Commendation Medal (two awards), the Joint Service Achievement Medal, the Navy and Marine Corps Achievement Medal and a host of unit and campaign service medals.

Chairman QUAYLE. I would like to thank the whole panel for their testimony today. Now, I want to remind Members that Committee rules limit questioning to five minutes. The Chair will at this point open the round of questions, and I will recognize myself for five minutes.

My first question is to you, Dr. Strawn. In your testimony, you stated that the research in NITRD's portfolio is managed, selected and funded by one or more of the 14 member agencies under their own individual appropriations. Now, my question is, how do we avoid duplication here and is there some sort of mechanism that you currently have in place to monitor where all these federally funded research initiatives are going and what they are accomplishing?

Mr. STRAWN. Thank you for the question. We do believe, Mr. Quayle, that one of the primary functions of the NITRD program which provides for interaction among the agencies and discussion of what their plans and programs are for the coming years results in cooperative ventures in finding out that other agencies are doing something that they thought they would need to do and now they can rely on the other agencies' results rather than doing so. So filling gaps and avoiding overlaps is something that I think we have always considered to be an important part of our obligations.

Chairman QUAYLE. So you think that you have the ability to make sure that we are not having duplicative research and also within the various agencies? One of the other things within that is that there are some concerns that as various agencies try to fight for turf, especially within the cybersecurity realm, that they are going to less likely to want to work with other agencies because they have that protective turf battle going on.

Mr. STRAWN. Well, I suppose agencies are a little like companies in that there is cooptition going on, cooperating at some places and yet there is a limited amount of federal funds and so forth they are in competition for appropriations. Certainly the NITRD program as a venue for cooperation doesn't enforce or attempt to boss the agencies around in these regards but when they become aware of what each other is doing, we have seen plenty of cases where it has led to cooperation and better extension of federal funds.

Chairman QUAYLE. Thank you.

My next question is for Ms. Furlani. When you have the changing nature of cyber threats, and we are going to be starting to develop some standardization for cybersecurity procedures, and standardization always conjures up a very inflexible model, how do we make sure that we do set up the procedures so that we have the flexibility to address these changing cyber threats because they will continue to change as years go on?

Ms. FURLANI. We frequently change our recommended standards for the Federal Government and we do that because we work so closely with industry, who is aware of what is changing and they give us that feedback and that recognition of how we should be modifying. We put out our drafts for public comment. We get comments internationally as well as locally and we adapt as we go, and we also work to move our standards and other standards along in the international arena because we also have the responsibility to work with industry to develop voluntary consensus standards and

make sure that the Federal Government is using voluntary, consistent standards wherever applicable. And so being aware and connected with industry as closely as we are has been very effective in making sure that we are adapting as we move along because technology moves just too fast for standing in one place.

Chairman QUAYLE. So as different best practices are developed in various industries that you deal with, especially on the cybersecurity front, that you just have an evolving standards practice basically?

Ms. FURLANI. We are flexible enough to adapt to new changes, new needs and we listen and we have our mechanisms that work that through and again try to move them into the international standards so our industries can compete globally.

Chairman QUAYLE. Okay. Thank you very much.

Now, Rear Admiral Brown, the Administration has proposed a cybersecurity legislative package tasking the Secretary of DHS with working with interested parties to propose standardized frameworks to address cybersecurity risks to critical infrastructure. The package also states that the Secretary should work with the Director of NIST to develop alternate standards if the voluntary standards developed by the interested parties do not meet the required criteria. What role, if any, does the Secretary envision for NIST in the initial voluntary standards development process?

Admiral BROWN. Sir, we already have a very close relationship with NIST. We have been working in particular on several parts of the private sector and believe that building upon that information and the relationship that we have, the development of the standards, and from DHS's operational perspective that we will continue to leverage that and apply that in the rule sets that we will be putting forward.

Chairman QUAYLE. Okay. Thank you very much.

The Chair now recognizes Mr. Wu for five minutes.

Mr. WU. Thank you very much, Mr. Chairman.

I would like to use my five minutes to put two questions to whomever on the panel wishes to answer them. The concept of anonymity and privacy are frequently conflated in our discussions, and setting privacy aside for the moment, I would like to focus on anonymity. It is very, very legitimate to very much completely identify someone who is going into look at, say, medical information or banking information whereas if someone is going to read a newspaper or do a posting on a political wall, at least in our society we would view that as something which should be protected by anonymity if the user so chooses. There are increasingly attribution technologies. Also, if you come off your Facebook page, you are locked in by your community pretty much as your identity and there are also proposals for inherently secure Internet backbone, which may also lead to traceability on the Internet. Could you all address how these what we view as advantageous technologies can also be reconciled with a continuing need for freedom of the Internet so that certain societies, certain governments will not be further empowered to crack down on what we view as inherently private and desirable activities.

Mr. STRAWN. Let me take a quick crack at that, Mr. Wu. I think that better identity management may also help assure anonymity

in the right situations. For example, in the academic world, library checkouts are an example of where anonymity has typically been appropriate and probably continues to be, but let us say at a university, only students of that university and perhaps some others are permitted to check books out or do what have you. If we have the ability to do identity management by attribute as opposed to just by name, if a person can log into a trusted identity management and indicate that they are in fact a student because it is trusted who they are, then the attribute of being a student can be used to check out the books and the publications at a library, and so better identity control can enable anonymity in that sense as well as enable full identity when appropriate.

Ms. FURLANI. Yes, I would like to amplify on that because of the National Strategy for Trusted Identities in Cyberspace. This is one of the goals to have an ecosystem where there might be credentials and you could choose, each individual could choose whether they want to be anonymous today or whether they want their bank to know who they are, that they really can move that money around, and so that is one of the goals. We have workshop coming up in June to explore what it means to have such a system, and we will be talking with industry as usual to understand how this could be facilitated.

Mr. JAHANIAN. I would just add that as my colleague highlighted already, identity management is key to this. I would also like to add that at National Science Foundation, we have a number of research activities that look at this issue, particularly at anonymization techniques, identity management, and we all recognize that ultimately we have to reach a balance between protecting public privacy and public safety, national security and economic prosperity. So I do want to add that we have a number of research activities that are ongoing addressing the very issue that you highlighted.

Mr. WU. Thank you very much.

My second question is directly international rather than obliquely international, and that is that just as the proposed legislation preempts a lot of state legislation, so many of the problems really are of a multinational nature. But there has been already a lot of jockeying about international standards, and could you address the issue of how to negotiate truly international standards and the issue of certain countries jockeying for advantage in setting up islands of technology and these islands not only grant commercial advantage but they also potentially decrease Internet freedom in those islands?

Ms. FURLANI. Certainly this is an issue that we work with, and the openness and the way that the international standards are developed and we try to make sure that our experts are participating actively and the value is seen of having standards that everyone can use and setting that baseline has been pretty effective in solving this issue, and we continue to watch out for such opportunities to make sure that the understanding is there because it is really a value proposition that if we can collaborate on these, we all benefit.

Mr. WU. Let me just add that I look forward to NIST continuing to take a lead role in international negotiation. Thank you for your tolerance, Mr. Chairman.

Chairman QUAYLE. Thank you, Mr. Wu.

The Chair now recognizes Mr. Brooks for five minutes.

Mr. BROOKS. Thank you, Mr. Chairman. As much as I am going to be able to be here for the entire hearing, some of the other Members have time constraints, I am going to defer my time to Mr. Smith.

Mr. SMITH. Thank you, Mr. Chairman. Thank you, Mr. Brooks. I appreciate the courtesy there.

I have a couple of questions, and the first question is for all Members, all witnesses here today, and Dr. Furlani, I realize you have touched on this subject in response to the Chairman's question a while ago but I would like to ask all of you this. One of the concerns that is often voiced about the Federal Government's approach to cybersecurity is that it does not take into consideration often enough the expertise that is available in the private sector, and so I would like to ask each of you how your agency intends to collaborate with the private sector, private industry to take advantage of their expertise, and I guess, Dr. Strawn, we will begin with you.

Mr. STRAWN. Thank you, Mr. Smith. I think that a little historical example might help. I mentioned previously that our agencies have been working on a strategic plan for cybersecurity research, and that plan has not only involved agency collaboration but has involved several interactions with the private sector, holding workshops where private sector experts are invited in to comment and assist us in formation of that plan. We have a history of doing that with other activities as well and we continue to see that mechanism both in asking for public feedback from documents that we prepare and prior to that asking input as we prepare documents from experts in the various fields.

Mr. SMITH. Thank you.

Dr. Jahanian?

Mr. JAHANIAN. Yes, I am happy to answer that. Our panel review process actively involves not only scholars from academic institutions but also government folks as well as experts from industry, so that is one aspect of it. We run a number of workshops that involve both academics as well as individuals from the private sector as they advise us about our programs, about the future of research investments and so on, but I also want to highlight a couple of other things. For example, the research contributions that I have listed in my written testimony and other outcomes and innovations that have been developed with National Science Foundation's funding and other federal partners are now being used by the private sector as well as government agencies. In fact, recently I did a quick count of past five years of various technology that has been transferred from the cybersecurity program from National Science Foundation. I was pleasantly surprised to see the number of technologies that have made it into the private sector, commercialized, used by Federal Government agencies and by the private sector. I counted 20 startups that have been launched just over the last 2, three years based on the research that we funded. I also highlight

that some of this of course is leading toward securing our infrastructure, protecting our national security, but also is fueling job growth. Another program that I want to highlight is that the National Science Foundation relies heavily on SBIR and STTR to fuel innovation and foster adoption of that innovation by government as well as the private sector.

Mr. SMITH. Okay. Thank you.

Dr. Furlani?

Ms. FURLANI. Yes. I had mentioned it earlier that we hardly do anything without talking with industry first. If we see a problem that we need to consider and how we might formulate some strategy for protecting cyberspace, we would typically open a workshop and ask anyone of interest to come and discuss it. Then once we collect our thoughts and put something down in writing that people can react to, it is put out for public comment and we take those comments extremely seriously. We work through every one. We put back publicly what we have done with each comment, and if whatever draft we put out changes significantly, then we put it out again so that there is a second round, so we move very carefully.

Mr. SMITH. Thank you.

Admiral Brown, since I am almost out of time, let me ask you to address another question in addition, if you would. In San Antonio, we have an Operations Warfare Center at Lackland Air Force Base that you are probably familiar with, very similar to the National Counterterrorism Center. The Operations Warfare Center helps the Department of Defense in planning to stop or prevent cyberattacks. Do you think there is any possibility of that kind of operations center might be a prototype and useful to the government in other areas?

Admiral BROWN. Yes, sir. Tied to your first question, what we have established inside DHS is the National Cybersecurity and Communications Integration center. It is an operations center to be able to look at and provide situational awareness, and tied to your first question, that is part of our relationship with the private sector. We have representatives there from an operational view and so that has proved to be very effective in our ability to operate in the environment that we see.

Mr. SMITH. Thank you, Admiral Brown.

Thank you, Mr. Chairman.

Mr. MCCAUL. [Presiding] The Chair now recognizes a good friend from Illinois, we co-introduced the Cybersecurity Enhancement Act the last Congress, which passed overwhelmingly, Mr. Lipinski.

Mr. LIPINSKI. Thank you, Mr. McCaul.

I want to start out by asking a question of Dr. Jahanian and Dr. Strawn. In a 2009 hearing before this Committee, one expert described the "never ending tug of war between security and usability," and this is, I think, a very important issue that has at times been overlooked. I think we are now giving a better focus to this. I just wanted to ask if you can describe how research in social, behavioral and economic sciences can improve both usability and security, and also how is social science research incorporated into the soon-to-be-released R&D strategic plan, whoever wants to start?

Mr. STRAWN. Thank you, Mr. Lipinski. I will say a quick word on it and then I will turn to my colleague since much of this work is done in the National Science Foundation. But the NITRD program has had working groups in socioeconomic impacts of information technology for some time. It also has a subgroup of that group specifically in education purposes, which is a social science activity, I would say. The cybersecurity research program, research strategic program that we have has a dimension of seeking economic incentives for better cybersecurity practices. So I think that within the NITRD program, we have a number of cases where socioeconomic research is functioning and is a part of the overall picture.

Mr. JAHANIAN. Congressman Lipinski, you raise a very important point. The issue of cybersecurity goes far beyond technology. It involves human beings. It involves humans in a loop, if you will. Two years ago when we launched the—3 years ago when we launched the trustworthy cross-cutting program at National Science Foundation, we actually acknowledged that there are four components or themes to this program. One is security, how vulnerable is it to attack, the system is vulnerable to attack; reliability, does it work as it is intended, privacy, does it protect a person's information, and finally, usability, can human beings use the system in an efficient way, in a secure way. I do believe that in fact the programs that we have launched in recent years directly address the usability issue. We have a number of research activities that are funded by National Science Foundation that recognize humans in the loop and interaction of humans with computer systems.

As part of our new initiative, we are also looking at cybereconomic incentives, and if you permit me in 30 seconds I will try to explain what that is. Consider the attacks that exploit human behavior, user behavior, weak passwords, for example. We are also seeing increasingly social engineering where you receive an e-mail and you click on a link in your e-mail and inadvertent you download, one downloads a program that infects your computer and can be used for all sorts of malicious activities. So recognizing that, we need to look at human behavior, understanding human behavior and also understanding the motivation of attackers and be able to reconcile that with the technologies that we develop and technologies that we deploy. Also, we need to consider incentives that make cybersecurity ubiquitous. Why is it that not everybody is using good hygiene, if you will, when it comes to cybersecurity? How do you incentivize good behavior and disincentivize bad behavior? Also, understanding the motivation behind bad actors, as I mentioned, and also understanding various kinds of user models. Incentives to facilitate adoption of trustworthy technologies is not just limited to individuals, it also includes government agencies and the private sector. So understanding all of that plays an important and critical role in our solution and our approach to dealing with this important problem.

Mr. LIPINSKI. Thank you. In the very short time I have left, what is being done—because I think cybersecurity education and building our workforce to address cyber challenges is very important. Is there anything that you are doing with K–12 students, any of the agencies, for education? Just quickly.

Admiral BROWN. Yes, sir. From DHS, we have an ongoing relationship with the National Cybersecurity Alliance, a program called C–SAVE, and that is very much focused on K–12 and we are going to continue to build that capability.

Ms. FURLANI. And also with the National Initiative on Cybersecurity Education, we work as the lead but the Department of Education is one of our partners and looking at that very issue.

Mr. JAHANIAN. NSF is also participating in that same activity and looking at the issue.

Mr. LIPINSKI. Thank you very much. I yield back.

Mr. MCCAUL. Thank you.

The Chair now recognizes the gentleman from Maryland, Mr. Bartlett.

Mr. BARTLETT. Thank you very much.

In the Department of Defense, our weapons system developments take a very long time. They can easily take a decade. Obviously in that decade, technologies are changing, some of them dramatically. So when we begin a development, we are interested in the technologies and how fast they can develop and what is the ultimate achievable. For an airplane, for instance, we are interested in stealth and how little can we look to the radar. On the other hand, we are also interested in how fast the capability of radar will grow so that they can see us, although we are really tiny, and then what about the capability of once they have identified our airplane of taking it out with a missile from another airplane or from the ground or by and by maybe something from a satellite.

A bit ago, Gina Dugan, the director of DARPA, was in my office and I asked her if she could help us in that kind of an analysis because we are looking to develop a new deep strike heavy bomber, and I have no idea which of those technologies is growing the faster and I don't want to put billions of dollars in developing a plane that is simply going to be easily spotted and taken out of the sky when it is finally fielded 12, 15 years from now. She said oh, we really can help you with that sort of thing, and what she gave me as an example was something in cybersecurity, and she showed me a graph, and it showed that the codes, the lines of code that the bad guys use in malware is not increasing but the lines of code that we are using to defend ourselves is increasing exponentially. Every month, every year it gets bigger and bigger.

What we are asking of the system is two things which kind of appear to be mutually exclusive. On the one hand, we want it wide open so that it is readily accessible, and on the other hand, we want it really secure. Are we going to be able to bend that curve, that exponentially increasing curve of the lines of code that we use to defend ourselves and will our systems ultimately be consumed with the necessity of protecting themselves so they won't be able to do any useful work for us?

Mr. JAHANIAN. Congressman Bartlett, we should have you write our solicitations for the National Science Foundation. You articulated the problem extremely well. The technology base for our systems is rapidly evolving. Every three to five years, we deploy new computers, new systems because their new functionalities have come out, new performance enhancements. The settings in which our computer systems are being deployed and the functionalities

that they provide also is not static. My belief is that future security challenges will follow adoption of Internet patterns that we see. For example, mobile devices with cloud computing, different settings are going to impose new challenges for us.

So you are absolutely right that the code base is increasing. The complexity of systems that we are trying to secure is definitely getting more challenging. We are also seeing an increasing trends toward cyber-enabled infrastructures and system such as power grids. Information technology has become so pervasive that we are seeing it in power grids, we are seeing it in the financial sector, transportation networks and so on and so on, and it has been identified already our national critical infrastructure has become so dependent on information technology and computer networks that the vulnerability is there and we need to do something about it.

From a research point of view, our thoughts and our thinking, I should say, the thinking of the broader scientific community is that we need to develop a scientific foundation for dealing with this problem. We cannot be just chasing the bad guys, trying to stay slightly ahead of the latest attack and latest trends that we see. The scientific approach must promote discovery of new laws, if you will, meaning scientific laws. We have to be able to do hypothesis testing. We have to be able to demonstrate repeatable experiments. We have to enable data gathering. We need new metrics. We need to have critical analysis to this problem. In doing so, I should just highlight that the National Science Foundation did launch a program in our trustworthy computing program that focuses on the overall trustworthiness of our critical infrastructure and it directly addresses the scientific foundation that is needed to solve this problem.

Mr. BARTLETT. Thank you. Clearly, this affects just about every one of us and every part of our government, and I still am not certain that we can bend that curve. It seems to me that we are going to be using ever-increasing percentages of our capability just to protect ourselves. It is a huge problem. Thank you all for being involved, and thank you, Mr. Chairman, for holding this hearing.

Mr. MCCAUL. And thank you, Mr. Bartlett, for your expertise.

The Chair now recognizes the gentleman from Maryland, Mr. Sarbanes.

Mr. SARBANES. Thank you very much, Mr. Chairman. Thank you all for your testimony today.

Congressman Bartlett and I and other Members of the Maryland delegation are very excited and proud that the new cyber command is going to be stood up at Fort Meade in our state, and we are trying to prepare for that as well as we can, and I wanted to go back and maybe give you all a little bit more time to speak to the question that Congressman Lipinski posed about how you prepare a workforce because that is obviously something we are very interested in seeing happen in Maryland and sort of where do you start, where does that pathway, that career pathway to being ready to take these diverse set of job opportunities that cybersecurity will provide, you know, chief security officers, analysts, forensics experts, etc., where that pipeline starts, what is the kind of coursework you think is important to offer, what is the role of two-year colleges, community colleges as well as the four-year colleges?

And in particular, I would be curious to have you speak to the complications with respect to security clearance. That always seems to be an issue. You can deliver up a cohort of highly qualified people and they still have to jump through the security clearance process. Are there ways to anticipate that and integrate it into the educational process so that when they kind of graduate from the pipeline, they are actually ready to get right into the job? And so I offer that to any of the panel members to respond to. There is three minutes. Thank you.

Mr. STRAWN. I will just say a quick overview about how important the NITRD program agrees or believes that these issues are. We have also recently been working on a strategic plan for the whole NITRD activity in addition to the Strategic Plan for Cybersecurity, and the three pillars of the NITRD strategic plan are technology and its increasing partnership with us and new ways of use. That is pillar one. Pillar two is trust and confidence, which we are here talking about today, and pillar three is a cyber-ready society including pipeline issues of professionals and general knowledge for the public to fully utilize cyber. So we are focusing our efforts to focus on these activities directly.

Admiral BROWN. Sir, I will talk a little bit about what we are doing at DHS, but I also want to right up front talk about what the teamwork is that you see here. We have already mentioned the efforts that NICE has. We have mentioned the fact that I think there are over 106 centers of academic excellence that DOD and DHS have been working on scholarship for service to identify people early on to be able to get them the right skill sets and afford them an opportunity to work for the government. We have also just recently started, again, DOD, DHS, doing the same type of center for academic excellence for the two-year schools that you mentioned.

The clearances are an issue but part of what we have been doing, particular under the NICE initiative, is to identify all the skills that are required, career paths. There are many that don't necessarily require clearances and so we need to take advantage of that opportunity and the skills and the people that come there. And finally from a DHS perspective on that last point that you talked about, trying to bring them in so they are ready, we started an intern program inside DHS as well as a fellowship program, and we look to be able to take that model and expand it and bring it across the rest of the Federal Government. That is just some of the things that we are doing.

Mr. JAHANIAN. May I add a couple of points? As you probably know from my bio, in addition to my academic experience, I have private sector experience, particularly in cybersecurity. I think this problem of education, workforce development, curriculum development is extremely important to the Nation. It is a very, very important problem that is being addressed by multiple agencies. I will highlight a couple of programs. Scholarship for Service, that was mentioned. National Science Foundation has been extremely pleased with our involvement in the Scholarship for Service program. In particular, it is being offered at 34 institutions today and more than 1,000 students who have graduated from this program have returned to government service, so it is a great success story.

Another track related to Scholarship for Service includes capacity building. Again, we offer funds to universities and colleges to develop curriculum, and there are a number of center-scale activities that have been launched related to this which involve multiple institutions collaborating, developing new curriculum specifically in the cybersecurity area.

Another program that I think is extremely important in terms of training technicians and training particularly entry-level positions is the Advanced Technological Education program which addresses directly the two-year colleges. In my testimony, I highlighted three regional centers, and again, it is a terrific success story, allowing individuals to be retrained or go through a two-year program led by our community colleges, be trained and go back into the workforce, particularly the government sector.

Mr. MCCAUL. The Chair now recognizes the gentleman from Alabama, Mr. Brooks.

Mr. BROOKS. Thank you, Mr. Chairman.

Dr. Strawn, in the Administration's proposed legislation released in early May, you mention a few places where research and development is mentioned. For the sections you reference, it is clear that NITRD would lead these efforts—excuse me. Is it clear that NITRD would lead these efforts? Is it necessary for that leadership to be explicitly defined in the statute?

Mr. STRAWN. Mr. Brooks, we are usually careful to use the word "coordinate" as opposed to "lead" in terms of the activities of the NITRD program based on the fact that each agency has their separate mission, has their separate appropriations and appropriations committees, and our goal is to make the whole greater than the sum of the parts by bringing everyone together in terms of the knowledge of what is going on, finding ways to work together and collaborate, but given the way the government is organized, it seems to us that collaboration is the way we can best fulfill our mission.

Mr. BROOKS. Thank you.

Next, Dr. Jahanian, is there a current need for postdoctoral research fellowships in cybersecurity and are cybersecurity postdocs eligible for already established NSF fellowship programs?

Mr. JAHANIAN. At this point in time, we don't believe that we need to have a separate postdoc program for the cybersecurity area in particular. As you probably know, information technology and computer science is a very hot, exciting area. There are jobs available for our Ph.D.s all over the country, in the private sector, in government as well as our academic institutions, and yes, the postdoc funding that is available through the National Science Foundation through my directorate that goes through our research programs is available to support postdocs across the field.

I do want to highlight that during the recent economic crisis 2, three years ago, we recognized that there were a number of bright minds who were getting their Ph.D.s and were potentially leaving the research field, so we came up with a program which lasts only two or three years called computing innovation fellows that allowed us to support postdocs specifically for a short period of time to maintain the pipeline for our research activities, research programs in academic institutions and industry, and it has been a very, very

successful program, supporting more than 100 postdocs. But I don't believe in the long run this is something that we need to invest in. However, it is something that we are looking at and we are going to continue to consider.

Mr. BROOKS. Thank you. Another unrelated question to Dr. Jahanian. The fiscal year 2012 budget request includes $12 million in new spending for cyber activities within the Social, Behavioral and Economic Sciences Directorate. What is the need and purpose for this funding? Does SBE have appropriate expertise in cybersecurity issues to accomplish the goals of this funding or will other directorates be taking the lead?

Mr. JAHANIAN. I briefly alluded to this issue of our need to address the role of humans in dealing with cybersecurity challenges. First, let me state that we expect that there will be a single cybersecurity solicitation from NSF including the science directorate, SBE and Office of Cyber Infrastructure, so these are not independent programs that are all going to be under one umbrella.

The second thing that I want to raise is that we expect fully to have scientists from various disciplines to participate in addressing some of the issues dealing with cybersecurity including computer scientists, mathematicians as well as economists. I responded to an earlier question about our thoughts toward cybereconomic incentives, in particular, dealing with the kind of threats that involve social engineering. By that I mean, when you receive an e-mail and you click on a link and suddenly your machine is infected, your computer is infected. So we need to understand incentives that make cybersecurity ubiquitous, how do we incentivize, as I mentioned, good behavior and disincentivize bad behavior, understand the motivation behind bad actors and understand new user models, and I also mentioned that we need to incentivize facilitation of adoption of trustworthy technologies by various government agencies as well as the private sector. So understanding all of that allows us to develop new technologies and incorporate some of that into the technologies that we expect will come down the road.

Mr. BROOKS. Thank you, Dr. Jahanian.

I yield the remainder of my time.

Mr. MCCAUL. Thank you, Mr. Brooks.

The Chair now recognizes himself for five minutes. As I mentioned, Congressman Lipinski and I introduced a cybersecurity enhancement bill last Congress that passed overwhelmingly. We plan to reintroduce that as early as next week, but we wanted to have the benefit of your testimony on this bill. I know you have had a opportunity to review the legislation, and if I could go over four major points to the legislation that I wanted to cover, and the first deals with, Dr. Strawn and Dr. Furlani, the NIST standards, giving NIST the authority to set security standards for federal networks. Can you give me your comments in terms of whether that is helpful to the Federal Government? Dr. Strawn?

Mr. STRAWN. I think the fact that NIST has been involved with setting standards for us for the last decade in my direct experience as CIO has been very helpful and so any additional responsibilities that NIST might take such as identified in the proposed legislation I think would be helpful.

Mr. MCCAUL. Ms. Furlani?

Ms. FURLANI. We have been working in that space for some time, particularly thinking about the security aspects of domain name security and working to deploy that in the dot-gov and dot-com domains and so I think it is a reasonable fit.

Mr. MCCAUL. The next area establishes a federal university-private sector taskforce to coordinate research and development and also authorizes I think much-needed cybersecurity research and development programs. I think, Dr. Jahanian, you may be best qualified to speak to that provision.

Mr. JAHANIAN. Yes. I think it is very important and it has been already highlighted by others that we need to involve the private sector as we think about addressing the issues that confront the country, cybersecurity challenges that impact our economic security, national security and of course public safety. So as I indicated already in my testimony, the National Science Foundation and other agencies actively involve the private sector in how we approach cybersecurity in our research programs, in our merit review programs, in the workshops we run, SBIR, STTR, So expanding that and bringing the private sector and academics together, I think it serves the country well.

Mr. MCCAUL. Well, thank you for that.

And lastly, there has been a lot of talk about a cybersecurity workforce professionals. The bill creates scholarship programs, both undergraduate and graduate, at the NSF, and that is to be repaid with federal service. So I think that question actually could go to both Dr. Jahanian and to Mr. Brown in terms of DHS having a cyber federal workforce. Dr. Jahanian?

Mr. JAHANIAN. Yes. The question was—as I indicated in answer to a previous question, I believe the issue of workforce development, education and curriculum development and capacity building is extremely important. It has to be at the center of our response to cybersecurity challenges. So this is very much aligned with the needs of the country.

Mr. MCCAUL. Admiral Brown?

Admiral BROWN. Sir, I think Scholarship for Service is extremely important. It has been great for us in the public sector. From DHS perspective, we have teamed extremely well with NSF on that, and we have reaped some of the benefits. Some senior leaders have been graduates of that program as well as some of our phenomenal analysts, so it is a great program.

Mr. MCCAUL. So I take then from the witnesses' testimony that you are all supportive of this legislation? Is that correct? You don't have to all yell at once.

Mr. JAHANIAN. I forgot to push the button.

Mr. MCCAUL. One last question, and this has to do probably more when I was ranking Member on the Cybersecurity Subcommittee on Homeland Security, Admiral Brown. The cyber command is standing up at Fort Meade. In my home state, Lackland Air Force Base which, as you know, conducts cyber operations, and the coordination between DHS and I think the DOD and NSA is very important in terms of the left hand knowing what the right hand is doing. It seems to me, you can't fully protect and defend the Nation as DHS is charged with their mission if you are not coordinating with those who know the offensive capability the best.

Has that enhanced over the years and can you tell me to the extent you can in an open setting what your relationship is now with the Air Force?

Admiral BROWN. Sir, the basic premise of your question, the answer is, you just described my job description. As the cybersecurity coordinator for DHS, my responsibility is to work with both NSA and with U.S. Cyber Command so that we are synchronizing, we are from both the DOD and DHS perspective aware of our operations, that we are capable of working together, and for U.S. Cyber Command, that means working with its components like the 24th Air Force. So that is part of my job is to make sure that I am providing that situation awareness to DHS so that we are prepared when we are looking at protecting the dot-gov and working with the private sector and the dot-com and vice versa to be able to provide that information, to be able to work with NSA and with U.S. Cyber Command as they are executing their missions and responsibilities.

Mr. MCCAUL. That is excellent news, because five years ago when we held hearings on the issue, that was not the case. There wasn't that kind of coordination, so I commend you for taking the lead on that, and I think that is going to make the country a lot safer.

Thanks to the witnesses. We have one last round of questions, as I understand. Mr. Wu is recognized.

Mr. WU. Thank you, Mr. Chairman, and I understand, this may be the last question. I want to do the Congressional hearing question equivalent of a core dump. There has been a lot of discussion about cloud computing. We have also migrated to mobile devices, a lot of computing there, a lot of information sharing. Could whomever wants to address this, address the security implications and challenges of cloud computing and mobile devices and directions to go to try to solve some of those issues?

Mr. STRAWN. Thank you, Mr. Wu. You have nailed some important questions right there, and they are illustrative of the history of IT that every time we think we are on top of things, something new emerges, and therefore we have to sort of think it over again and start up and we are always looking for basic principles like Dr. Jahanian was talking about but many times we are simply reacting to the new technologies. It is certainly true that cloud computing for one is a potentially very important technology. The NIST activities have been taking some lead in that and I am sure that Ms. Furlani will have something to say about that.

I have an opinion that once we are over the transition to cloud computing, we will actually be in a more secure environment rather than a less secure environment because we will have people whose core competencies are to provide secure information and secure access to information. The various organizations that are required to provide that type of security for themselves, it isn't a core competency, so once we are over the transition, I look for actually superior security.

Ms. FURLANI. Yes, we are leading the Federal Government's look at how standards need to be deployed and worrying about the cybersecurity privacy and security issues, and we have recently published a special publication to look at those specific issues. It

is out for public comment right now. We have also established the—proposed a definition for cloud computing which has been taken up by everyone so that we are all at least speaking on the same terms so that we know what we are speaking about, which helps get us over that hump. The second piece I wanted to mention is the mobile devices. That is something we have been looking at and again holding workshops on understanding what we need to be thinking in that aspect from the standards and testing point of view.

Admiral BROWN. Sir, just to build off of what Ms. Furlani had said, we have been active participants in that work, particularly the cloud computing, the definitions and interagency efforts have been going on, but from a mobile-device standard, U.S. Cyber Command on a regular basis is putting out information to the public sector about what the threats are, the best practices that need to be done and making sure that some of that is available as we continue to look at the employment and deployment of those capabilities.

Mr. WU. Thank you very much.

Mr. MCCAUL. Thank you, Mr. Wu.

I want to thank the witnesses for their valuable testimony. The record will remain open for two weeks and so Members may have additional questions for you in writing. I would ask that you respond.

With that, the witnesses are excused and this hearing is adjourned.

[Whereupon, at 11:30 a.m., the Subcommittees were adjourned.]

Appendix

Answers to Post-Hearing Questions

ANSWERS TO POST-HEARING QUESTIONS

Responses by Dr. George O. Strawn, Director, National Coordination Office for Networking and Information Technology Research and Development

Strawn – Response to Congressional queries

Response of Dr. George O. Strawn
Director, National Coordination Office for
Networking and Information Technology Research and Development
to questions posed by the Subcommittee on Technology and Innovation and
Subcommittee on Research and Science Education
of the
Committee on Science, Space, and Technology
U.S. House of Representatives

Chairmen Brooks and Quayle:

Thank you for your invitation to provide additional information regarding cybersecurity research and development and related activities of the Federal Networking and Information Technology Research and Development Program (NITRD).

Question 1 from Chairman Brooks

> In your testimony you state that the "role of the NITRD Program in advancing the Government's cybersecurity efforts is to identify the technologically hard but critical problems and coordinate effective research and development to address them." How is this role carried out? How does NITRD go about identifying these problems? NITRD has a broad mission that includes targeting critical needs, avoiding duplication of effort, maximizing resource sharing, and partnering in investments to pursue higher-level goals. How is NITRD accomplishing and coordinating these efforts?

Making cyberspace more secure is a national goal. The President's Cyberspace Policy Review concluded that piecemeal measures are no longer adequate in responding to the challenges of securing cyberspace and called for coordinated, "game-changing" research and development. The activities in which NITRD agencies are currently engaged to secure our cyber infrastructure provide an excellent example of the role that the NITRD Program plays to coordinate R&D efforts, target critical needs, avoid duplication of effort, and maximize resource sharing and partnerships.

To identify the critical problems in cybersecurity, the NITRD agencies are conducting an ongoing national outreach program. In an extensive series of workshops, meetings, discussions, and calls for ideas, the NITRD agencies are asking security experts, researchers, and stakeholders throughout the public and private sectors to help envision conceptual and technical approaches that could "change the game" in cyberspace. The agencies have applied key ideas emerging from these discussions in developing a new strategy for Federal cybersecurity R&D. Now in final draft form, the forthcoming strategic plan for Federal cybersecurity R&D focuses on a framework of game-changing R&D themes to prioritize Federal cybersecurity research activities. If realized, such game-changing R&D could potentially redress the balance of power in cyberspace. Currently, cyber attackers have the upper hand (anonymity; stealth; rapidly shifting and increasingly damaging methods; asymmetric strength) and defenders are caught up in an endless cycle of patching networks and systems. But this defends only against previously

identified threats, not the constantly emerging new ones. What if the attackers' advantages could be eliminated? What would have to be changed to make it very difficult to do damage in cyberspace and much easier to assure the security of systems, networks, and information? Those are the research challenges of game change.

The draft Federal cybersecurity R&D strategic plan exemplifies how NITRD coordination enables agencies to achieve together results that no single agency could achieve alone. The draft plan incorporates the best thinking of cyber experts from some 20 Federal agencies as well as of experts from academia and industry. Its framework for R&D collaborations focused on fundamental technological change provides the blueprint for a new national agenda in cybersecurity research to guide future investments, both public and private. It proposes close partnerships with the private sector to accelerate R&D results and the transition of new technologies into practice. By targeting critical research needs, such a document enables NITRD agencies and their private-sector partners to discuss directly who will focus on what activities to maximize synergies of effort, assure coverage of high-priority hard problems, and minimize duplicative activities. Agencies with classified research missions in cybersecurity also participate in this coordination and collaboration.

An example of R&D coordination under NITRD is the Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) program, a public-private partnership among four research universities funded by DOE and supported by DHS (initial funding was provided by NSF) with active involvement by industry. TCIPG includes an industry board made up of many of the Nation's largest energy providers, system operators, and equipment vendors, as well as researchers from DOE's national laboratories. Together, the universities, board members, and government agencies rationalized and prioritized the research issues in securing power grid infrastructure and developed an interrelated group of R&D projects that enable each university and national lab to focus on discrete components of the technological challenge while sharing ideas, issues, and advances with all TCIPG participants. (http://tcipg.org)

Coordinated NITRD planning also illuminates certain shared research needs that tend to be overlooked as individual agencies allocate their research dollars on the basis of diverse mission priorities. For example, the draft Federal cybersecurity R&D strategic plan identifies the need for fundamental R&D to develop *a sound scientific basis* for the engineering of cybersecurity technologies. The architecture of today's digital infrastructure originated decades ago when the focus was on reliability and survivability rather than security. We now need to revisit the fundamentals from a 21st century vantage point and make a major effort to reshape cyber technologies – as well as our understanding of how to manage and interact with digital infrastructure – to stay ahead of the curve in a very dangerous world. A new "science of security" research focus has been identified and prioritized through the draft Federal cybersecurity R&D strategic plan to assure that the next generation of security solutions is built on a strong foundation of scientific principles, laws, and testable hypotheses.

Strawn – Response to Congressional queries

Question 2 from Chairman Brooks

You mention the SEW-Education subgroup's work on "raising the national profile of computing-related knowledge through fundamental changes in K-12 computer science education." Exactly what kind of "fundamental changes" are they working on? Are kindergarten and elementary students currently being taught cybersecurity in the classroom, and if so, how?

The fundamental changes that NITRD's SEW-Education group seeks to help promote would integrate instruction about the science of computing throughout the K-12 curriculum. Indeed, the former co-chair of the NITRD Subcommittee – Dr. Jeannette Wing, now back in the computer science department at Carnegie-Mellon University – introduced the concept of "computational thinking for everyone." She spearheaded NSF initiatives to support development of innovative ways to familiarize students at all levels with the fundamental concepts of computation, such as algorithms, and how they can be applied to solve problems in every domain – just as students now learn fundamental concepts in mathematics and other sciences in grade-appropriate curricula starting at the elementary level.

The SEW-Education subgroup's effort is a direct outgrowth of NITRD multi-agency planning activities. In national public forums we held in 2008 and 2009 to inform strategic planning for the NITRD Program as a whole, academic computer scientists and K-12 educators alike told us that a K-12 curriculum in computer science did not exist. Computer science teaching, they said, was limited to an introductory high-school course in programming, offered by only 65 percent of high schools in 2009 and taken by a small percentage of students. In lower grades, they said, teachers informally helped students use computer applications but there was virtually no instruction about the science of computation. In a society increasingly dependent on complex digital systems, the NITRD agencies believe, this gap in K-12 students' knowledge and experience is worrisome and needs to be addressed through rigorously-evaluated and proven grade-appropriate computer science curricula.

The managers of the NSF programs targeting this problem participate in the SEW-Education group and are contributing to development of its action plan. The first NSF effort, Computing Education for the 21st Century (CE21), is focusing special attention on the middle-school through early-college levels, with the goals of: increasing the number and diversity of students and teachers who develop and practice computational competencies in a variety of contexts; and increasing the number and diversity of postsecondary students who are engaged and have the background in computing necessary to successfully pursue degrees in computing-related and computationally intensive fields of study. http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503582

The second NSF activity, CS 10K (which stands for 10,000 Computer Science teachers in 10,000 high schools), aims to increase the effectiveness of computing education in high school through the introduction of an entirely new curriculum (based on a proposed, new

Advanced Placement course) concomitant with the preparation of teachers prepared to teach it by 2015. http://www.computingportal.org/cs10k

The NIST NICE lead is also one of the Co-Chairs of the SEW-Ed sub-group and links the activities of each at every opportunity. As I mentioned in my written testimony, these efforts are complemented by the National Initiative for Cybersecurity Education led by NIST. This comprehensive program, to which many NITRD agencies are contributing, includes activities in four component areas: national cybersecurity awareness; formal cybersecurity education; cybersecurity workforce structure; and cybersecurity workforce training and professional development.

Question from Congressman Wu

In Rear Admiral Brown's testimony, he notes that no single agency controls cyberspace and that the success of our cybersecurity mission relies on effective communication and critical partnerships across the government. However, the Administration's legislative proposal released on May 12th recommends consolidating a significant amount of cybersecurity-related activities at DHS, arguably making DHS the *de facto* lead on cybersecurity activities in the Federal government. If this structure is enacted, how can we ensure that it will not reduce incentives for other agencies to be actively engaged on cybersecurity, believing that DHS has it covered?

The Department of Homeland Security (DHS) is an active participant in the NITRD Program, and its NITRD representatives bring very useful insights from the operational side of the DHS cybersecurity mission. The proposed cybersecurity operational DHS activities would complement and promote the research efforts of the NITRD agencies.

Regarding the concern that Federal agencies would leave cybersecurity research to DHS, I think this will not happen because agencies must be actively engaged every day. For example, Federal IT managers spend a significant amount of time in activities to improve the security of Federal systems, networks, and information. I also wish to note that the NITRD Program will continue to play a central role in maintaining communication, coordination, and partnerships among all Federal research agencies.

Question from Congressman Neugebauer

What aspects of the current federal system of research and development in the United States allow us to stay ahead of the curve in predicting and responding to future cybersecurity threats? What must be improved?

The Federal government's ability to predict and respond to future cybersecurity threats will depend on sustaining the breadth and diversity of what many term this Nation's "innovation ecosystem." Over the decades, we have developed a richly textured IT R&D enterprise that stretches from Federal programs and laboratories, across university

campuses and research centers, to industrial R&D facilities and small business start-ups. As the National Academies and others have noted, there are innumerable feedback loops in this ecosystem through which ideas and concepts travel, get transformed, fuel new directions, turn student experimenters into skilled technologists and keen entrepreneurs, and ultimately produce path-breaking innovations. We need to support the vitality of the innovation ecosystem as a whole and the talent pool it generates.

Security is a system property, not just a property of its components. It poses a research grand challenge: how to build a secure system from potentially insecure components. In this moment of growing cyber threats, Federal leadership is necessary to highlight the grand challenge goal, develop a unified approach for addressing it, and energize the research communities in every sector to collaborate in achieving advances.

In this regard, the forthcoming Federal cybersecurity R&D strategic plan helps illuminate the way forward. It calls on researchers to think radically rather than incrementally and it highlights the fundamental missing underpinning – a scientific basis – for developing effective cybersecurity improvements.

The development of a science of security was also recommended in a 2010 study for the Department of Defense by the JASON group, an independent scientific advisory group that provides consulting services to the U.S. government on matters of defense science and technology.

Thank you again for affording me the opportunity to address the important questions you raise on a topic so vital to the future of our country. On behalf of the NITRD Program, I look forward to working with you to realize a truly trustworthy cyberspace.

ANSWERS TO POST-HEARING QUESTIONS

Responses by Dr. Farnam Jahanian, Assistant Director, Directorate for Computer and Information Science and Engineering, National Science Foundation

Question submitted by the Honorable Mo Brooks

Q1. Your testimony touches on the way investments in cybersecurity research are tied to investments in cybersecurity education and workforce development. Why is this important? Are there real-world implications if federal investments shift from education and workforce development in this field?

A1. If these investments were to shift or stop, the pipeline of cybersecurity scientists, engineers and professionals would be slowed. With insufficient cybersecurity experts, the US would no longer be competitive in the science and engineering of cybersecurity and in the development of new cybersecurity technologies and start-ups.

For example, the Scholarship for Service (SFS) program at NSF provides direct evidence that investments in cybersecurity education can have a profound impact on the Nation and its ability to secure cyberspace. To date, SFS has admitted 1400 students; 1100 of the graduates have been successfully placed in the Federal government, including at the National Security Agency, Department of Homeland Security, Central Intelligence Agency, and the Department of Justice.

The Advanced Technology Education (ATE) program focuses on the education of technicians in high technology fields. The ATE center-scale track is funding three cybersecurity education centers. Each center has myriad partners, including a dozen or more community colleges and universities; each center has enrolled over 1500 students since its inception. Both SFS and ATE reach every region of the country and significantly increase the pool of cybersecurity professionals available for jobs in the U.S.

Our investment in fundamental, unclassified, long-term research in cybersecurity has an educational component as well. NSF-funded research projects are the training grounds for the graduate students who will turn into the next generation of advanced cyber security professionals. NSF principal investigators (who are usually university faculty) recruit graduate students to work with them side by side to make discoveries. This day by day faculty-student research training is the basic way we ensure a continuing supply of innovators. Trustworthy Computing currently has about 500 ongoing projects; most of them have at least one graduate student. These NSF principal investigators also recruit undergraduates to work in their labs through supplements to their grants in the Research Experiences for Undergraduates (REU) program. Finally, NSF's most prestigious program that supports junior faculty—the CAREER program—explicitly addresses the integration of research and education to ensure that young faculty learn early in their careers the critical connection between fundamental research and science and engineeering education.

Question submitted by the Honorable David Wu

Q1. In Rear Admiral Brown's testimony, he notes that no single agency controls cyberspace and the success of our cybersecurity mission relies on effective communication and critical partnerships across the government. However, the Administration's legislative proposal released on May 12th recommends consolidating a significant amount of cybersecurity related activities at DHS, arguably making DHS the de facto lead on cybersecurity activities in the Federal government. If this structure is enacted, how can we ensure that it will not reduce incentives for other agencies to be actively engaged on cybersecurity, believing that DHS has it covered?

A1. The model proposed in the legislation reflects established partnerships with Department of Homeland Security (DHS) on broad cybersecurity operational matters and those involving FISMA legislative and policy requirements. In addition, NSF interacts with DHS and other agencies to share cybersecurity "best practices" and "lessons learned" through the government-wide Chief Information Security Officer forum and routinely leverages DHS expertise to address an increasingly dynamic threat environment. DHS conducts independent benchmarking and qualitative reviews of Federal agency cybersecurity programs as part of the FISMA review process. NSF has participated in these assessments for the last two years, and has used the results to make continued improvements to our cybersecurity program.

Such a framework clearly defines the structure of the authorities and responsibilities of the partners. In this case, subsection 3553 assigns DHS a leadership role in setting overall policy and providing guidance and requirements. Subsection 3554 assigns specific responsibilities to agencies, including: assessing risk; determining appropriate levels of security; implementing policies and procedures; actively monitoring effectiveness; and sharing cybersecurity information. Thus, the proposal envisions DHS and the agencies working together towards better cybersecurity operations across the federal government.

NSF frequently works in partnership with other agencies. Another example—focused on cybersecurity education—is the National Initiative for Cybersecurity Education (NICE), which is led by NIST with the participation of the Departments of Homeland Security, Defense, Labor, and Education, the Office of Personnel Management, the National Science Foundation, the Director of National Intelligence, and other Federal agencies.

NSF remains the lead agency, however, for long-term, foundational research in cybersecurity. In FY 2011, NSF will invest up to $129.4 million in cybersecurity research, including $55 million in the cross-cutting Trustworthy Computing program. Its projects range from security at the microscopic level, detecting whether a silicon chip contains a malicious circuit, to the macroscopic, determining strategies for securing the next generation electrical power grid. These investments are critical to an effective national strategy of achieving a "trustworthy" cyberspace.

Question submitted by the Honorable Randy Neugebauer

Q1. What aspects of the current federal system of research and development in the United States allow us to stay ahead of the curve in predicting and responding to future cybersecurity threats? What must be improved?

A1. A major reason that cybersecurity is such a challenging problem is that attacks and defenses co-evolve. Every day, we learn about more sophisticated and dangerous attacks: systems that were secure yesterday are no longer secure. To respond to this continued escalation, we have created a healthy and vibrant U.S. cybersecurity R&D ecosystem that—with effective nurturing—has kept us at the frontier of innovation and deployment.

This ecosystem is driven by fundamental research. It is important to note that many of our cybersecurity technologies deployed today capitalize on fundamental research and discoveries made years, even decades, ago. Fundamental problems that are being addressed now are often difficult to solve but may bear fruit that will give us dramatic new advantages against cyberthreats. For example, *doubly homomorphic encryption* is a technique that will allow us to secure computers at the same level we can currently secure networks: even physical access to a computer would not allow useful information to be stolen. While this approach was first proposed back in 1978, recent NSF-funded research has led to its implementation, but only in limited ways. With continued work by our brightest researchers, we could soon see a fully practical approach that will be adopted by industry.

NSF's cybersecurity research efforts are focused on building systems whose trustworthiness derives from first principles. To do that, we are formulating and developing a comprehensive research portfolio around a view of systems that are deemed *trustworthy,* i.e., systems that people can depend on day after day and year after year to operate correctly and safely. Such systems include transportation systems (avionics, metro, automobile systems), medical devices (medical implants, robotic surgery operated remotely that can be used to save lives in remote areas and on battlefields), and the rapidly developing smart power grid. Included in this notion of trustworthiness are a number of critical concepts: *reliability* (does it do the right thing?); *security* (how vulnerable is it to attack?); *privacy* (does it protect a person's information?); and *usability* (can a human easily use it?). Such research needs to be game-changing and forward-looking.

Of course, one program in one agency cannot solve the challenges of cybersecurity alone, and so part of the research ecosystem is the rich exchange of ideas, goals, and results. This exchange is across disciplines, across governmental agencies via the NITRD program, between industrial partners and research institutions, and across nations; it has fueled new ideas, approaches, and results.

Exchanges between academia and industry bring fundamental results into practice. NSF-funded principal investigators, working with industry partners and mission agencies, continually seed translation of knowledge into new technologies and more effective practice. NSF-funded research activities have led to the formation of start-up companies in the IT sector that are bringing innovative solutions and technologies to the marketplace, both helping to protect cyberspace and fueling job

growth. Other NSF-funded research activities have led to current industries directly adopting results to harden existing IT infrastructure. By promoting a healthy connection between academia and industry, NSF further enhances its research portfolio in trustworthy computing with foundational concepts and new ideas that are directly relevant to the commercial sector.

For example, the NSF Team for Research in Ubiquitous Security Technology (TRUST) Science and Technology Center combines 6 universities with 16 industrial partners, and has produced new knowledge ranging from how to protect automobile control systems from attack to revealing flaws in methods used by websites to guard against attacks by programs impersonating people. Such partnerships need to be encouraged.

The trend toward increasingly cyber-enabled systems, i.e., the integration of computation, communication, and control into physical systems, offers new challenges. Healthcare, education, and finance are already at risk of attack, and physical infrastructure—manufacturing, energy production, and transportation—will be next. An effective national strategy to secure cyberspace must include investments in these areas of research, which will allow our society to continue to benefit from a robust, secure, dependable cyber infrastructure that supports all application sectors, including those on which our lives depend. NSF will continue to make significant investments in support of a secure cyberinfrastrucrue.

Cybersecurity researchers need access to research infrastructure with operational data in order to develop and validate their new theories, approaches, and technologies. For many reasons, such data has been hard to obtain. One excellent example of a long-term effort to provide such data is the PREDICT archive, developed by the Department of Homeland Security's Science & Technology Directorate. In partnership with industry and other organizations, more data archives like this need to be developed and put into routine use.

More broadly, as we become ever more cross-disciplinary, cross-agency and international, the coordination costs of supporting the R&D enterprise increase. Partnerships are a critical component, but they also require considerable investments of time. We need to develop tools and approaches to become more efficient and effective. For example, new technologies need to be employed that allow for more effective remote collaboration such as virtual presence, as well as for research portfolio and gap analysis.

ANSWERS TO POST-HEARING QUESTIONS

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

Questions submitted by Representative Ben Quayle

Q1. I understand the National Initiative for Cybersecurity Education (NICE) and the expectation of a NICE strategic plan being released in the near future. Can anyone provide further clarity on when that document will be available for our review?

A1. The NICE strategic plan is expected to be released for public review in mid-July.

Q2. You mention NIST's participation in international consensus standards. Could you elaborate on how cybersecurity standards development happens in conjunction with other nations? How are other nations dealing with the protection of their civilian networks?

A2. Cybersecurity standards development occurs in conjunction with other nations in open, consensus based standards organizations. NIST and other U.S. agencies participate in these international bodies and, in particular, NIST and other U.S. agencies work closely with the American National Standards Institute (ANSI), a federation of standards developers, government, industry, consumers, and other stakeholders. ANSI is the U.S. Member Body (i.e., representative) to the International Organization for Standardization (ISO) and serves to promote and facilitate U.S. voluntary standards development activities. ANSI's collaboration with the U.S. government performs a vital coordinating role for the entire standards community, ensuring that U.S. interests are adequately represented in international standards arenas.

Q3. Under the Administration's proposed cybersecurity legislative package, the Secretary of DHS is tasked with working with interested parties to propose standardized frameworks to address cybersecurity risks to critical infrastructure. The package also states that the Secretary should work with the Director of NIST to develop alternate standards if the voluntary standards developed by the interested parties do not meet the required criteria. What role, if any, do you envision for NIST in the initial voluntary standards development process?

A3. NIST has a long history and depth of expertise in voluntary consensus standards development processes. We will continue to work closely with DHS in areas of cybersecurity standards and standardized frameworks. In this case we plan to continue to bring our technical expertise, experience working with industry and extensive cybersecurity body of work to assist with organizations who are working on addressing their cybersecurity risks.

Q4. Some witness testimony touched on cloud computing. Could you provide more detail about how cybersecurity impacts the growing cloud services, and what your agency is doing to secure this region?

A4. Concerns over cybersecurity are having a number of impacts on the growing cloud services. Significant impacts include:

- For some customers, limiting their use of public cloud services primarily to low security impact data and processing. Many customers are reticent to use a cloud solution for moderate or high security impact data and processing.
- Some customers choose the private cloud deployment model for security reasons. In some cases, use of the private deployment model is a temporary phase during which a customer gains familiarity with cloud services before migrating to a public cloud solution. In other cases, customers may retain some portion of their cloud-based work in private deployments.
- Cloud providers often implement vendor-specific security measures (such as monitoring of customer processing) and impose customer agreements (contracts) that specify that a customer's account will be terminated if it uses a cloud service to launch cyber attacks.

NIST is addressing the need for cybersecurity in cloud services through several complementary efforts: NIST has produced three draft special publications (SP800-144, SP800-145, and SP800-146) focusing on cloud computing. Two of these address security. SP800-144 addresses security issues in public cloud computing, and SP800-146 provides general guidance on cloud computing, including security.

- The NIST Cloud Computing program runs a working group dedicated to security issues. The group is generating a document that will list security impediments that could limit the adoption or usefulness of cloud computing and, for each impediment, information on how to mitigate it. The mitigation of a security impediment may be a NIST-led effort or may refer to efforts conducted by other entities. The NIST Cloud Security Working Group's output will be incorporated into the "NIST U.S. Government Cloud Computing Technology Roadmap" document. Release 1.0 of this document, for public comment, is planned for early November 2011.
- NIST is working with various voluntary consensus standards bodies. These include, but are not limited to,
  - European Telecommunications Standards Institute (ETSI),
  - Distributed Management Task Force (DMTF),
  - IEEE,
  - Organization for the Advancement of Structured Information Standards (OASIS),
  - Open Grid Forum (OGF),
  - Object Management Group (OMG), and
  - US National Body contributing to the International Organization for Standardization (ISO).
- The NIST Cloud Computing program also runs several other working groups that relate to security. The Standards Roadmap Working Group includes security in its consideration of the standards needed for cloud computing adoption. The Reference Architecture Working Group includes security as a key element for cloud architectures. The Business Use Cases Working Group identifies security requirements which must be implemented to support an agency's deployment and use of cloud computing to support its mission. The Standards Acceleration to Jumpstart Adoption of Cloud Computing (SAJACC) Working Group considers technical security aspects in low-level technical use case scenarios.
- NIST also serves in a Cloud Computing technical advisory role to the U.S. Chief Information Officer Council. The scope of this effort includes security. An example is the security guidance NIST provides to the Federal Risk and Authorization Management Program (FedRAMP), which specifies requirements to satisfy a number of controls for managing security in cloud services.

Q5. In mid-April, the Obama Administration released the National Strategy for Trusted Identities in Cyberspace (N-STIC). It establishes a framework for the development of securing online transactions, and within the FY12 budget request is the establishment of a National Program Office focused on interagency coordination, headed by NIST. Could you please discuss your agency roles in NSTIC, and why NIST has been selected to lead the implementation of the Strategy?

A5. The National Program Office (NPO) will be responsible for coordinating the processes and activities of organizations that will implement the Strategy. NIST - with its long history of working collaboratively with the private sector to develop standards and best practices for cybersecurity and identity management - is uniquely suited to work with the private sector to bring the collective expertise of the nation to bear in implementing the Strategy.

The NPO will lead the day-to-day coordination of NSTIC activities, working closely with the Cybersecurity Coordinator in the White House. The National Program Office will:

- Promote private-sector involvement and engagement;
- Support interagency collaboration and coordinate interagency efforts associated with achieving programmatic goals;
- Build consensus on policy frameworks necessary to achieve the vision;
- Identify areas for the government to lead by example in developing and supporting the Identity Ecosystem, particularly in the government's role as a provider and validator of key credentials;
- Actively participate within and across relevant public- and private-sector fora; and
- Assess progress against the goals, objectives, and milestones of the Strategy and the associated implementation activities.

A core focus of NSTIC is to help the country address some of the key policy and technology challenges - such as cost, interoperability and privacy - that have prevented Americans from obtaining and regularly using stronger authentication technologies. Passwords today are easily defeated through a variety of attacks from cybercriminals and identity thieves, and do not provide appropriate levels of security for many online transactions. Because of this, many transactions that could be online - in health care, banking, government, and other sectors - still require indi-

viduals to appear in person. NIST will work collaboratively with industry to develop standards and best practices that will address these challenges, enabling American consumers, businesses, governments and other organizations to more easily adopt stronger types of authentication that augment or replace passwords while enhancing individuals' privacy.

Question submitted by Representative David Wu

Q1. In Rear Admiral Brown's testimony, he notes that no single agency controls cyberspace and that the success of our cybersecurity mission relies on effective communication and critical partnerships across the government. However, the Administration's legislative proposal released on May 12th recommends consolidating a significant amount of cybersecurity-related activities at DHS, arguably making DHS the de facto lead on cybersecurity activities in the Federal government. If this structure is enacted, how can we ensure that it will not reduce incentive for other agencies to be actively engaged on cybersecurity, believing that DHS has it covered?

A1. Cybersecurity is a dynamic and complex space that needs to leverage a combined talent of active partnerships with industry and academia. No one organization can have it covered and this very hard problem requires collaboration for us to continue to succeed in cyberspace. Two of the many great attributes of NIST are its close collaboration with other agencies, industry and academia as well as NIST's open processes used to develop, design and deploy its extensive cybersecurity tools, guidelines and reference materials for doing everything from DNSSec for securing the internet to Information Security Best Practices for Small Businesses.

Questions submitted by Representative Randy Neugebauer

Q1. What aspects of the current federal system of research and development in the United States allow us to stay ahead of the curve in predicting and responding to future cybersecurity threats? What must be improved?

A1. One aspect for NIST is our active and collaborative work with other agencies, industry and academia in areas of research and development. This gives NIST access to a large body of experts whose cutting edge work in the IT industry enables us to stay ahead of the curve on the development, design and deployment of new technologies. NIST uses this extensive knowledge base and legacy of connections to continue its internationally recognized cybersecurity research and development efforts. As a result, NIST's cybersecurity-related R&D and associated technology transfer has directly resulted in the adoption by the public and private sectors of many commonly assumed security programs such as USCERT, CERT-CC, Role Based Access Controls, PIV Cards, eCommerce, Security Automation and Digital Signatures. NIST is always looking to improve its methods, techniques and reference materials for conducting accurate and repeatable measurements in all areas of science and technology, including cybersecurity.

Q2. In your testimony, you mention the international voluntary consensus cybersecurity standards. What is the assessment of both the strength of current international standards and their flexibility in responding to unanticipated events in the future? What are key areas in which international consensus standards must be strengthened or improved?

A2. The U.S. Government recognizes the importance of international voluntary cybersecurity standards for both US industry and US citizens. This focus aligns well with NIST's mission. Consistent with that focus and in keeping with our mission, NIST ensures its cybersecurity experts play key and leading roles in international standards bodies whether serving as members, co-chairs or chairs in various cybersecurity workgroups. These standards bodies are comprised not only with experts from government, but mostly from the US private sector, to ensure that they continue to be responsive to the needs of U.S. industry.

National and international cybersecurity standards efforts include, but are not limited to 100's of published standards and current standards projects such as:

- Biometric standards for data interchange formats, common file formats, application program interfaces, profiles, and performance testing and reporting
- Management of information security and systems
- Management of third party information security service providers
- Intrusion detection

- Network security
- Incident handling
- IT Security evaluation and assurance
- Cryptographic and non-cryptographic techniques and mechanisms
- Security of the global supply chain
- Identity management
- Privacy enhancing technologies.

Based on current technology, the relevant cybersecurity standards portfolio is quite strong in most of the areas listed above, while others are still actively being developed. As an example, one new technology for which current cybersecurity standards are being revised or for which new standards are being pursued is cloud computing. NIST is actively engaged to ensure that this standards work comes to fruition as quickly as possible and is focused on standards that will be immediately useful. All stakeholders must be vigilant to ensure that these and other cybersecurity standards are updated to keep pace with technology advances.

ANSWERS TO POST-HEARING QUESTIONS

Responses by Rear Admiral Michael A. Brown, Director, Cybersecurity Coordination, Department of Homeland Security

Questions submitted by Representative Ben Quayle

Q1. What will be the impacts on U.S. industry if other countries do not adopt similar approaches to cybersecurity as proposed in the Administration's legislation? How can we assure that there would be a balance between legitimate risk reduction efforts and the ability of U.S. businesses to compete globally?

A1. The Administration will make every effort to coordinate our domestic efforts to secure critical infrastructure with our international engagement. As President Obama stated in the May 2011 International Strategy for Cyberspace, ″the United States is committed to working with like-minded states to establish an environment of expectations, or norms of behavior, that ground foreign and defense policies and guide international partnerships.″ To that end, as the United States moves forward with efforts to better protect critical infrastructure networks, we will collaborate with our international partners in an effort to harmonize those efforts, where appropriate.

The Administration's cybersecurity proposal would establish a risk mitigation regime, in which industry would develop the solutions to common cyber risks, and other critical infrastructure companies would use those frameworks as a guide to better secure their own networks. Under this proposal, the Administration does not encourage a top-down, government-developed approach, but rather a broader implementation of security practices that are currently working for global companies. The Administration believes that companies that already have robust cybersecurity practices will not be significantly impacted by this proposal, regardless of where they do business. However, to ensure that industry has a strong voice in the process and that U.S. business interests are adequately considered, the proposed risk mitigation regime would be implemented through a public rulemaking process.

Q2. Some witness testimony touched on cloud computing. Could you provide more detail about how cybersecurity impacts the growing cloud services, and what your agency is doing to secure this region?

A2. Cloud computing raises many of the same security issues that emerged when shared computer services were created in the 1960s; however, the cybersecurity mission to protect integrity, availability, and confidentiality remains the same. The inherent advantages of cloud computing create some security challenges, but they also provide a number of security advantages. Although we may never fully eliminate all cloud computing risks, we are able to tolerate the different levels of risk posed to different users, organizations, and missions. Even if private, community, and public cloud computing business models use the same security mitigations and countermeasures, different business models create different security risk environments. The Department of Homeland Security (DHS) encourages cloud computing providers to propose innovative security solutions that effectively protect Federal systems, information, and communications.

DHS does not support requiring providers to follow particular designs or architectures for cloud computing. Such an approach would interfere with the innovative and entrepreneurial forces that created cloud computing. Instead, DHS is collaborating with industry and government partners to establish cloud computing security standards. For example, the Federal Chief Information Officer established the Federal Risk and Authorization Management Program (FedRAMP) to provide a standardized approach to assessing and authorizing cloud computing services and products. The National Protection and Program Directorate's Office of Cybersecurity and Communications is actively participating in FedRAMP development. FedRAMP allows joint authorizations and continuous security monitoring services for government and commercial cloud computing systems intended for multi-agency use.

Q3. In mid-April, the Obama Administration released the National Strategy for Trusted Identities in Cyberspace (N-STIC). It establishes a framework for the development of securing online transactions, and within the FY12 budget request is the establishment of a National Program Office focused on interagency coordination, headed by NIST.

Could you please discuss your agency roles in NSTIC, and why NIST has been selected to lead the implementation of the Strategy?

A3. The Department of Homeland Security (DHS) provided its privacy and cybersecurity subject matter expertise during the development of the National Strategy for Trusted Identities in Cyberspace (NSTIC). This effort enabled the Administration to obtain input from public and private sector critical infrastructure partners through working groups that meet under the Critical Infrastructure Protection Advisory Council and the National Infrastructure Protection Plan partnership frameworks.

The Department uses NSTIC to build a shared foundation for authentication of identity across government, business, and the general public. DHS's cybersecurity mission allows it to work with Federal, state, local, and critical infrastructure partners to encourage and employ improved authentication policies and technologies. A healthy cyber ecosystem, however, is dependent on privacy-enhancing, interoperable, and reliable risk-based authentication capabilities for information and data exchanges that occur within domestic and international commerce. The Department of Commerce is well-positioned to promote this aspect of the cyber ecosystem through the NSTIC. Because users' communication devices need to be interoperable, appropriate underlying standards are necessary. The National Institute of Standards and Technology (NIST), in collaboration with DHS and other Federal, state, local, and private sector partners, can effectively address standards requirements on both the national and international levels. Additionally, DHS has provided a detailee to NIST to support the implementation of the NSTIC and will continue to support the NSTIC through additional subject matter expertise as needed.

Questions submitted by Representative Lamar Smith

Q1. How does the cybersecurity division work of the Science and Technology Directorate's Homeland Security Advanced Research Projects Agency (HSARPA) inform the activities of the National Protection and Programs Directorate (NPPD) and the National Cybersecurity Center (NCSC)? Conversely, how does the NPPD and the NCSC inform the research and development direction of the cybersecurity division? Is there anyone who serves as a formal liaison between these entities within DHS?

A1. The National Protection and Programs Directorate's Office of Cybersecurity and Communications' (CS&C) Research and Standards Integration (RSI) program serves as the formal liaison between the operational needs of CS&C and the Homeland Security Advanced Research Projects Agency's (HSARPA) Cyber Security Division (CSD). RSI's mission is to gather cybersecurity-related research and development (R&D) requirements from all elements within CS&C, including the National Cyber Security Division and the National Cybersecurity and Communications Integration Center (NCCIC), and prioritize and harmonize them. RSI then communicates these requirements to CSD for inclusion in its overall R&D requirements. RSI also participates in the identification and selection of R&D supported by CSD. By participating in principal-investigator meetings, RSI tracks and helps apply CSD's R&D results to enhance operational capability within CS&C through the use of a repeatable technology transition process.

CS&C has detailed a member of the Senior Executive Service to HSARPA/CSD to assist in the establishment of the Transition to Practice program, which is aimed at identifying projects and technologies that can be transitioned and commercialized. This detailee works to identify technologies related to the cybersecurity needs of CS&C.

Q2. Over the past several years, DHS cybersecurity personnel have grown from around 30 to over 400 full time employees. The legislative plan proposed by the Administration codifies and expands many of DHS's current cybersecurity responsibilities. How much additional funding will be needed to carry out these duties and employ the necessary workforce? Recognizing the growth of cyber threats, can we expect the costs of managing these responsibilities to continue to grow in future years? How can we guarantee any sort of cost containment?

A2. Similar to the Department of Homeland Security's (DHS) public and private sector partners, DHS is growing its cybersecurity workforce. The Department estimates that within the National Protection and Programs Directorate, the workforce will continue to steadily increase from current strength during the next several years. However, we do not anticipate the Administration's legislative proposal to increase the Department's resource needs substantially as much of the proposal is codifying ongoing activities. Additionally, the mandatory critical infrastructure risk mitigation regime was purposely crafted to minimize Federal Government growth and utilize existing private sector resources. DHS has requested a modest increase

in cybersecurity funding for FY 2012 and does not intend to alter that request based on the legislative proposal.

Question submitted by Representative David Wu

Q1. In your testimony, you note that DHS's operational missions benefit from, and drive the requirements for, the research and development work of the Science and Technology Directorate. In the fiscal year 2012 homeland security appropriations bill passed by the House on June 1st the budget proposed for the Science and Technology Directorate was $398 million, a 54 percent reduction from fiscal year 2010. How would the proposed budget for the Science and Technology Directorate impact the ability of DHS to meet its operational goals and mission in the area of cybersecurity?

A1. The proposed budget passed by the House allocates $398 million for the Science and Technology Directorate's (S&T) Research, Development, Acquisition, and Operation (RDA&O). At that funding level S&T would have virtually no money for discretionary research and development. S&T would not fund any cybersecurity R&D.

Q2. To what extent was the Science and Technology Directorate involved in the development of the first and second iterations of EINSTEIN? And what involvement does the Science and Technology Directorate currently have with the development of the third phase of the EINSTEIN system?

A2. The Department of Homeland Security's (DHS) Science and Technology Directorate (S&T) served as the testing oversight body for the deployment of EINSTEIN's Security Incident and Event Management analytics capability (referred to as National Cybersecurity Protection System Block 2.1). S&T did not perform any testing activities for the first or second iterations of EINSTEIN. EINSTEIN 1 was not an acquisition program and did not require test and evaluation. The MITRE Corporation performed test and evaluation oversight for EINSTEIN 2.

With respect to EINSTEIN 3, the S&T Test and Evaluation and Standards Office designated a Test Area Manager for Test & Evaluation oversight of the Program. This Manager has been engaged in the EINSTEIN 3 project since October 2010. S&T's focus in this area is on the formal operational test and evaluation of the acquisition. The S&T representative is also a standing member of the DHS Acquisition Review Team, in support of the DHS Acquisition Review Board, and is actively involved in the bi-weekly EINSTEIN 3 integrated product team meetings and the Test and Evaluation working integrated product team meetings. S&T has been actively engaged with the program throughout the development of test related acquisition artifacts and is providing subject matter expertise for the duration of EINSTEIN 3's testing activities.

Question submitted by Representative Randy Neugebauer

Q. What aspects of the current federal system of research and development in the United States allow us to stay ahead of the curve in predicting and responding to future cybersecurity threats? What must be improved?

A. The Department of Homeland Security (DHS) participates in the Networking and Information Technology Research and Development (NITRD) Cyber Security and Information Assurance Interagency Working Group (CSIA IWG) to enhance the flow of rapidly changing information assurance needs and recent research and development (R&D) advancements across the Federal R&D community. The CSIA IWG is co-chaired by DHS's Science and Technology Directorate (S&T) and the National Institute of Standards and Technology's Computer Security Division. Through collaborative execution of the R&D roadmap and national R&D theme areas, DHS works with other stakeholders in the R&D community to ensure that current and future threats are addressed.

DHS S&T has led the development of a Federal R&D Strategic Plan within the CSIA IWG. A primary objective of the Federal cybersecurity R&D strategic plan is to express a vision for the research necessary to develop technologies that can neutralize the attacks on the cyber systems of today and lay the foundation for a scientific approach that better prepares the field to meet the challenges of securing the cyber systems of tomorrow.

Maintaining a long-term focus on the national theme areas and their relationship to the R&D requirements of DHS is essential to providing consistent and continuous

support to the Federal R&D community. While the threats rapidly change, R&D approaches must be maintained to facilitate the fundamental breakthroughs necessary to predict and respond to future cybersecurity threats.

An important area of improvement is reconciling the tension between short-term needs for operational tools and long-term acquisition cycles. We need to develop efficient and effective processes for rapidly transitioning new R&D products into operational use. The Federal R&D Strategic Plan includes the definition of an interagency program for transitioning government-funded R&D into commercial operations.

○