CYBERSECURITY ACTIVITIES AT NIST'S INFORMATION TECHNOLOGY LABORATORY

HEARING

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY AND INNOVATION

COMMITTEE ON SCIENCE AND TECHNOLOGY

HOUSE OF REPRESENTATIVES

ONE HUNDRED ELEVENTH CONGRESS

FIRST SESSION

OCTOBER 22, 2009

Serial No. 111–59

Printed for the use of the Committee on Science and Technology

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

U.S. GOVERNMENT PRINTING OFFICE

52–857PDF WASHINGTON : 2010

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON SCIENCE AND TECHNOLOGY

HON. BART GORDON, Tennessee, *Chair*

JERRY F. COSTELLO, Illinois
EDDIE BERNICE JOHNSON, Texas
LYNN C. WOOLSEY, California
DAVID WU, Oregon
BRIAN BAIRD, Washington
BRAD MILLER, North Carolina
DANIEL LIPINSKI, Illinois
GABRIELLE GIFFORDS, Arizona
DONNA F. EDWARDS, Maryland
MARCIA L. FUDGE, Ohio
BEN R. LUJÁN, New Mexico
PAUL D. TONKO, New York
PARKER GRIFFITH, Alabama
STEVEN R. ROTHMAN, New Jersey
JIM MATHESON, Utah
LINCOLN DAVIS, Tennessee
BEN CHANDLER, Kentucky
RUSS CARNAHAN, Missouri
BARON P. HILL, Indiana
HARRY E. MITCHELL, Arizona
CHARLES A. WILSON, Ohio
KATHLEEN DAHLKEMPER, Pennsylvania
ALAN GRAYSON, Florida
SUZANNE M. KOSMAS, Florida
GARY C. PETERS, Michigan
VACANCY

RALPH M. HALL, Texas
F. JAMES SENSENBRENNER JR., Wisconsin
LAMAR S. SMITH, Texas
DANA ROHRABACHER, California
ROSCOE G. BARTLETT, Maryland
VERNON J. EHLERS, Michigan
FRANK D. LUCAS, Oklahoma
JUDY BIGGERT, Illinois
W. TODD AKIN, Missouri
RANDY NEUGEBAUER, Texas
BOB INGLIS, South Carolina
MICHAEL T. MCCAUL, Texas
MARIO DIAZ-BALART, Florida
BRIAN P. BILBRAY, California
ADRIAN SMITH, Nebraska
PAUL C. BROUN, Georgia
PETE OLSON, Texas

SUBCOMMITTEE ON TECHNOLOGY AND INNOVATION

HON. DAVID WU, Oregon, *Chair*

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

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

RALPH M. HALL, Texas

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

CONTENTS

October 22, 2009

Page

Appendix: Answers to Post-Hearing Questions

CYBERSECURITY ACTIVITIES AT NIST'S INFORMATION TECHNOLOGY LABORATORY

THURSDAY, OCTOBER 22, 2009

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

The Subcommittee met, pursuant to call, at 2:07 p.m., in Room 2318 of the Rayburn House Office Building, Hon. David Wu [Chairman of the Subcommittee] presiding.

Subcommittee on Technology and Innovation's

Hearing on

CYBERSECURITY ACTIVITIES AT NIST'S INFORMATION TECHNOLOGY LABORATORY

Thursday, October 22, 2009
2:00 p.m. – 4:00pm
2318 Rayburn House Office Building

Witness List

Ms. Cita Furlani
Director, Information Technology Lab,
National Institute of Standards and Technology (NIST)

Dr. Susan Landau
Distinguished Engineer, Sun Microsystems, Inc.

Dr. Phyllis Schneck
Vice President of Threat Intelligence, McAfee

Mr. William Wyatt Starnes
Founder and CEO, SignaCert

Dr. Fred Schneider
Samuel B. Eckert Professor of Computer Science, Cornell University

Mr. Mark Bohannon
General Counsel and Senior Vice President, Public Policy, Software & Information Industry Association (SIIA)

HEARING CHARTER

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

Cybersecurity Activities at NIST's Information Technology Laboratory

THURSDAY, OCTOBER 22, 2009
2:00 P.M.–4:00 P.M.
2318 RAYBURN HOUSE OFFICE BUILDING

1. Purpose

On Thursday, October 22, 2009 the Subcommittee on Technology and Innovation of the Committee on Science and Technology will hold a hearing to review the recommendations made in the Cyberspace Policy Review that may be appropriate for the National Institute of Standards and Technology (NIST) and the proposed reorganization of the NIST Information Technology Laboratory.

2. Witnesses

Ms. Cita Furlani is the Director of the Information Technology Laboratory at NIST.

Dr. Susan Landau is a Distinguished Engineer at Sun Microsystems. She is a former member of the Commission on Cyber Security for the 44th Presidency and the NIST Information Security and Privacy Advisory Board.

Dr. Fred Schneider is the Samuel B. Eckert Professor of Computer Science at Cornell University and a current NIST Information Security and Privacy Advisory Board member.

Dr. Phyllis Schneck is the Vice President of Threat Intelligence at McAfee. She served as a commissioner for the Commission on Cyber Security for the 44th Presidency and on the National Board of Directors for the Federal Bureau of Investigation's InfraGuard.

Mr. William Wyatt Starnes is the Founder and CEO of SignaCert, Inc. He is formerly a member of the NIST Visiting Committee on Advanced Technology.

Mr. Mark Bohannon is the General Counsel and Senior Vice President, Public Policy at Software & Information Industry Association (SIIA). Prior to working at SIIA, Mr. Bohannon was the Chief Counsel for Technology at the U.S. Department of Commerce where he helped oversee NIST cybersecurity activities.

3. Brief Overview

On May 29, 2009, the Administration released its 60-day review of federal cybersecurity activities entitled, "Cyberspace Policy Review." The review team acknowledged the difficult task of addressing cybersecurity concerns in a comprehensive fashion due to the large number of federal departments and agencies with cybersecurity responsibilities and overlapping authorities. The document detailed a number of near-term and mid-term action plans and stated that it would not only take increased organization and coordination within the Federal Government, but extensive public-private partnerships and international collaboration to achieve these recommendations.

The witnesses were asked to address any recommendations from the Cyberspace Policy Review, focusing on three specific recommendations: the need for a single locus for Federal Government involvement in international standards, an increased public awareness and education campaign, and a larger focus on identity management.

4. NIST Background

The NIST Information Technology Laboratory (ITL) is currently organized into six divisions that perform research and development in the areas of network technology,

computer security, information access, mathematics, statistics, software and systems. ITL has a budget request of $72 million for FY 2010.

Computer Security Division (CSD)

CSD is tasked with protecting the federal non-classified information technology network by developing and promulgating cyber security standards for federal civilian network systems. CSD developed minimum security requirements for these systems in Federal Information Processing Standard (FIPS) 200. CSD also does work in cryptology, electronic identity management, methodology for assessing effectiveness of security requirements, and developing tests to validate security in information systems. Cybersecurity tasks were appointed to NIST in the *Computer Security Act of 1987* (P.L. 100–235), the *Cyber Security Research and Development Act of 2002* (P.L. 107–305), and the *Federal Information Security Management Act of 2002* (P.L. 107–347).

Advanced Network Technologies Division (ANTD)

ANTD works to improve the quality of networking specifications and is currently focusing on advanced areas of cryptography, domain name system security, and evaluation of wireless networks for first responder communication.

Information Access Division (IAD)

IAD provides measurements and standards in areas such as speech recognition, biometrics, and inter-operability of interactive technologies.

Mathematical and Computational Sciences Division (MCSD)

MCSD performs research and development in areas of mathematical modeling, mathematical software, and their scientific applications.

Software and Systems Division (SSD)

SSD develops software testing tools and methods to improve the quality of software and testing in areas such as health care information technology, computer forensics, and voting systems.

Statistical Engineering Division (SED)

SED provides statistical consulting to the NIST laboratories and performs statistical research to improve statistical modeling and data analysis.

5. Issues and Concerns

Recommendations from the Cyberspace Policy Review

The Technology and Innovation Subcommittee has asked the witnesses to discuss recommendations from the Cyberspace Policy Review that may be appropriate for NIST and to specifically address three of the recommendations:

- *The need for a single locus for Federal Government involvement in international cybersecurity technical standards*—Currently, the United States is represented by an array of standards setting organizations, both federal and private industry. The Cyberspace Policy Review calls for a single entity to coordinate federal representation for cybersecurity technical standards and develop an engagement plan for use with international standards bodies.
- *The need for an increased public awareness and education campaign*—the CSD currently conducts limited cybersecurity outreach and education through its Small Business Corner. Also, NIST has a well-established program called the Manufacturing Extension Partnership (MEP) that provides services and information to businesses from regional MEP Centers. NIST can expand upon these resources to increase cybersecurity education and public awareness amongst private citizens and small business, as well State, local, and Federal governments.
- *The need for a larger focus on identity management*—The Cyberspace Policy Review states that cybersecurity cannot be improved without improving identity management. It goes on to say that identity management is not only about authenticating people, but that online transactions involve trustworthy data, hardware, and software for networks and devices. As noted above, NIST has extensive expertise in identity management areas throughout its six divisions.

The report states that future cybersecurity technical standards plans must address the convergence of information technologies and infrastructures. NIST represents an opportunity to address these recommendations because of its broad array of expertise in cybersecurity technology standards and established relationships with private industry and international standards organizations.

Reorganization of ITL

The ITL Director, Ms. Furlani, has proposed a reorganization that would, as part of its actions, split the CSD and combine its programs with others to form two new divisions. Cybersecurity experts are concerned that the split of CSD will take focus away from cybersecurity and are not clear on how the reorganization will improve the function and future capabilities of ITL. Witnesses were asked to assess the reorganization and discuss how it may improve the outcomes of ITL activities.

Chairman WU. This hearing will now come to order. I would like to welcome everybody this afternoon to this hearing on cybersecurity, and we increasingly put all sorts of information, including personal information, online. Our nation's entire infrastructure, from traffic systems and air traffic control to manufacturing to power distribution, depends on internet networked systems. I can think of few topics as important for this subcommittee to address than cybersecurity. And I want to welcome all witnesses here this afternoon for this very, very important hearing.

As anyone who has seen movies recently, including movies like *Ocean's Eleven,* thieves have become increasingly sophisticated in their method of heists, and it should be no surprise that cybercriminals in real life are becoming also more sophisticated in their crimes.

Congress realized the dangers of networked systems as far back as the 1980s, and in 1987, this committee wrote the *Computer Security Act,* which charged NIST (National Institute of Standards and Technology) with developing the technical standards to protect non-classified information on federal computer systems. Congress has remained concerned about cyber-threats, and since 1987, Congress has passed 13 laws related to cybersecurity.

Today OMB (Office of Management and Budget) reports that federal agencies spend approximately $6 billion per year on cybersecurity to protect a $72 billion IT (Information Technology) infrastructure. In addition, the Federal Government funds $356 million in cybersecurity research each year. I don't believe that simply spending more money or creating more programs is the means to improve cybersecurity. We also need to use our existing resources more efficiently and with specific achievable goals in mind. This is also the main conclusion of the Administration's recent cybersecurity review.

The focus of today's hearing is not to review what NIST has done but to address what should be its focus going forward. Since NIST is the only federal agency tasked with protecting non-classified federal computer systems, the testimony we hear today will have a vital and long-lasting affect on our nation's economic and national security.

We have a distinguished panel of witnesses who have a long history of working with NIST and detailed knowledge of NIST's IT activities. I want to assure them that this subcommittee is prepared to act on their recommendations.

And now I would like to recognize Ranking Member Representative Smith for his opening statement.

[The prepared statement of Chairman Wu follows:]

PREPARED STATEMENT OF CHAIRMAN DAVID WU

I want to welcome everyone to this hearing on cybersecurity. More and more of our personal information is making its way online, and our nation's entire infrastructure—from traffic systems and air traffic control to manufacturing—depends on Internet networked systems. I can think of no topic more important for this subcommittee to address than cybersecurity.

As anyone who has seen *Ocean's Eleven* can tell you, thieves have become increasingly sophisticated in their heists. It should be no surprise that cybercriminals are also becoming progressively sophisticated in their crimes.

Congress realized the inherent dangers in networked systems as far back as 1987, when this committee wrote the *Computer Security Act,* which charged NIST with

developing the technical standards to protect non-classified information on federal computer systems. Congress has remained alert to cyber-threats. Since 1987, Congress has passed 13 major laws related to cybersecurity.

Today OMB reports that Federal agencies spend $6 billion on cybersecurity to protect a $72 billion IT infrastructure. In addition, the Federal Government funds $356 million in cybersecurity research each year. I don't believe simply spending more money or creating more programs is the means to improve cybersecurity. We need to use our existing resources more efficiently and with specific achievable goals in mind. This is also the main conclusion of the Administration's recent cybersecurity review.

The focus of today's hearing is not to review what NIST has done, but to address what should be their focus going forward. Since NIST is still the only federal agency tasked with protecting non-classified federal computer systems, the testimony we hear today will have a vital, long-lasting effect on our country's security.

We have a distinguished panel of witnesses who have a long history working with NIST and detailed knowledge of NIST's IT activities. I want to assure them that this subcommittee is prepared to act on their recommendations.

Mr. SMITH. Mr. Chairman, thank you for calling this hearing today on cybersecurity, the fourth in a series of hearings held by the Committee this year. Thank you to the witnesses as well. While our earlier hearings reviewed cybersecurity through a relatively broad lens, today we are here to examine the specific role NIST plays or should play in supporting computer and network security.

Our starting point for this review is the White House's 60-Day Cyberspace Policy Review which was released in May and which provided a broad outline of the actions the Administration intends to emphasize moving forward. A number of these actionaries appear well-suited to NIST's capabilities and expertise. With respect to security practices and standards, NIST is a proven and trusted entity within the Federal Government, the private sector, and even around the world.

It is also well-known for its excellence in advancing research and the fundamental science of computer security. For these reasons, it is important for the Committee to consider more closely the specific additional or expanded activities which makes sense for NIST to undertake and what, if any, associated legislative authority or direction is necessary to enable this.

In doing so, I think it is also important that we work to prioritize these activities and identify those which provide the greatest security returns, recognizing the universe of computer security activities we would like NIST to do is significantly larger than any realistic budget expectations. Additionally, and as I emphasized in our prior hearings, I think we should also be careful to delineate which activities NIST shouldn't undertake, particularly with respect to anything which could take on a regulatory nature, either directly or indirectly.

I thank the Chairman and the panel today. Thank you for dedicating your time and donating your time to this productive discussion. Thank you, Mr. Chairman.

[The prepared statement of Mr. Smith follows:]

PREPARED STATEMENT OF REPRESENTATIVE ADRIAN SMITH

Mr. Chairman, thank you for calling this hearing today on cybersecurity—the fourth in a series of hearings held by the Committee this year.

While our earlier hearings reviewed cybersecurity through a relatively broad lens, today we are here to examine the specific role NIST plays—or should play—in supporting computer and network security.

Our starting point for this review is the White House's 60-day Cyberspace Policy Review which was released in May and which provided a broad outline of the actions the Administration intends to emphasize going forward.

A number of these action areas appear well-suited to NIST's capabilities and expertise. With respect to security practices and standards, NIST is a proven and trusted entity within the Federal Government, the private sector, and around the world. It is also well-known for its excellence in advancing research and the fundamental science of computer security.

For these reasons, it is appropriate for the Committee to consider more closely the specific additional or expanded activities which make sense for NIST to undertake, and what if any associated legislative authority or direction is necessary to enable this. In doing so, I think it is also important we work to prioritize these activities and identify those which provide the greatest security returns, recognizing the universe of computer security activities we would like NIST to do is significantly larger than any realistic budget expectations. Additionally, and as I emphasized in our prior hearings, I think we should also be careful to delineate what activities NIST shouldn't undertake—particularly with respect to anything which could take on a regulatory nature, either directly or indirectly.

I thank the Chairman for assembling an excellent panel today, and I look forward to a productive discussion.

Chairman WU. Thank you very much, Mr. Smith, and if there are any Members who wish to submit their opening statements, the statements will be added to the record at this point.

[The prepared statement of Mr. Mitchell follows:]

PREPARED STATEMENT OF REPRESENTATIVE HARRY E. MITCHELL

Thank you, Mr. Chairman.

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

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

Specifically, we will review that recommendations made in the Cyperspace Policy Review that may be appropriate for the National Institute of Standards and Technology (NIST) and the proposed reorganization of the NIST Information Technology Laboratory.

I look forward to hearing more from our witnesses.

I yield back.

Chairman WU. And now it is my pleasure to welcome our witnesses. Ms. Cita Furlani is the Director of the Information Technology Laboratory (ITL) at the National Institute of Standards and Technology. Dr. Susan Landau is a Distinguished Engineer at Sun Microsystems, and a former member of the Commission on Cybersecurity for the 44th Presidency. I thought that was a mistake at first, but that is the title of the group, and the NIST Information, Security and Privacy Advisory Board. Let us see, we have a different order here. Dr. Phyllis Schneck is the Vice President of Threat Intelligence at McAfee. She serves as a commissioner also on the Commission on Cybersecurity for the 44th Presidency and is on the National Board of Directors for the FBI's InfraGard. Mr. William Wyatt Starnes is the Founder and CEO and a great Oregonian, I might add, of SignaCert. He is formerly a member of the NIST Visiting Committee on Advanced Technology. Professor Fred Schneider is the Samuel B. Eckert Professor of Computer Science at Cornell University and is a current NIST Information Security and Privacy and Advisory Board Member. And finally, our last witness is Mark Bohannon who is the General Counsel and Senior Vice President, Public Policy at Software & Information Industry Association. Prior to working at SIIA, Mr. Bohannon was the Chief

Counsel of Technology at the U.S. Department of Commerce where he helped oversee NIST cybersecurity activities.

The witnesses will each have five minutes for your spoken testimony, and your written testimony will be included in its entirety in the record for the hearing. When you complete your testimony, we will begin with questions, and each Member will have five minutes to ask questions of the panel.

Ms. Furlani, please proceed.

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

Ms. FURLANI. Chairman Wu, Ranking Member Smith, and any other 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.

Cybersecurity is a vital, central mission of our laboratory. The impacts of NIST's cybersecurity activities extend beyond providing the means to protect federal IT systems. They provide the cybersecurity foundations for the public trust that is essential to our realizing the national and global productivity and innovation potential of electronic business and its attendant economic benefits.

Consistent with our mission and the recommendations of the Administration's Cyberspace Policy Review, NIST is actively engaged with many others in coordination and prioritization of cybersecurity research, standards development, standards conformance demonstration, and cybersecurity education and outreach activities.

The Review observed that it is our total national information infrastructure which is under attack. The President has developed a coordinated national response approach that places leadership for cybersecurity-related policies amongst the team within the White House. This team provides an effective means for coordination and collaboration across the Federal Government and with the private sector.

The intelligence community, the other elements of the national security community, and NIST are actively coordinating their standards and processes for cybersecurity. This effort is producing a single set of requirements. For the first time, NIST has included security controls in its catalog for both national security and non-national security systems. The updated security control catalog incorporates best practices and information security from the defense, intelligence and civil agencies, an historic achievement.

The Review recommended building a cybersecurity-based identity management, vision and strategy. In response, NIST is working with OSTP (Office of Science and Technology Policy), OMB and the NSC (National Security Council) through a new sub-interagency policy committee focusing on on-line identity management. Working with OMB and other agencies, NIST is helping to develop a security and privacy profile that will provide guidance to enterprise architects on integrating information security and privacy requirements into the Federal Enterprise Architecture.

NIST hosts the Information Security Automation Program which is an effort to enable the automation and standardization of technical security operations including automated vulnerability management and policy compliance evaluations. The NIST National Vulnerability Database is one such tool. It makes available information on vulnerabilities, impact measurements, detection techniques and remediation assistance. It provides reference data that enable the information security automation program's security automation capabilities. This database also is key to the payment card industry in their efforts to mitigate vulnerabilities in credit card systems. The Review recommended a national public awareness and education campaign to promote cybersecurity. NIST, working with the SBA (Small Business Administration) and the FBI, has put an instructional video on YouTube and published a guide to help small businesses and organizations. In addition, the Review recommended strengthening federal leadership and accountability for cybersecurity. In response, NIST was asked by OMB to contribute to the Security Metrics Task Force to develop new metrics for information security performance for federal agencies.

The Review recognizes the role of international standards in protecting our information infrastructure. We are actively working with others in fostering international standards and protocols that are conducive to a free and safe information processing and interchange environment. NIST also actively contributes to the NITRD (Networking and Information Technology Research and Development) program and its five-year strategic plan.

Consistent with the Review's recommendation, NIST works with other members of the Cybersecurity and Information Assurance Interagency Working Group in establishing research and development priorities to address actions that compromise or threaten to compromise computer and network-based systems.

NIST has undertaken an internal assessment of its operational structure and allocation of resources to ensure that our programs fully reflect the complex interdisciplinary nature of today's threats. Based on the feedback we continue to receive, I have decided to put the proposed reorganization of ITL on hold. We have received expressions of both support and concern from various stakeholders. We are seriously considering this input and plan to reevaluate how to ensure that our structure is as flexible and efficient as possible in meeting the many challenges and opportunities ahead. Regardless of whatever recommendations emerge from this internal assessment, the technical program of work currently performed by the Computer Security Division (CSD) would not change. ITL welcomes and appreciates all input and looks forward to continued conversations on this matter.

Thank you for the opportunity to testify. I would be happy to answer any questions you may have.

[The prepared statement of Ms. Furlani follows:]

PREPARED STATEMENT OF CITA M. FURLANI

Chairman Wu, Ranking Member Smith, and Members of the Subcommittee, I am Cita Furlani, the Director of the Information Technology Laboratory (ITL) at the Department of Commerce's National Institute of Standards and Technology (NIST). Thank you for the opportunity to appear before you today to discuss our role in

cybersecurity and our perspective on the Administration's Cyberspace Policy Review Recommendations.

As one of the major research components within NIST, the Information Technology Laboratory accelerates the development and deployment of information and communication systems that are reliable, usable, inter-operable, and secure; advance measurement science through innovations in mathematics, statistics, and computer science; and develop the measurements and standards infrastructure for emerging information technologies and applications. In addition to research into cybersecurity technologies, NIST is responsible for development of, publishing, and providing explanatory support for federal cybersecurity standards, guidelines, and best practices. Just as the standards function extends beyond writing federal standards to playing an active role in the development of national and international consensus standards, the support function is extended to State and local governments and private sector elements that voluntarily adopt NIST-developed cybersecurity standards.

NIST doesn't rely solely on Federal resources and insights. We employ collaborative partnerships with our customers and stakeholders in industry, government, academia, and consortia to take advantages of their technical and operational insights and to leverage the resources of a global community. We are actively seeking to expand the scope of these collaborative efforts in general, and of our private sector collaborations in particular.

The impacts of NIST's cybersecurity activities extend beyond providing the means to protect federal IT systems. They provide the cybersecurity foundations for the public trust that is essential to our realizing the national and global productivity and innovation potential of electronic business and its attendant economic benefits.

The cybersecurity standards and support capabilities of NIST's Information Technology Laboratory rest on the foundation of the laboratory's cybersecurity research and development activities. Based on input from our customers and stakeholders, we have focused our R&D agenda on eight broad program areas: complex systems; cyber and network security; enabling scientific discovery; identity management systems; information discovery, use and sharing; pervasive information technologies; trustworthy information systems; and virtual measurement systems.

Many of our vital programs impact national security in ways that extend beyond what are generally recognized as the boundaries of cybersecurity. Examples of these impacts include improving the accuracy and inter-operability of biometrics recognition systems and facilitating communications among first responders. The combination of our mission and legislative mandates such as the *Federal Information Security Management Act* (FISMA), the *Cyber Security Research and Development Act,* the *USA PATRIOT Act,* the *Enhanced Border Security Act,* and the *Help America Vote Act* lead to rich programmatic diversity.

Cybersecurity is a vital, central mission of our laboratory. 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 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.

The Cyberspace Policy Review observes that it is our total national information infrastructure, not just the federal information infrastructure, which is under attack, recognizing a national response is necessary to prevent catastrophic consequences for society, including those critical infrastructures which integrate information systems into their operations. To provide for such a national response, the President has developed a coordinated approach that places leadership for cybersecurity-related policies within the White House. This includes the appointment of a Chief Technology Officer, located in the Office of Science and Technology Policy, a Chief Information Officer in the Office of Management and Budget, and the pending appointment of a Cyber Advisor in the White House. This team provides an effective means for coordination and collaboration across the Federal Government and with the private sector. This includes integrating the responses of national security organizations and those of federal organizations that do not have a primarily national security mission. In fact, we observe that the intelligence community, the other elements of the national security community, and NIST are, in response to the *Federal Information Security Management Act of 2002,* actively coordinating their standards and processes for cybersecurity. This effort is producing a

single set of requirements, rather than the past's three independent sets of requirements for consumers and providers of information processing and interchanges resources.

A key output of this initiative to develop a unified information security framework for the Federal Government and its contractors occurred on August 1, 2009, when NIST announced the release of Special Publication 800–53, Revision 3, Recommended Security Controls for Federal Information Systems and Organizations. NIST Special Publication 800–53, Revision 3, is historic in nature. For the first time, NIST has included security controls in its catalog for both national security and nonnational security systems. The updated security control catalog incorporates best practices in information security from the United States Department of Defense, Intelligence Community, and civil agencies, to produce the most broad-based and comprehensive set of safeguards and countermeasures ever developed for information systems. This unified framework provides a standardized method for expressing security at all levels, from operational implementation to compliance reporting. This allows for an environment of information sharing and interconnections among these communities and significantly reduces costs, time, and resources needed for finite sets of systems and administrators to report on cybersecurity to multiple authorities.

The NIST Identity Management Systems Program is pursuing the development of critical standards and metrics to support the effective management of digital identities for large-scale enterprises throughout their life cycle. These efforts will improve the strength, usability, and inter-operability of identity management systems; protect users' personal data; and assure that U.S. interests on this issue are represented in the international arena. We have been heavily involved in Federal Government identity management efforts, including developing the standard for the personal identity verification (PIV) card in response to HSPD–12 and co-chairing the National Science and Technology Council (NSTC) Identity Management Task Force.

The Cyberspace Policy Review included in its top ten action items, "Build a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties interests, leveraging privacy-enhancing technologies for the Nation." To this end, NIST is working with the Office of Science and Technology Policy, the Office of Management and Budget (OMB), and the National Security Council staff to determine how to address this action item, through a new Sub-Interagency Policy Committee which will focus on online identity management.

NIST is taking other proactive steps to increase the long-term security of federal information systems. Working with the Office of Management and Budget and several federal agencies, NIST is helping to develop a Security and Privacy Profile that will provide guidance to enterprise architects on integrating information security and privacy requirements into the Federal Enterprise Architecture. This initiative will ensure that information security and privacy requirements are built into federal information systems early in the system development life cycle rather than attempting to add these requirements after systems are deployed into operational environments. NIST will also be working with its partners within the Federal Government to publish guidance on best practices in systems and security engineering to address the effective integration of commercial information technology products into federal information systems. This guidance will build on the excellent work published by the National Security Agency as part of the Information Assurance Technical Framework over a decade ago and make the information widely available to both public and private sector entities.

NIST hosts the Information Security Automation Program (ISAP), which formalizes and advances efforts to enable the automation and standardization of technical security operations, including automated vulnerability management and policy compliance evaluations.

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

In addition to the initiatives described above, NIST has implemented an aggressive outreach program to work with State, local, and tribal governments as well as private sector entities to raise the awareness of government officials and corporate executives with regard to the ongoing and increasingly sophisticated nature of cyber threats. The outreach program will help organizations external to the Federal Government have a better understanding of NIST's suite of security standards and guidelines and provide an opportunity for voluntary adoption of the standards and guidelines by those organizations to facilitate an increased level of information security for the Nation's critical information infrastructure.

On a broader scale, in response to the Cyberspace Policy Review's recommendation to initiate a national public awareness and education campaign to promote cybersecurity and as a contribution to October's Cyber Security Awareness Month, NIST, working with the Small Business Administration and the Federal Bureau of Investigation, has published a guide to help small businesses and organizations understand how to provide basic security for their information, systems, and networks. The 20-page guide, *Small Business Information Security: The Fundamentals,* uses simple and clear language to walk small business owners through the important steps necessary to secure their computer systems and data. The guide provides ten "absolutely necessary steps" to secure information, which includes such basics as installing firewalls, patching operating systems and applications, and backing up business data, as well as controlling physical access to network components and training employees in basic security principles. NIST also created a video that explores the reasons small businesses need to secure their data.

We are encouraged to observe that the Cyberspace Policy Review recognizes that cybersecurity strategies and solutions must be structured in a manner that accommodates commerce, economic growth, scientific collaboration, and individual liberties. The report reflects the notion that we are not looking for "lockdown solutions" that achieve security at the expense of essential services or civil liberties. Recognizing the economic impact of cyberspace, NIST is working to provide measurement techniques to facilitate offsetting the cost of both public sector and private sector security solutions by decreases in losses or cost of insurance or increases in business due to increases in trust. In order to meet the cyber threat to our total national infrastructure, we must demonstrate that implementing measures that increase security is good business sense. We'd note that not all of these measures need to be technical or regulatory in nature. Some simple procedural steps can have a materially positive effect on security. One example is the financial sector's having introduced a delay into the conversion of electronically transferred funds into tangible assets, a delay sufficient to permit invocation of fraud detection processes.

As acknowledged in the Cyberspace Policy Review, measurement of information security performance can benefit organizations in many ways, by increasing accountability, improving the effectiveness of safeguards, demonstrating legislative and policy compliance, and providing quantifiable inputs for risk-based resource allocation decisions. The Cyberspace Policy Review recommended strengthening federal leadership and accountability for cybersecurity, including identifying cybersecurity as a management priority and assessing the progress of federal agencies against cybersecurity goals, ultimately leading to increased accountability, compliance with cybersecurity policies, and effective implementation of cybersecurity safeguards. Because of its strengths in measurement science and cybersecurity, NIST was asked by OMB to contribute to the Security Metrics Taskforce. This taskforce was established to develop new outcome-focused, rather than compliance-focused, metrics for information security performance for federal agencies, resulting in more effective provisioning of security controls and resources, and improved protection in support of critical mission and business processes.

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

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

Under the provisions of the *National Technology Transfer and Advancement Act* (P.L. 104–113) and OMB Circular A–119, NIST is tasked with the key role of en-

couraging 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 such as the State Department to coordinate standards issues and priorities with the private sector through consensus standards organizations such as the American National Standards Institute (ANSI), the International Organization for Standardization (ISO), the Institute of Electrical and Electronic Engineers (IEEE), the Internet Engineering Task Force (IETF), and the International Telecommunication Union (ITU).

Key contributions NIST has made include:

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

Understanding the value of interagency coordination of research as well as of standards development, NIST actively contributes to the Networking and Information Technology Research and Development (NITRD) program and the development of the NITRD five-year strategic plan. Within the past year, the NITRD Program has assumed expanded responsibilities for coordination of federal cyber research and development, and NIST is well represented in, and leverages, these activities.

The Cyberspace Policy Review challenged the federal networks and Information Technology (IT) research community to develop a framework for research and development strategies that focus on game-changing technologies. Over the past year, through the National Cyber Leap Year and a wide range of other activities, the government research community, including NIST, sought to elicit the best game-changing ideas from the broader research and technology community.

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

There are others ways in which NIST's expertise can help to drive improvements in the cybersecurity arena. NIST has integral roles in a number of Administration initiatives, including Health Information Technology, Smart Grid, Broadband, and Web 2.0. NIST can continue to work on more effective metrics (security controls effectiveness determination), expand education and other outreach, improve product assurance processes, expand national and international cybersecurity standards participation, and automate security controls. This is in addition to our cryptography, technical guidelines, and best practices work.

To address the interdisciplinary nature of security in cyberspace, ITL also has programs in the usability of systems such as voting machines, health information technology and software interfaces; research in mathematical foundations to determine the security of information systems; the National Software Reference Library, computer forensics tool testing, software assurance metrics, tools, and evaluation; approaches to balancing safety, security, reliability, and performance in supervisory control and data acquisition and other industrial control systems used in manufac-

turing and other critical infrastructure industries; technologies for detection of anomalous behavior, quarantines; standards, modeling, and measurement to achieve end-to-end security over heterogeneous, multi-domain networks; and biometrics evaluation, usability, and standards (fingerprint, face, iris, voice/speaker, multimodal biometrics.) Research activities in ITL 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.

We, at NIST and the Department of Commerce, recognize that we have an essential role to play in realizing the vision set forth in the Cyberspace Policy Review. NIST will continue to conduct the research necessary to enable and to provide cybersecurity specifications, standards, assurance processes, training, and technical expertise needed for securing the U.S. Government and critical infrastructure information systems to mitigate the growing threat. NIST will continue to closely coordinate with domestic and international private sector cybersecurity programs and national security organizations. Finally, consistent with the NIST Three-Year Planning Report, NIST plans to broaden its focus on cybersecurity challenges associated with health IT, the Smart Grid, automation of federal systems security conformance and status determination, and cybersecurity leap-ahead research.

Cybersecurity is a vital, central mission of our laboratory. Given the increasing importance and complexity of cybersecurity, NIST has undertaken an internal assessment of its operational structure and allocation of resources to ensure that ITL programs fully reflect the complex interdisciplinary nature of today's threats. For example, NIST is considering whether it needs to strengthen the authority and purview of the NIST Chief Cybersecurity Advisor. Regardless of whatever recommendations emerge from this internal assessment, the technical program of work currently performed by the Computer Security Division would not change. NIST welcomes, through our Advisory Committee, key external stakeholders, and this subcommittee, input on NIST operations and structure and looks forward to continued conversations on this matter.

Thank you for the opportunity to testify today on NIST's work in the cybersecurity arena. I would be happy to answer any questions you may have.

BIOGRAPHY FOR CITA M. FURLANI

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

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

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

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

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

Previously, Furlani was Director of the Information Technology and Electronics Office within the Advanced Technology Program (ATP) at NIST. Before joining ATP, Furlani served as Chief of the Office of Enterprise Integration, ITL, NIST, coordinating Department of Commerce activities in the area of enterprise integration. Furlani also served as special assistant to the NIST Director in the Director's role as Chair of the Committee on Applications and Technology of the Administration's Information Infrastructure Task Force. Previously, Furlani was on detail as tech-

nical staff to the Director of NIST in the position of Senior Program Analyst. Prior to August 1992, she managed research and development programs within the NIST Manufacturing Engineering Laboratory, applying information technology to manufacturing since 1981.

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

Chairman WU. Thank you very much, Ms. Furlani. Dr. Landau, please proceed.

STATEMENT OF DR. SUSAN LANDAU, DISTINGUISHED ENGINEER, SUN MICROSYSTEMS, BURLINGTON, MA

Dr. LANDAU. Thank you very much, Mr. Chairman, and Members of the Committee. I am a distinguished engineer at Sun where I concentrate on security and public policy issues. I have done this for ten and a half years. I served on ISPAB, Information Security and Privacy Advisory Board, that advises NIST and got a chance to see firsthand what a terrific job the people at the Computer Security Division do, but I had seen that earlier in my work in cryptography. They have a very difficult job and a very complicated situation. The designing and security standards and guidance for federal agencies, those are their customers, but the work that they do actually gets used by businesses, private sector as well as being used internationally. That is when they do things right, and they do things right most of the time. I am very impressed.

But the reason it is a complicated job is because they—in order for them to do their work, providing standards for the Federal Government for federal civilian agencies, they need not only to do just basic research but mostly applied research and security guidance, and they are doing that within an agency, NIST, that focuses on scientific research. So doing the applied work is often a complicated dance for NIST, for the Computer Security Division. And I think they do it extremely well. They do it extremely well because they listen to their customers and they work well with the industry. They are seen as an honest broker.

The 60-Day Review was very clear on the need to work internationally. In order to work internationally, it is extremely useful to have a scientific agency at your side providing guidance. We show up in this country with NIST to do that. Sun was part of a group of industry that had concerns over the Chinese government trying to impose mandatory security requirements on 13 different products. We showed up at the table with NIST, not NSA (National Security Agency), not DHS (Department of Homeland Security). Having NIST at the table was extremely important because the Chinese government saw that as an agency that was not interested in snooping, not interested in finding out about things from China that it shouldn't, but as a scientific agency. And it really helped the decisions that happened, and we as industry are quite happy with the results, and we really relied upon NIST to do that.

That was part of what the 60-Day Review said, the importance of international agreements, and that calls for an elevated role for the Computer Security Division. There are other things that the Computer Security Division should be doing, and I am delighted to

hear, by the way, that the reorganization is off the table because I thought that that was problematic. But there are other things that the Computer Security Division should be doing.

We need to address privacy standards. In recent months, there had been technical work that describes how easy it is to take data that looks as if it is anonymized and re-identify it with other data outside that particular data set, taking information from Netflix that has been anonymized and comparing it with data outside the Netflix database and being able to figure out who the people are. We need scientific standards, technical standards, to talk about how data should be handled to protect privacy. In the past, NIST has worked almost entirely on computer security standards and not on privacy standards, and I think that this role is very important, especially as we move forward with health care. We need NIST, we need the Computer Security Division to be active in the international arena, we also need greater independence for the Computer Security Division. It is impossible to separate policy from security. I am not asking here for NIST to be setting government policy on security. What I am asking is for NIST to be providing advice when a computer security issue comes very close to a policy issue, whether it is about identity verification, identity management, or any one of another technical issues. NIST has that expertise and should be using it more in government.

It is also important to keep the branding of the Computer Security Division which is well-known both within the government now as a result of FISMA (*Federal Information Security Management Act*) and outside the government because of all the excellent work that CSD does.

For all these reasons, I think it is time to elevate the Computer Security Division to the level of a laboratory. I think that that would help a great deal in international work, I think it would be appropriate in terms of the policy effort that I think a computer security group should be doing, I think it is important for privacy standards.

Thank you very much, and I would be happy to answer questions.

[The prepared statement of Dr. Landau follows:]

PREPARED STATEMENT OF SUSAN LANDAU

Mr. Chairman and Members of the Committee:

Thank you for the opportunity to testify today on the Computer Security Division and its role in developing computer security standards and guidance for the Federal Government and the wider community. I am a distinguished engineer at Sun Microsystems, where I concentrate on security, cryptography, and public policy. I have been involved in Sun efforts on cryptography and export control, security and privacy of federated identity management systems, developing our policy stance in digital rights management, and in analyzing security risks of surveillance in communications infrastructures. I am a member of the Commission on Cyber Security for the 44th Presidency, established by the Center for Strategic and International Studies, and I serve on the advisory committee for the National Science Foundation's Directorate for Computer and Information Science and Engineering. I am also a former member of NIST's Information Security and Privacy Advisory Board, where I served six years. I have been a strong supporter of the Computer Security Division for many years.

Fulfilling the Cyberspace Policy Review Recommendations

Over the last decade there have been many discussions and reports regarding the ways and means to achieve cybersecurity. The problem is partially technical and a great deal policy. The most recent *Cyberspace Policy Review*[1] raises several new points.

One of these is the need to work internationally in order to achieve security in cyberspace. With the somewhat boundaryless nature of the Internet, this point is abundantly clear, but this direction has not been a focus of recent U.S. policy. It should be.

Working with other nations on securing cyberspace requires policy efforts—treaties and international agreements of various sorts—but it also requires technical work—standards, for example. NIST is the appropriate agency for the latter. I would expect the Computer Security Division (CSD) at NIST to work hand-in-hand with the Department of State in forging international agreements to secure cyberspace. CSD has a proven history of working well with multiple partners inside and outside the Federal Government. It has played an excellent role in developing standards accepted by the international community. This combination of collaboration and insistence on technical and scientific integrity means that CSD will be a respected partner in discussions with other nations and scientific societies. It is the only U.S. Government agency able to play this role on the civilian side. In fact, it has already been doing so.

Two years ago, for example, the Chinese government notified the World Trade Organization that it planned to impose new mandatory information security certification rules for thirteen product areas. The proposed rules might have barred several types of U.S. products from China's marketplace. Industry, working with the Department of State, the U.S. Trade Representative, and NIST held a series of policy-level and technical level discussions with the Chinese government and impacted the rules finally promulgated this year. CSD's help in this was invaluable.

The *Cyberspace Policy Review* points out the need for defined performance and security objectives. The organization with experience to develop these is CSD.

Indeed, while this was undoubtedly not the intent of the review, the document is a ringing call for the skills, activities, and interventions of CSD. The report certainly makes the case for an expanded role for the division. The review underscores the fact that cybersecurity is a problem that will need international cooperation, emphasizes the importance of working with private industry, and stresses the need for protecting privacy and civil liberties rights while securing cyberspace. The U.S. Government agency with a history and a reputation for scientific integrity and with an ability to work well with civilian groups outside the Federal Government is NIST's Computer Security Division.

In light of such additional responsibilities, it is appropriate to ask how should the CSD be structured to achieve these goals. In one sense, no change is needed: the organization works. In another, some change will be needed because of the additional responsibilities. NIST's Information Technology Laboratory is proposing a restructuring of the division within ITL. I believe such a change is a mistake and will actually hinder CSD's new roles rather than enhance them. I believe that instead that the Computer Security Division should become its own laboratory, the Computer Security Laboratory. CSL more properly suits the U.S.'s cybersecurity needs for the twenty-first century.

What the Computer Security Division Contributes

I look at the proposal to reorganize the Computer Security Division from the perspective of the cryptographic standards DES and AES, and the superb job that CSD did in organizing the competition for the Advanced Encryption Standard. Not only did the division run the competition in an open way that encouraged submissions from around the world, the division even asked for comments on the proposed requirements and changed those requirements in order to fit public needs. This openness resulted in a standard that was accepted immediately almost everywhere. This acceptance of AES is a tremendous win for security. I note that the situation is in sharp contrast to that for 1970's algorithm, DES, about which doubts about secret back doors and weak keys persisted for many years; these impeded the algorithm's acceptance.

The fact is that CSD knows how to work with industry and in a public environment. That means better security not just for the civilian Federal Government,

[1] *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure,* 2009.

whose computer security standards and guidance the division develops, but also for the U.S. private sector and the world.

What Needs to be Sustained and What Needs to be Changed

Developing security standards for federal civilian agencies has various components. In addition to basic research, it requires applied work and guidance documents. Successful security means knowing what customers—in CSD's case, that is the federal civilian agencies—need. It also means knowing how to work with industry to develop the standards and guidance documents that enable computer security to be implemented. This means computer security not just for federal agencies, but for much broader constituencies.

Having CSD within NIST is complicated, because CSD's efforts, including the guidance documents, are out of synch with NIST's research mission. But nonetheless it is NIST, and not DHS or NSA, that is the right home for CSD. In order to be effective CSD must work with industry, developing standards that function at both a technical level and a policy one. A standard that is too complex to implement, or that contradicts customer needs, is a standard that will not be widely deployed. For this reason, the correct home for CSD is the Department of Commerce, the U.S. department that works with industry and that has responsibility for U.S. competitiveness and e-commerce.

CSD is viewed as vendor neutral and an honest broker. The honesty with which CSD does its work and the openness in which it develops its standards and guidance, contribute to the work's broad acceptance and usage. Over the last dozen years, CSD has done a superb job in developing standards and guidance that works, from AES, to SCAP, to the new work on hash standards (Because SHA–1 is increasingly vulnerable to attack, NIST's decision to pursue a SHA–3 algorithm seems to have been prescient). NIST's work on cloud computing has provided reference definitions upon which the Cloud Security Alliance relies; NIST has definitely provided thought leadership in this important and emerging area.

CSD guidance and standards are ones that make sense in a civilian context. The health care industry, for example, which keeps 95 percent of U.S. health care records does not want to adopt computer security standards developed by the military; it wants standards developed for a civilian context. Many CSD standards are used by private industry and in countries around the world. Both U.S. industry and computer security benefit from this.

At the same time, there are things that are missing within CSD. Although the division is not a policy setting organization, CSD needs to be more willing to be involved in policy decisions that verge on technical ones. This includes the Personal Identity Verification (PIV) standards, where CSD should have pushed back on OMB, and said that these standards cannot be implemented effectively within the time frame; there will be security costs, there will be privacy costs that a slower timetable would alleviate. Other discussions in which CSD should be involved on the policy level includes the current Identity, Credential, and Access Management (ICAM) effort on identifiers for Level of Assurance 1.

CSD also needs to work more on usability and security, and on usability and privacy. Security controls that are too complex to use and privacy standards that are unclear help neither security or privacy. I understand that CSD has begun active work in this direction.

Finally—and this is a long-term challenge—CSD could do a better job of making its work public. From the state of its web page, in which it is challenging to find information (this is a subject about which the Information Security and Privacy Advisory Board, and probably others, have raised concerns), to its lack of sufficient workshops on implementing its standards, CSD does not do sufficient outreach. It is, for example, CSD which should be running workshops for small businesses on security (and not the FBI). CSD produces high quality, vendor-neutral security guidance, and this high quality information should be much more broadly publicized—and therefore used—than it is.

If CSD is to develop privacy standards and to do effective outreach, CSD will need an increased budget. These are new responsibilities and CSD's people are already stretched thin. These are difficult budget times and funding is tight, but given the criticality of our nation's cybersecurity needs, such increased appropriations are both appropriate and necessary. The money spent now will prevent higher costs to society as a result of weak cyber protections; it would be money well spent.

The Proposed Reorganization

For reasons that are not entirely clear, the Information Technology Laboratory is attempting a reorganization. Some aspects of this seem excellent—moving the head

of CSD to the secretary's office to work on policy-related aspects of computer security is a smart plan—but others raise great concern. The argument is being made that there would be increased synergy by moving aspects of security, such as identity management, into other parts of the organization. I disagree.

Synergy is best achieved by keeping members of the Computer Security Division together. Researchers find commonalities in security issues, whether it is protecting VoIP or securing virtual worlds, when they work closely together. While spreading security across an IT support organization might be useful, the same is not true for an organization doing research. The rationale for one split, moving identity management to the testing division and separating that group from most of computer security, is that identity management is intimately tied up with testing. This is correct, but in fact identity management is also intimately tied to computer security, and separating the two areas weakens the whole. Dividing different groups supporting CSD's mission will be detrimental to the work CSD does. Ultimately the effect will be to weaken CSD's impact on federal civilian security.

In addition, having multiple sources for federal civilian computer security standards and guidance will cause CSD to lose its identity as the "go-to" organization for federal civilian security, and the division will lose the branding recognition that has already occurred. The proposed reorganization, if it should happen, will make it more difficult for people to locate the NIST computer security information they need (a problem that is already too difficult). This is the wrong step at the wrong time.

I believe that instead we should be looking to create a separate Computer Security Laboratory within NIST. There are many arguments for such a change.

The first is that there are new responsibilities the division should take on. In the world of massive databases and such privacy-threatening technologies as social networks, the CSD mission should create privacy standards. This includes, for example, how to handle data to prevent loss of privacy due to data aggregation, what suitable anonymization techniques are, etc. This is a new and important job for CSD.

A second issue is that increasingly we will need to bring to the bilateral and multilateral bargaining table a government partner on technical cybersecurity issues. This partner must be one that is trusted by all sides and this means the division will be part of a U.S. team negotiating internationally on issues of cybersecurity. In such negotiations, NIST's technical people must be perceived as having the right stature. The elevation of the division to a laboratory would be very useful to U.S. interests and fits in with the actions proposed by the *Cyberspace Policy Review.*

A third important reason is that a NIST laboratory-level computer security organization would provide the correct level of independence for such an organization. The director would be in a better position to provide the policy guidance needed in discussions related to computer security and privacy. Note that I am not talking about setting government policy, but advising on the policy implications of what appear to be purely technical decisions, whether in the adoption of a PIV card that allows the biometric authenticator to be read without a guard present, or in the use of OpenID as a Level of Assurance 1 identifier.

In elevating CSD to a laboratory within NIST, CSD's branding is retained. This is important to the effective filling of the CSD mission.

As we all know, cybersecurity will only increase in importance with time. A separate Computer Security Laboratory will enhance CSD's visibility, and ensure that CSD's work is not diluted by other, excellent work in ITL (but work that is unrelated to the computer security effort). In order to function effectively, CSD needs to be a single unit, but with more independence, with strong support from its parent agency of NIST, and with the ability to speak with an honest, scientific voice. A separate laboratory within NIST is the right way for CSD to go at this time.

Thank you very much for the opportunity to address the Committee. I eagerly await any questions you might have.

BIOGRAPHY FOR SUSAN LANDAU

Susan Landau is a Distinguished Engineer at Sun Microsystems Laboratories, where she works on security, cryptography, and policy, including surveillance and digital-rights management issues. Landau had previously been a faculty member at the University of Massachusetts and Wesleyan University, where she worked in algebraic algorithms, and she held visiting positions at Yale, Cornell, and the Mathematical Sciences Research Institute at Berkeley.

Landau is co-author, with Whitfield Diffie, of *"Privacy on the Line: the Politics of Wiretapping and Encryption"* (MIT Press, original edition: 1998; updated and expanded edition: 2007), which won 1998 Donald McGannon Communication Policy Research Award, and the 1999 IEEE–USA Award for Distinguished Literary Contributions Furthering Public Understanding of the Profession.

Landau participated in the 2006 ITAA study on the security risks of applying the *Communications Assistance for Law Enforcement Act* to Voice over IP, and is also primary author of the 1994 Association for Computing Machinery report *"Codes, Keys, and Conflicts: Issues in US Crypto Policy."* Prior to her work in policy, Landau did research in symbolic computation and algebraic algorithms, discovering several polynomial-time algorithms for problems that previously only had exponential-time solutions.

Landau is a member of the Commission on Cyber Security for the 44th Presidency, established by the Center for Strategic and International Studies, and serves on the advisory committee for the National Science Foundation's Directorate for Computer and Information Science and Engineering. She is also an Associate Editor for *IEEE Security and Privacy* and a section board member of Communications of the ACM. Landau serves on the Executive Council for Association for Computing Machinery Committee on Women in Computing, as well as on the Computing Research Association Committee on the Status of Women in Computing Research. Landau served for six years on the National Institute of Standards and Technology's Information Security and Privacy Advisory Board. She has been a member of ACM's Advisory Committee on Privacy and Security and ACM's Committee on Law and Computing Technology as well as an Associate Editor of the Notices of American Mathematical Society.

Landau is the recipient of the 2008 Women of Vision Social Impact Award, a Fellow of the American Association for the Advancement of Science, and a Distinguished Engineer of the Association for Computing Machinery. More information on her publications and awards can be found at *http://research.sun.com/people/slandau*

Landau received her Ph.D. from MIT (1983), her MS from Cornell (1979), and her BA from Princeton (1976).

Chairman WU. Thank you very much, Dr. Landau. Dr. Schneck, please proceed.

STATEMENT OF DR. PHYLLIS SCHNECK, VICE PRESIDENT, THREAT INTELLIGENCE, MCAFEE CORPORATION

Dr. SCHNECK. Good afternoon, Chairman Wu, Ranking Member Smith, Members of the Subcommittee. My name is Phyllis Schneck. I am the Vice President of Threat Intelligence at McAfee. We are headquartered in Santa Clara, California. A core of our cyberlabs and our cyber research is in Beaverton, Oregon.

I testify today on behalf of the BSA, the Business Software Alliance. Thank you for the opportunity to testify on cybersecurity and the role of the ITL. I commend the Subcommittee for focusing on these important issues.

McAfee and BSA believe that innovation and standards are among the most important tools we have to improve our cybersecurity. Therefore, our primary recommendation regarding the role of the ITL in implementing the recommendations of the 60-Day Review is to contribute to an integrated, U.S. Government strategy to influence the development of international standards on cybersecurity.

Please allow me to explain the important links between innovation, cybersecurity and international standards. First, we believe innovation is key to cybersecurity. Those persons intent on doing harm, whether cybercriminals, spies, hostile nations, even terrorist groups, find new ways to attack. They adopt those new technologies all the time, and we must stay ahead of them, and to do that innovation is key.

Second, we believe that global industry-led voluntary standards are critical to innovation. This is because first, they facilitate interoperability between systems built by different vendors. Second, they facilitate competition between those vendors, leading to great-

er choice, lower cost. Finally, they spur the development and the use of innovative and secure technologies because they are regularly updated.

Cybersecurity depends on innovation which in turn depends on global industry-led standards. This is why we urge the United States to support and uphold these standards by developing a comprehensive, international cybersecurity standards strategy.

Currently the U.S. Government's involvement in standards development is ad hoc, incomplete and uncoordinated. The 60-Day Review recognized this lack of coordination and called for a comprehensive strategy that defines what cybersecurity standards we need, where they are being developed and what agencies will represent the United States for each.

NIST has expertise in standards and in cybersecurity and is internationally respected, so it should play an important role in the creation and implementation of such a strategy.

Conversely there are missteps the government should avoid. Most importantly, we should not impose country-specific, government-created technology standards for cybersecurity. This would set a dangerous precedent that other nations would follow to create their own divergent standards. This would be at odds with the global nature of the Internet, it would Balkanize the global marketplace, and it would inhibit inter-operability. We believe our position is fully consistent with President Obama's statement when he released the Cyberspace Policy Review on May 29. President Obama said, "My Administration will not dictate security standards for private companies. On the contrary, we will collaborate with industry to find technology solutions that ensure our security and promote prosperity."

I will now address the proposed reorganization of the ITL and CSD. We believe the success of CSD depends first on budget and manpower. CSD is already under-resourced and understaffed. As we give them new missions in the context of tighter federal budgets, they will need sufficient resources. We will also need to ensure that NIST funds intended for Congress for cybersecurity are not spent on other projects.

Second, CSD works with a wide range of industry and academic partners. The process under way needs to be open and transparent so that it can be informed by the views of the stakeholders.

And third, whatever we do, we should avoid diminishing the visibility, priority and resources accorded to cybersecurity within NIST.

Finally, I would like to close my testimony with a few other recommendations about further activities of CSD. As Congress considers how to elevate cybersecurity as a government priority, including how to reform FISMA, the *Federal Information Security Management Act,* CSD should produce the following. First, government-wide standards and guidelines for real-time monitoring, audit and analysis of data about the security of federal networks. And second, government-wide standards and guidelines developed jointly with industry for sharing threat and vulnerability information among federal agencies and with the private sector.

NIST must also continue to invest in cybersecurity research and development. BSA has called for the creation of a national

cybersecurity R&D plan, and we believe that NIST would play an important role under such a plan, given its own R&D work and its private-sector relationships.

Thank you, and I look forward to answering any questions.

[The prepared statement of Dr. Schneck follows:]

PREPARED STATEMENT OF PHYLLIS SCHNECK

Chairman Wu, Ranking Member Smith, Members of the Committee, thank you for the opportunity to testify today on the important issue of cybersecurity, and the role of the National Institute of Standards and Technology (NIST)'s Information Technology Laboratory (ITL).

My name is Phyllis Schneck, and I am the Vice President of Threat Intelligence at McAfee. McAfee is the world's largest dedicated security technology company. McAfee is committed to relentlessly tackling the world's toughest security challenges. The company delivers proactive and proven solutions, services and global threat intelligence that help secure systems and networks around the world, allowing users to safely connect to the Internet, browse and shop the web more securely.

As Vice President of Threat Intelligence, I am responsible for the design and application of McAfee's Internet reputation intelligence, strategic thought leadership around technology and policy in cybersecurity, and leading McAfee initiatives in critical infrastructure protection and cross-sector cybersecurity.

I testify today on behalf of the Business Software Alliance (BSA), of which McAfee is a member. BSA is the foremost organization dedicated to promoting a safe and legal digital world. BSA is the voice of the world's commercial software industry and its hardware partners before governments and in the international marketplace.[1]

My testimony will address three questions:

1. What could NIST do to address some of the recommendations of the Cyberspace Policy Review?
2. What is our assessment of the proposed reorganization of NIST's ITL, and how will it improve the outcomes of ITL activities?
3. Given the current emphasis on information assurance and cybersecurity, what recommendations do we have on how ITL might improve its effectiveness or expand the scope of its activities and their impact?

1. What could NIST do to address some of the recommendations of the Cyberspace Policy Review?

McAfee and BSA welcomed the 60-day review ordered by the President. We believe that cybersecurity needs to be elevated as a priority of this country. We also welcomed the openness of the review process, which allowed a wide range of stakeholders, and in particular owners and operators of critical cyber infrastructure, to provide their views and recommendations. In the end, while the final report contains many recommendations and so will require that industry remain engaged throughout their implementation, McAfee and BSA were broadly supportive of the Cyberspace Policy Review's conclusions.

I would like to touch on a few of the recommendations of the Cyberspace Policy Review that we believe are of particular importance and relevance to NIST.

Firstly, we strongly support the Cyberspace Policy Review's call for an integrated U.S. Government strategy to influence the development of international standards on cybersecurity.

Such a strategy would recognize the important links between innovation, cybersecurity and international standards.

We believe innovation is key to greater cybersecurity. Those persons intent on doing harm, whether profit-motivated cyber criminals, cyber spies, hostile nations or terrorist groups, find new ways to attack and adopt new technologies all the time. We must stay a step ahead of them. To do this, innovation is key.

A necessary element of ensuring continued innovation is sound standards policy. Global, industry-led, voluntary standards and best practices create the environment where multiple innovative solutions can flourish by:

---

[1] BSA members include Adobe, Apple, Autodesk, Bentley Systems, CA, Cadence Design Systems, Cisco Systems, Corel, CyberLink, Dassault Systèmes SolidWorks Corporation, Dell, Embarcadero, HP, IBM, Intel, Intuit, McAfee, Microsoft, Minitab, Quark, Quest Software, Rosetta stone, SAP, Siemens, Sybase, Symantec, Synopsys, and The MathWorks.

- Facilitating inter-operability between systems built by different vendors.
- Facilitating competition between vendors, leading to greater choice and lower cost.
- Spurring the development and use of innovative and secure technologies, because industry-led standards are regularly updated.

This is why we urge the U.S. Government to support and uphold global, industry-led standards and best practices on cybersecurity, by doing the following:

- First, the U.S. Government needs to develop a comprehensive international cybersecurity standards strategy. What we have currently is a collection of ad hoc, incomplete and uncoordinated efforts. The White House Cyberspace Policy Review recognized this lack of coordination. NIST should play an important role in the creation and implementation of such a strategy. The strategy needs to answer the following questions:
  1. What cybersecurity standard development efforts is the U.S. currently involved in?
  2. What cybersecurity standards do we need?
  3. Where are they being developed?
  4. What agencies will represent the U.S. for each of them?
- Second, the government should identify the relevant international industry-led cybersecurity best practices, and recognize and promote their use in federal systems. Government, industry and academia should collaborate to identify international industry-led best practices, and McAfee and BSA would eagerly contribute to such a process.

But there are also missteps the government should avoid. Most importantly, the government should not impose country-specific technology standards for cybersecurity, in particular standards developed by government agencies, except in narrowly tailored national security situations. This would set a precedent that other nations would follow to create their own, divergent standards. The end result would be at odds with the global nature of the Internet, would contribute to breaking up the global marketplace into national markets, and would inhibit rather than promote inter-operability.

Finally, I would add that if NIST were tasked with creating and mandating such domestic standards, it would lessen the high regard it enjoys not just in the United States, but also internationally, as an arbiter of a process grounded in science.

Therefore, cybersecurity policy-makers should support the global nature of the IT marketplace, rather than contribute to breaking it up into national markets.

We believe our position is fully consistent with President Obama's statement, when he released the Cyberspace Policy Review on May 29: *"My administration will not dictate security standards for private companies. On the contrary, we will collaborate with industry to find technology solutions that ensure our security and promote prosperity."*

Secondly, I would like to say a few words about the Cyberspace Policy Review's recommendation to launch a public education and awareness campaign.

Educating the public about threats and about common sense measures it can adopt to protect itself, is important. That is why the CEOs of BSA raised this issue when they met with Secretary of Homeland security Napolitano this year. Many BSA members, including McAfee, have made important investments in educating the public about cybersecurity, for example by actively supporting and sponsoring the National Cyber Security Alliance (NCSA), the preeminent public-private partnership between industry, the U.S. Department of Homeland Security (DHS) and non-profit institutions, to promote cybersecurity awareness for home users, small and medium size businesses, and primary and secondary education.

McAfee and BSA believe a major education and awareness campaign on the scale envisaged by the Cyberspace Policy Review should build upon the foundation of the NCSA. If NIST were to take a role in education and awareness, we recommend that it do so through the national campaign that NCSA should coordinate. NCSA should be the focal point, using and expanding the relationships and brand it has already built with a multitude of local stakeholders—schools and universities, community-based organizations, local governments, local chambers of commerce, home-owners associations, etc.

Thirdly, NIST has a valuable role to play in carrying out the Cyberspace Policy Review's call for building a cybersecurity-based identity management vision and strategy.

Identity and authentication are foundational building blocks of a modern and fundamentally secure cyberspace. The Administration is already working to implement this recommendation of the Cyberspace Policy Review, and we expect them to issue a draft document in the coming months to the public for comment.

NIST should play a critical role in crafting and implementing this government strategy, on the basis of the important contributions it has made to previous federal identity and authentication initiatives, such as the implementation of Homeland Security Presidential Directive 12 (HSPD–12). As identity and authentication can apply not only for individuals, but also for devices, NIST's ability to advise and influence this strategy will be critical to ensuring its technical feasibility and operational success.

As the Cyberspace Policy Review notes, it is important that the government not mandate the use of specific identity management systems, but rather ensure that they are available as opt-ins. We also agree with the Review that a variety of interoperable systems should be offered, rather than the government picking a single provider or technology, which would stifle innovation.

2. What is our assessment of the proposed reorganization of NIST's ITL, and how will it improve the outcomes of ITL activities?

BSA has not had the opportunity to reach a common position among its members on the reorganization of the ITL. However, I would like to make the following comments about what is at stake.

First, we believe two important factors in the future success of the Computer Security Division (CSD) of the ITL are budget and manpower. CSD is already underresourced and under-staffed. As we give them new missions in a context of tighter federal budgets, sufficiency of resources will be a key concern. We will also need to ensure that NIST funds intended by Congress for cybersecurity are not spent on other projects, and this can be achieved by requiring that ITL regularly report to this committee on how it spends funds designated for cybersecurity.

Second, the process that will determine the future course of the ITL needs to be open, transparent and based on the input of the wide range of stakeholders, in particular from the IT industry and academia, who work with CSD.

And third, the guiding principle should be to avoid diminishing the visibility, priority, and resources accorded to cybersecurity within NIST.

3. Given the current emphasis on information assurance and cybersecurity, what recommendations do you have on how ITL might improve its effectiveness or expand the scope of its activities and their impact?

First, McAfee and BSA want to restate their deep appreciation for the outstanding work done by the ITL and CSD over the years.

I would like to highlight two reasons in particular that have contributed to establishing ITL as a widely-respected leader:

1. ITL works collaboratively with stakeholders. Its work products are well regarded because they draw upon the best contributions of leading experts in their fields, from industry but also from academia. One of the most salient examples is the AES encryption standard, whose underlying cryptographic algorithm had been developed by Belgian academics and selected through a rigorous competition. The openness of the selection process has greatly contributed to inspiring confidence in AES and thus in its wide adoption outside the Federal Government.
2. For the security of federal systems, and with very few exceptions, ITL does not in fact enact mandatory technology standards. Rather, it offers guidance—through its Special Publications 800 (SP 800) series—that are flexible enough to allow each agency to adopt the security posture most appropriate to its risk profile. We need to ensure that federal agencies more consistently implement this guidance.

As Congress considers how to reform FISMA to place greater emphasis on actual security of federal networks and systems, federal agencies will need in particular that CSD expand its scope of activities, building on its legacy of public-private collaboration and non-mandatory guidance, to produce the following:

- Government-wide standards and guidelines for real-time monitoring, auditing and analysis of data about the security, performance and health of federal networks and systems across the entire Federal Government. This would contribute to providing holistic, end-to-end security of federal networks, rather than focusing on the security of single points of failure.

- Government-wide standards and guidelines for sharing threat and vulnerability information among federal agencies and with the private sector. While we think, as I said before, that NIST should always work collaboratively with stakeholders, given the private sector impact of information sharing, any NIST effort in this area should be undertaken jointly with the private sector, in coordination with DHS.

Global, industry-led standards must continue to underpin the global IT ecosystem. Therefore, these two categories of NIST standards and guidelines should draw from global, industry-led standards to the greatest extent possible.

Importantly, in producing such standards and guidelines, NIST should spur innovation by always striving to, per the terms of the *National Institute of Standards and Technology Act, "ensure that such standards and guidelines do not require specific technological solutions or products, including any specific hardware or software security solutions; ensure that such standards and guidelines provide for sufficient flexibility to permit alternative solutions to provide equivalent levels of protection for identified information security risks; and use flexible, performance-based standards and guidelines that, to the greatest extent possible, permit the use of off-the-shelf commercially developed information security products."*[2]

Finally, NIST must continue to push at the edges of cybersecurity research and development. BSA has expressed in the past to this committee the importance that we attach to research and development (R&D) to improve our nation's cybersecurity, and we have called for a national cybersecurity R&D plan. We believe that NIST would play an important role under such a plan, given its own R&D work and its ability to reach out to the R&D arms of many companies.

In conclusion, I want to reiterate the importance that we attach to:

- Innovation as a major tool to improve our cybersecurity;
- The role that R&D and international, industry-led standards play in spurring innovation and in improving cybersecurity; and
- The development by the U.S. Government of an international cybersecurity standards strategy.

BIOGRAPHY FOR PHYLLIS SCHNECK

For more than a decade, Dr. Phyllis Schneck has held a distinguished presence in the security and infrastructure protection community. Currently serving as Vice President of Threat Intelligence at McAfee, she is responsible for the design and application of McAfee's Internet reputation intelligence, strategic thought leadership around technology and policy in cybersecurity, and leading McAfee initiatives in critical infrastructure protection and cross-sector cybersecurity.

Schneck recently served as a commissioner and a working group co-chair on the public-private partnership for the CSIS Commission to Advise the 44th President on Cyber Security. Schneck also served for eight years as Chairman of the National Board of Directors of the FBI's InfraGard program and as Founding President of InfraGard Atlanta, growing the InfraGard program from 2,000 to over 26,000 members nationwide. Named one of *Information Security Magazine*'s Top 25 Women Leaders in Information Security, Schneck holds three patents in high-performance and adaptive information security, and has six research publications in the areas of information security, real-time systems, telecom and software engineering.

Before joining McAfee, she served as Vice President of Research Integration at Secure Computing. Schneck holds a Ph.D. in Computer Science from Georgia Tech where she pioneered the field of information security and security-based high-performance computing.

Chairman WU. Thank you very much, Dr. Schneck. Mr. Starnes, please proceed.

[2] Section 20 of the *National Institute of Standards and Technology Act* (15 U.S.C. 278g–3), subsection (c)(5–7).

STATEMENT OF MR. WILLIAM WYATT STARNES, FOUNDER, CEO, AND PRESIDENT, SIGNACERT, INC.; FOUNDER, TRIPWIRE, INC.

Mr. STARNES. Good afternoon, Mr. Chairman, and respected Members of the Committee. I appreciate the opportunity to present today before the Committee.

As you know, my name is Wyatt Starnes. I am the founder of a company called Tripwire, Incorporated. Tripwire has been heavily used in both government and commercial security practice, and I currently serve as the CEO and President of SignaCert, also involved in information assurance issues.

We have been working with both companies very closely with commercial and government sectors in the areas of information assurance and cybersecurity for better than a decade.

For purposes of my testimony and for reasons better described in my written testimony, we prefer the term "cyber assurance," and the reason we tend to think this way is we deal both with non-malicious and malicious activity and have found empirically that non-malicious activity, unauthorized changes and uncontrolled changes can cause up to 90 percent of the failures in complex information technology systems. We really believe that that view needs to be broader than just cybersecurity.

Relative to NIST and the 60-Day Review, my personal experience tells me that NIST is already ahead of the curve in most of the key areas discussed in the report. What I would observe in general about the report is it lacks substantive, out-of-the-box thinking. There are bigger and more important things we can be doing than pure black list-based cybersecurity, which is the goal of keeping the bad guys out of the systems. We must more broadly assure that the systems are intact as designed.

But NIST's contributions relative to all of these issues, cyberassurance and cybersecurity, have in fact been formidable. So I am going to talk about three of those.

One and perhaps most importantly is the 800-series body of work which is literally volumes of work, and this work has contributed significantly to the state-of-the-art for both federal and commercial IT software and systems management.

Secondly, I would like to focus on some extension of that work on a practical sense, and that is a multilateral and both private and public partnership and teaming that has been in place to effect the security, content, automation protocol, or SCAP methodology. Ms. Furlani referred to that in generalized security cataloging. We as an industry participant see this as an extremely important method and protocol, leveraging heavily the work of NIST with the 800-series documents as well as bringing in the best of some of the intelligence community and DOD (Department of Defense) work.

In my opinion, the SCAP method and the increased emphasis on continuous monitoring as opposed to pure accreditation and auditing methods represent far and away the most important advance federal IT systems management that I have seen.

I think I can be even briefer on the subject of the reorganization of ITL. My personal belief there, having worked inside and outside of NIST, that the management team is very capable of making decisions like this. I would expect that the goal of these changes are

to align the expertise with a changing mission requirements and budgetary requirements and would also believe that this movement to a broader view of cyberassurance as opposed to pure computer security is a motivation. IT best practices are increasingly a horizontal cross-agency issue, and therefore it is logical to consider this reorganization.

Relative to contributions on the 60-Day Review, the main missing element that we saw is again the focus on the defensive architecture. We actually see moving to a more offensive position. The SCAP framework leads us a long way down that path. So it is more than just keeping the bad guys out. It is making sure that the systems are good and deployed as we intended them. So there is a software supply chain issue. There is a change management detection issue. A lot of that is being encompassed in the work at SCAP, and generally industry refers to these methods as whitelisting methods, in complement to the black listing methods. Make sure the bad code is kept out, make sure the good code is good. The combination of those methods is very powerful.

So in conclusion, I would like to urge NIST to continue their great work multilaterally with their peers in government and industry to distill the best of the best ideas into the NIST standards and methods on a timeline that fully recognizes that we are behind and heavily exposed.

Thank you, and I welcome any questions.

[The prepared statement of Mr. Starnes follows:]

PREPARED STATEMENT OF WILLIAM WYATT STARNES

Good afternoon Mr. Chairman and respected Members of the Committee. I appreciate the opportunity to present before this committee today.

My name is Wyatt Starnes, a Founder of SignaCert, Inc. and Tripwire, Inc., and currently the CEO and President of SignaCert. Please see my narrative biography for more details on my background and experience.

I should note for the record that I did serve as member of the National Institute of Standards and Technology (NIST) Visiting Committee on Advanced Technology (VCAT), and while I have some recent experience with NIST and the Information Technology Labs (ITL), I am no longer serving as a VCAT member.

As you are aware Mr. Chairman, I have been working closely with both the commercial and government sectors in the areas of information assurance and cyber security for many years. For the purposes of this testimony I will generally reference the Information Assurance and Cybersecurity issues as "Cyber Assurance" for the following reasons:

> In my opinion labeling our challenge as "Cybersecurity" is limiting. Our full goal must be to address ALL issues that relate to improving the security, availability, stability and reliability of the computing devices used to create and deliver complex IT business processes.
>
> We must address the risks that are hostile in source and nature (malicious), as well as hardware and software design, delivery, and maintenance weaknesses (non-malicious) that are also known to induce risk.
>
> It is well established that undetected non-malicious changes do increase malicious risk, and also cause IT business service delivery instability and failure.

It is my belief that we are at a very critical time in our nation's history with regards to our Cyber Assurance practices. We must act now, and bring increased creativity, technology and innovation to these challenges.

I would like to commend this subcommittee, led by Congressman Wu and his staff, for continuing to direct focus to our cyber assurance challenges, and the important contributions that NIST has made, and continues to make, in support of these critical national cyber assurance priorities.

Specific questions posed by the Subcommittee

The Committee posed three questions for me to address during this hearing:

1. What could NIST do to address the recommendations in the 60-day review?
2. What are my thoughts and comments on the Reorganization of ITL?
3. Given the current emphasis on Information Assurance and Cybersecurity, what are my recommendations on how ITL might improve its effectiveness or expand its scope/activities and impact?

NIST and the 60-Day Review

Relative to question one, regarding NIST and the *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (the 60-day review), my personal experience tells me that NIST is already ahead of the curve with its contributions to the key issues and priorities presented in the 60-day review document that was delivered to the President.

Before I address these specifically, I would like to briefly comment on the role of NIST and its legislated mission and budgeted charter.

As the Committee knows, NIST is a non-regulatory agency founded on March 3, 1901, as the National Bureau of Standards and was the Federal Government's first physical science research laboratory.

While it may surprise many citizens, it is no accident that NIST was created as an agency within the Department of Commerce where its primary mission is 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.**

An even simpler way to state this mission is **to reduce the friction of commerce by advancing measurement science, standards and technology.**

NIST's role against the 60-day review is clearly in relation to creating and administering IT measurement standards, technology and methods to enable better, and more standardized methods for optimizing the efficacy of cyber assurance methods.

For the purposes of this, my written statement, I would like to elaborate on some of the specific work accomplished by NIST. While there is much more Information Technology Labs (ITL) work that deserves acknowledgment, I will focus these comments on the following areas:

- The 800-series Information Technology Support for *Federal Information Security Management Act* (FISMA).
- The National Software Reference Library (NSRL) work, and it relationship to the *Help America Vote Act* (HAVA), and its potential contributions to FISMA and the Security, Content and Automation Protocol (SCAP).
- The multilateral (public and private) effort to establish and enhance the SCAP method.

FISMA and the "800-Series" body of work:

From the NIST special publication 800–53 Revision 2 (The bold text was added by this author for emphasis):

> The **Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure.** ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. **ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.** The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

With the charter and intent of the work described here (from the same publication):

> This document has been developed by the **National Institute of Standards and Technology (NIST) to further its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, P.L. 107–347. NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such stand-**

ards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A–130, Section 8b(3), Securing Agency Information Systems, as analyzed in A–130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A–130, Appendix III.

This guideline has been prepared for use by federal agencies. It may also be used by non-governmental organizations on a voluntary basis and is not subject to copyright. (Attribution would be appreciated by NIST.) Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official.

Mr. Starnes Observations on the 800-series work:

While the creators and authors of the 800-series publications have been consistently humble relative to their contributions in bringing this important work forward, the impact to both government and industry has been enormous.

I congratulate the dedicated teams across NIST for their work and I'd like to specifically commend the Director of ITL, Cita Furlani, for her steadfast vision and support of the implementation of this work by NIST ITL in order to serve these critical national needs.

Additionally I would like to recognize Ron Ross, Stu Katzke, Arnold Johnson, Marianne Swanson, Gary Stoneburner and George Rogers and many others for their contributions to this foundational body of work.

Areas for NIST improvement:

In general, the areas I outline below are already well underway by NIST, and I raise them to encourage continued focus only:

- Make the 800-series documents and recommendations easier to read and use by the targeted constituencies. Bigger, in terms of content volume, is not necessarily better. I support the effort to streamline the 800-series documents making them more concise and easier to utilize.
- Continue to drive emphasis with all federal IT practices, including FISMA and the supporting standards and methods, from "Certification and Accreditation" (C&A) and periodic compliance to "Continuous Monitoring."

Help America Vote Act (HAVA) and the National Software Reference Library (NSRL):

From the NIST web site:

The Help America Vote Act:

The *Help America Vote Act* (HAVA) of 2002 (Public Law 107–252) was passed by Congress "to establish a program to provide funds to States to replace punch card voting systems, to establish the U.S. Election Assistance Commission (EAC) to assist in the administration of federal elections and to otherwise provide assistance with the administration of certain federal election laws and programs, to establish minimum election administration standards for states and units of local government with responsibility for the administration of federal elections, and for other purposes."

NIST's roles under HAVA:

HAVA established the Technical Guidelines Development Committee (TGDC) to assist the EAC with the development of voluntary voting system guidelines. HAVA directs the Director of the National Institute of Standards and Technology (NIST) to chair the TGDC and to provide technical support to the TGDC in the development of these voluntary guidelines.

- In addition HAVA directs NIST to conduct an evaluation of independent non-federal laboratories to carry out the testing of voting systems and to submit recommendations of qualified laboratories to the EAC for accreditation. HAVA also charges NIST with monitoring and reviewing laboratories accredited by the EAC.

National Software Reference Library:

From the NIST web site:

This project is supported by the U.S. Department of Justice's National Institute of Justice (NIJ), federal, State, and local law enforcement, and the National Institute of Standards and Technology (NIST) to promote efficient and effective use of computer technology in the investigation of crimes involving computers. Numerous other sponsoring organizations from law enforcement, government, and industry are providing resources to accomplish these goals, in particular the FBI who provided the major impetus for creating the NSRL out of their ACES program.

The National Software Reference Library (NSRL) is designed to collect software from various sources and incorporate file profiles computed from this software into a Reference Data Set (RDS) of information. The RDS can be used by law enforcement, government, and industry organizations to review files on a computer by matching file profiles in the RDS. This will help alleviate much of the effort involved in determining which files are important as evidence on computers or file systems that have been seized as part of criminal investigations.

The RDS is a collection of digital signatures of **known, traceable software applications.** There are application hash values in the hash set which may be considered malicious, i.e., steganography tools and hacking scripts. **There are no hash values of illicit data, i.e., child abuse images.**

Mr. Starnes' Observations on HAVA and NSRL:

In my opinion, HAVA comprises some of the most important technical work underway by USG to automate and enforce technical and social trust that helps enable our democratic process. HAVA can and should serve as a lighthouse for other countries to follow for enabling a seamless, automated and trusted voting and vote aggregation system.

I note HAVA in my testimony because the methods and technologies specified under the guidance, and the software measurement methods developed under the NSRL programs, have tremendous importance and utility over and above the HAVA use cases.

Essentially HAVA and NSRL represent a practical instantiation of a "trust-based" compute model. I believe that trust-based computing methods are crucial to achieve better and more transparent, holistic Cyber Assurance for both the government and commercial sectors.

A major tenet of the HAVA/NSRL method is the "positive system attestation" methods required by the HAVA language. Under HAVA, Software used to operate electronic voting apparatus must be cryptographically measured and validated to a trusted reference. NSRL data is used to create the "trust reference" for software attestation.

Generally referred to as software "Whitelisting" by industry, these capabilities promise to "close the blind spot" in our view of IT by establishing the capability to ensure the "as-deployed" software state (and ONLY the as-deployed software state) is currently in place on the IT device or system.

This "positive trust-based method" has broad ramifications for government and industry. By fully utilizing whitelisting techniques we can:

- Reduce the exposure of malicious and hostile software that is "hiding in plain sight."
- Establish and prove supply chain validity (provenance) of the software that is deployed on our mission critical IT devices ranging from Servers to Blackberry's. This is increasingly important in the "outsourced" and "open source" world that we now rely on.
- Increase the transparency and automation of complex IT system management by creating a systematic "closed-loop" measure/validate method. This addresses both malicious and non-malicious change quickly and efficiently.
- Enabling continuous monitoring of the positive state of the software stack has been shown to dramatically increase IT uptime and stability, while reducing the labor and manpower required for the delivery of that capacity.

Mr. Starnes' Recommendations to NIST on Whitelisting:

- NIST should explore its role with industry (companies and standards groups) relating to whitelist content exchange standards (XML schemas, etc.) in order to ensure that industry and government content and methods are "interchangeable." This not only serves government customers with improved frameworks such as SCAP (discussed below), but it also enables industry to

better serve broader government initiatives, such as HAVA and other extended NSRL-like use cases, such as improved cyber forensics.

- NIST should encourage industry (especially platform and software vendors) to support supply chain validation methods, such as whitelisting methods and content, as a standard practice for IT systems management and security. Broader adoption and support of Common Platform Enumeration, or CPE, should also be stressed as a part of the software measurement for operational monitoring and supply chain assurance purposes.

The Security, Content and Automation Protocol effort:

The SCAP method is described below.

From the NIST web site:

"The Security Content Automation Protocol (SCAP) is a synthesis of inter-operable specifications derived from community ideas. Community participation is a great strength for SCAP, because the security automation community ensures the broadest possible range of use cases is reflected in SCAP functionality. This web site is provided to support continued community involvement. From this site, you will find information about both existing SCAP specifications and emerging specifications relevant to NIST's security automation agenda. You are invited to participate, whether monitoring community dialogue or leading more substantive activities like specification authorship.

NIST's security automation agenda is broader than the vulnerability management application of modern day SCAP. Many different security activities and disciplines can benefit from standardized expression and reporting. We envision further expansion in compliance, remediation, and network monitoring, and encourage your contribution relative to these and additional disciplines. NIST is also working on this expansion plan, so please communicate with the SCAP Team early and often to ensure proper coordination of efforts."

Mr. Starnes' Observations on SCAP:

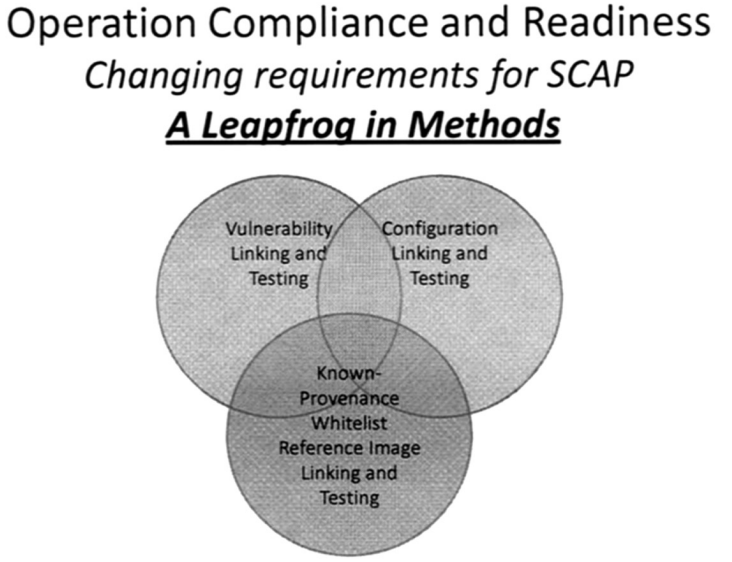
A major goal with SCAP was to create a normalized "content" view, specifically around IT vulnerability and configuration intelligence. Using several databases, vulnerabilities and configurations can be mapped to government IT platforms. This helps serve prescriptive IT device provisioning and deployment, operational compliance, continuous monitoring and remediation.

SCAP provides a powerful and extensible set of methods, content and embedded IT best practices, enhancing system visibility while improving the validation periodicity for complex IT environments.

SCAP is the culmination of many years of public-private cooperation and, within government, one of the best examples of multilateral government -to-government cooperation this witness has seen.

I applaud the efforts of NIST, NSA, DHS, DISA, MITRE and many others for bringing this ground-breaking best practices and content method to fruition.

Industry is already working to extend SCAP methods in several ways including known-provenance image management, as shown within the blue circle below.



Mr. Starnes' Recommendations on SCAP:

Government IT professionals, including NIST staff and management, are demonstrating pervasive IT leadership with the SCAP methods. It is my belief that these methods will become "de facto standard" not only for Civilian Agencies and DOD, but potentially within the commercial sector.

Vendor support and momentum of the Federal SCAP initiative is growing rapidly and is already impacting commercial companies on both the supplier and end-user side. Most of the major information security companies have, or are readying, SCAP-compliant products for use by their customers.

Additionally, ISVs are adding SCAP protocol to their software measurement content, such as the Common Platform Enumeration (CPE) fields utilized by SCAP.

My personal opinion is that SCAP represents **the most significant and impactful IT standard, content delivery and best practice framework ever conceived and delivered by the government IT community.**

Again I applaud the NIST team, and broader Federal IT community, for their strong leadership role to conceive and deliver SCAP.

General Observations for the Committee:

We must begin to better focus our IT legislation targeting the specific results that we want the constituencies to deliver. I favor emphasis on the use more carrots versus bigger sticks. It is important to recognize the leadership that led to the creation of important methods such as SCAP. We must also reward the political-will of the departments and agencies that are voluntarily stepping up to implement these important new methods ahead of any regulatory requirement to adopt.

Rethinking our budgeting and regulatory processes to drive faster real results:

With FISMA, government has traditionally focused on Certification and Accreditation (C&A) and periodic compliance checks for agency IT systems and infrastructure. This has resulted in a "check list" mentality where getting a "better grade" becomes the focus. This does not necessarily yield a more secure and robust IT environment.

Additionally, literally millions of dollars and thousands of man hours are spent by government every year to fill three-ring binders that are immediately out of date and irrelevant when the C&A process has been completed. This is driving a false

sense of security and is wastes tremendous capital and consumes precious manpower without significantly improving our real cyber risk.

We MUST move to systematic and continuous monitoring solutions that address and adapt to the current realities and dynamic demands of today's cyber world.

Our risk profile now mandates that we move to a more complete "sensor" view (whitelist plus blacklist), along with the active and systematic vulnerability and configuration checking enabled by the SCAP framework. We must change our C&A and compliance mindset, to one of "We are always exposed, so we must continually monitor report and act. This is just common sense.

I urge our legislators in both the House and the Senate to observe and support the tremendous technical work being done by government in partnership with the commercial sector with the SCAP framework.

We (industry and government) are already working side-by-side on live deployments where broad near real-time continuous monitoring is the goal. We believe that these goals are immediately feasible and expect they will quickly prove dramatic improvements in our IT operational readiness.

There is significant and immediate leverage to be gained by shifting dollars allocated for FISMA-based C&A and compliance projects to **full-scope continuous monitoring using the SCAP framework.** I strongly recommend to this committee, and other committees involved in oversight and legislation for targeting improved cyber assurance and regulation, to consider these suggestions.

If we do this (with the close cooperation of the legislative branches, EOP/OMB and DOD), significant national cyber assurance progress can be realized without significant incremental budget impact.

Realigning IT budgeting and spending to our current challenges, and moving from pure C&A to SCAP-enabled Continuous Monitoring, is likely budget neutral to positive. Further, it is expected that the immediate automation advantage will **lower** the demand for qualified IT personnel and **reduce** long-term IT operational expense.

Reorganization of ITL

On this point I can be quite brief. It is curious to me that an internal reorganization, conducted by the capable and professional management staff of NIST, should draw as much attention as it has. While I am not privy to the precise catalysts of, and motivations for, the contemplated and/or actual organizational event, it seems like the benefit of any doubt should be yielded to the Acting Director and staff at NIST.

That being said, like most organizations—government or otherwise—I would expect that the intent of the reorganization was to realign the human resources with the changing mission requirements. In this case I would further expect that NIST has realized that CYBER ASSURANCE methods and best practices are increasingly a horizontal-cross agency issue, and its core-competencies should not remain in a silo within NIST.

If this is the case, I applaud NIST for adjusting to changing needs, and my only advice perhaps would be a bit more advance marketing and communication to affected NIST constituencies.

Recommendations on how ITL might improve its effectiveness or expand its scope/activities and impact in Information Assurance and Cyber Security

Having worked with NIST from several perspectives for nearly a decade, I have only the deepest appreciation for the dedicated scientists and staff at NIST. I often use the story with family and friends to explain the reach and impact of NIST in the physical world by using the following statement:

In any room, in nearly any country, in any sector of our commercial endeavor—look around that room and I can almost assure you that at least SOMETHING in the environment has been touched, driven or impacted by work done at NIST.

Now when I look from my day-job perspective—and take that same view from a cyber assurance point of view and ask "What impact has NIST had on the security, reliability, stability, and utility of the operational computing infrastructure?" . . . We still have work to do.

I encourage NIST, perhaps with even a greater sense of urgency, to continue with its core mission of standards and best practices as they relate to the broader cyber assurance goals and objective.

I further encourage NIST and its government partners in these areas including NSA, DISA, DHS and others, to embrace more "out of the box" thinking around the cyber assurance challenges that the Nation is facing.

TIME IS OF THE ESSENCE:

Mr. Richard Marshall, senior information assurance representative for the Office of Legislative Affairs at the National Security Agency (NSA) said at a public event recently, "We're polishing stones instead of creating stones," he said. "If we don't do something in the near-term, there won't be a long-term. We are running out of time." I agree.

I encourage NIST to consider the following actions:

- Continue to create and advance measurement standards and methods for Cyberspace.
  - We must do this by continuing to improve our NEGATIVE AND DEFENSIVE posture:
    - This is the Risk and Vulnerability perspective—are we effectively identifying the "Bad things and risky things" in our computer environment—and improving the common language to express and communicate these risks.
    - NIST has done some great work in these areas including the Common Vulnerability Scoring System (CVSS) and National Vulnerability Database (NVD).
    - We need to continue to emphasize these as OPERATIONAL METHODS as opposed to (only) Certification and Accreditation (C&A) and compliance methods.
  - We need to supplement these negative detection and enforcement methods with an improved POSITIVE POSTURE: This is where the prescribed "good state" perspective is captured and enforced. We need operational methods and standards that measure "the known and good state" to assure that our deployed computer environments are intact. We can also address important supply chain provenance issues with these same techniques.
    - NIST has already worked in these areas but they appear "less connected" with the some of the methods described above. Much of this work is apparent in the National Software Reference Library (NSRL) and the *Help America Vote Act* (HAVA).
    - Many of the same "positive attestation" and trust attestation controls required by HAVA can and should be applied to SCAP-enabled IT operational best practices.

In my view there are MANY parallels between the ways NIST has contributed to this in the physical world for the last 108 years. Software, software assemblies and indeed entire software "stacks" used to enable and enhance our way of life, can and should be measured and operationally attested.

I urge NIST to continue to work multilaterally with their peers in government and industry on all the methods I mentioned above, and to distill these "best of the best" ideas into NIST standards and methods on an even a faster cycle than normal.

Summary

We are a crucial time in our history on multiple fronts. While I fully acknowledge that we are a vendor of methods used to improved cyber assurance, my primary motivation to "join the team" around SCAP and other important developments has been citizen-centered.

We are in a race of dramatic proportions and potential risk, and we are behind. Our National and Economic Security are at risk and if we can improve this as a team, then we must take action now.

We must advance the state-of-the-art in Cyber Assurance in order to get to the next level of visibility, control and efficiencies. Extended SCAP methods, along with Continuous Monitoring, are our best chance of getting ahead of our adversaries, and scaling that advantage quickly and efficiently across the federal enterprise.

I respectfully submit that our technical teams have given us the tools to significantly raise our odds of closing the large cyber assurance gap we now face. It is imperative that our legislative and executive branches show the political-will, and the program and financial resources to enable us to succeed.

Thank you and I welcome any questions from the Committee.

BIOGRAPHY FOR WILLIAM WYATT STARNES

William "Wyatt" Starnes was born in Atlanta, Georgia in October 1954. Mr. Starnes had a deep and immediate interest at an early age in everything mechanical, electrical and the emerging electronics industry. He built his first photocell sensor electronic project for a science fair while in still in elementary school. He went on to graduate from Ygnacio Valley high school in Concord, California in 1972 knowing that computers and electronics would become his life's work.

After graduating, Mr. Starnes was restless and ready to go to Silicon Valley to begin his career. He took a highly focused path graduating from Control Data Institute of Technology with an Associate Art's degree in computer science, and began his professional career with Data General (DG) Corporation in Sunnyvale, California in 1973.

Mr. Starnes' insatiable curiosity about "how things work" continued in Silicon Valley involving himself in "everything semiconductor" for the first several years. This work included everything from detailed courses in semiconductor physics to software design and engineering with many of the early programming languages. His early career was centered on semiconductor automated testing and measurement. Mr. Starnes not only helped design the first semiconductor memory and microprocessor devices for DG, he wrote or co-wrote all of the test programs used to verify the functionality of these complex chips.

Data General was the first of many successive entrepreneurial experiences for Mr. Starnes. He went on from DG to Monolithic Memories and helped to build the first MOS and CMOS processes and devices, including the 1k and 4k MOS dynamic RAM's. While still focused on programming of Automatic Test Equipment (ATE), he went on to Maruman Integrated Circuits, creating one of the first "Fab-less Semiconductor" resources in Silicon Valley. Maruman produced (and Mr. Starnes wrote the test programs for) much of the Atari game devices in late 1970's.

After having made significant technical contributions in the ATE industry, in 1978 Mr. Starnes took an early stage management position with MegaTest Corporation. Megatest revolutionized ATE by inventing and delivering the most cost-effective test and measurement equipment ever delivered. This contribution was viewed as critical to Intel Corporation, AMD, National Semiconductor and many others, for testing complex integrated circuits at a fraction of the cost of previous solutions. Interestingly this breakthrough had to do with "reference testing," which would become a model for additional breakthroughs in software assurance methodologies.

Mr. Starnes moved to Tokyo Japan in 1981 for two years to found MegaTest Japan. This provided much needed international market perspective to Mr. Starnes resume, and he continues to be very active in the Asian market.

After a 20-year career in semiconductor manufacturing and testing, Mr. Starnes made the shift to software in 1993. Having moved from Silicon Valley to Portland, Oregon in 1989—Mr. Starnes began a new chapter of his career with Infinite Pictures (now iMove). This company did pioneering work in 3-dimensional visualization software and hardware. iMove is now one of the leading producers of fixed and mobile surveillance devices for industry and government.

While Mr. Starnes has always maintained his deep technical roots, he has continued to expand his management, sales and marketing expertise. He has been deeply involved at the senior management level of every company he has worked in since 1973. This has allowed him to remain both technically adept at the "street level," while maintaining senior executive relationships across many enterprise and government sectors.

While at Infinite Pictures Starnes met Gene Kim, with whom he went on to found Tripwire, Inc. with in 1997. The Tripwire software was developed by Gene Kim under the close guidance of Purdue University professor Eugene Spafford (aka Spaf) beginning in 1991.

While CEO of Tripwire Mr. Starnes grew the company rapidly and was awarded *Inc. Magazine*'s 20th Fastest growing company in America award in 2002. More importantly, the Tripwire technology and products began to alter the state-of-the-art in information security and assurance by bringing the notion of integrity management to the market.

Due to a medical issue (early stage cancer) in the summer of 2003, Mr. Starnes left Tripwire to seek a cure with his family and doctors support. Quickly recovering after successful treatment, he returned to the software assurance and cyber security industry in spring 2004 with the formation of SignaCert, Inc.

It was in this timeframe that Mr. Starnes was invited by the Acting Director of NIST to serve on the Visiting Committee on Advanced Technology, or VCAT, which he served in that capacity from 2005 to 2008. Mr. Starnes also presided as the first

Chairman of the IT Subcommittee under the NIST–VCAT Oversight Committee in 2007 and 2008.

While at SignaCert, Mr. Starnes and his team have continued to drive the "think differently" vision in dealing with complex information security, compliance and information assurance. The fundamental breakthrough, covered now by two U.S. Patents, is that software can and should be "measured." This led to the long-term development of Global Software Trust Services based on the measurement of software that is built by the Independent Software Vendors, or ISVs.

In a way similar to the ATE methods now commonly used by companies such as Intel to test and verify semiconductor devices (as developed by MegaTest), SignaCert builds "reference views" of software, using software measurements, or "whitelists" to assure that IT devices (servers, workstations, routers, mobile devices, etc.) are in alignment to the prescribed reference measurement set, or "gold image."

This information assurance method, is complimentary and additive to traditional perimeter-centric, reactive and defensive IT methods (such as firewalls, intrusion detection, and anti-virus) by ensuring the established, known and presumed trusted, IT state is maintained over the deployment and usage life cycle of that IT device.

Knowing that the "as-deployed state" is accurate to a control reference has been shown to contribute immediate benefits for all market sectors and customers that depend on complex IT to deliver critical business and mission services.

In addition to improving cyber security against both inside and outside risk and adversaries, the method has been shown to dramatically increase mean-time-between-failure (MTBF) and reduce mean-time-to-repair (MTTR), which serve to increase IT business process stability and availability, while reducing the requirement for trained people to manage complex and broadly scaled IT infrastructure.

Mr. Starnes continues to passionately pursue his primary career mission of improving cyber assurance by providing greater efficacy and more transparency. Critical to this mission is lowering both costs and resource requirements through enabling automation across all critical enterprise sectors and geographies.

Chairman WU. Professor Schneider, please proceed.

STATEMENT OF DR. FRED B. SCHNEIDER, SAMUEL B. ECKERT PROFESSOR OF COMPUTER SCIENCE, CORNELL UNIVERSITY

Dr. SCHNEIDER. Thank you, Mr. Chairman. NIST's Computer Security Division serves today as a trusted source of expert information about secure computing. The recent proposal to reorganize the division in my opinion threatened its effectiveness and thus could have undermined a key national resource for civilian cybersecurity. Therefore, my remarks here will focus on CSD organization, but I will be prepared to answer other questions later.

What had been proposed involved two elements. The first element had the head of CSD reporting higher up in NIST's management chain. This would have been good. Higher levels of NIST's management increasingly will want to understand and champion computer security activities so they can secure needed resources and can provide guidance throughout the Federal Government.

The other element of the reorganization involved redefining which projects are part of CSD. CSD would no longer be the home for all cybersecurity activities within the information technology lab. I have not heard a compelling rationale for this, and I am not sure one exists.

First, I fear that having computer security activities outside of CSD would erode the CSD brand. This brand is a valuable asset. It keeps CSD visible to its customers so they know where to come for help, and it enables CSD to attract talent because CSD employees are seen to have an impact on computer security, both domestically and internationally. Second, I am concerned about loss of budget accountability for computer security activities. Put all the activities in a single division and it will be easy to ascertain that

funds appropriated to NIST for cybersecurity are used as intended. Disburse cybersecurity activities over multiple divisions and the funds will be intermixed with funding for other activities.

Finally and perhaps most important, I see no intellectual basis for deciding what computer security activities to place outside of CSD and what other activities to place inside of CSD. However, I do see difficulties when people who are working on closely connected initiatives are not under the same management. It removes imperatives for cooperation, for rational budgeting, and makes comparisons of people and projects difficult. So the proposed reorganization seemed to offer few benefits.

But a slightly different reorganization actually could have been a very wise move. Looking ahead, CSD will have to assume a larger role because trustworthy computing is so central to the future of our nation's critical infrastructures, private sector systems, and the Administration's new initiatives in healthcare and SmartGrid. Growth will be necessary to meet these needs. Although the recent reorganization proposal makes no allowance for such growth, there is a plan that does. Elevate CSD to become a laboratory in NIST so that it is parallel to the information technology lab currently housing CSD. With this alternative proposal, the director of the new lab would report higher up the NIST management chain, the CSD brand would be protected and perhaps even strengthened. Budget control and accountability are facilitated by having all and only computer security activities under one director, and there would be no need to separate various efforts that intellectually are closely related.

In sum, I find that entertaining a reorganization of today's CSD is sensible, but the recently proposed reorganization lacks a rationale and seems to create problems without offsetting benefits. An alternative reorganization that elevates CSD to form a new computer security lab at NIST has much to recommend it. Thank you.

[The prepared statement of Dr. Schneider follows:]

PREPARED STATEMENT OF FRED B. SCHNEIDER

Mr. Chairman and Members of the Committee, I appreciate this opportunity to comment on the role, activities, and proposed organizational changes within the Computer Security Division at the Information Technology Laboratory of NIST. I am Fred B. Schneider, a Computer Science professor at Cornell University and Chief Scientist of the NSF-funded TRUST[1] Science and Technology Center, a collaboration involving researchers at U.C.–Berkeley, Carnegie-Mellon University, Cornell University, Stanford University, and Vanderbilt University.

I have been a Computer Science faculty member since 1978, actively involved in research, education, and in various advisory capacities for both the private and public sectors. Besides my work at Cornell, I today serve as member of the Computing Research Association's Board of Directors and as a council member of the Computing Community Consortium. I also co-chair Microsoft's TCAAB external advisory board on trustworthy computing. And perhaps most relevant to today's hearing, I have served since Sept. 2006 on the Information Security and Privacy Advisory Board (ISPAB), a Congressionally mandated FACA board that advises NIST, the Congress, and OMB about cybersecurity in Federal and civilian computer systems. The comments that follow are my own opinions, however.

Our nation's needs for secure systems will surely grow over the next decade. The networked computing systems employed today to operate critical infrastructures (e.g., energy distribution, banking, finance, transportation, and communication) are vulnerable to attack. Systems running our civilian government offices and private sector business are also vulnerable. And we, as a nation, are now discussing a

[1] Team for Research in Ubiquitous Secure Technology.

"smart grid" for energy distribution and a new health care system that will depend critically on computing systems that must be trustworthy. Activities performed by Computer Security Division (CSD) are critical to the success of all.

CSD plays a special and important role for the Federal Government and the private sector, by serving as a respected source of objective information about ways to build and operate secure computing systems. This role is possible only because

- CSD is able to attract top talent,
- CSD is situated within an institution-NIST-where research is valued and is being conducted (even though only some CSD activities are, in fact, research), and
- CSD can be trusted as an advocate of security, by virtue of not being part of a law enforcement or national security organization, since there is then no basis for concern about CSD developing standards with a hidden purpose of collecting information.

Question: *The Cyber Space Policy Review makes a number of recommendations to improve federal efforts for cybersecurity. Examples of these recommendations include the establishment of a single federal entity to act as a locus for U.S. involvement in international standards, increased public education and awareness, and a larger focus on identity management. What could NIST do to address these and other recommendations from the Cyber Space Policy Review?*

NIST—and within NIST, CSD—indeed serves as a locus for U.S. involvement in international standards, increased public education and awareness related to cybersecurity, and a larger focus on identity management. Despite a modest budget, CSD has succeeded admirably in these tasks; I urge that it be supported to continue and expand these activities.

There is also much other work to be done in support of civilian system cybersecurity, especially with the crying need to revise FISMA and with the Administration's initiatives to create the expertise and standards for smart grid and health care. NIST is the right place to do this work and should aggressively embrace these challenges by increasing the size and funding for CSD.

Moreover, as noted above, CSD is ideally situated to provide cybersecurity information that its customers can trust. Other federal agencies (e.g., DHS, NSA, FBS, CIA, DOD) also have important roles to play in the cybersecurity landscape, but each has a mission that can only engender suspicion by a private sector wary of government surveillance. So these other federal agencies could neither replace nor host CSD activities.

Question: *NIST is proposing a reorganization of ITL. What is your assessment of this reorganization and how will it improve the outcomes of ITL activities?*

Plans for the reorganization of NIST's Information Technology Laboratory (ITL) and CSD first came to my attention about four months ago, in July. All of the details have still not been made public, but there was a public discussion of some aspects of a proposed CSD reorganization about two weeks ago (at the Oct. 7, 2009 ISPAB meeting).

The key parts of the reorganization described to me have two elements:

- The Office of the Associate Director for Cybersecurity Research and Development reports higher-up in the ITL management structure.
- The set of projects under CSD is changed slightly, with a few projects whose names suggest they concern cybersecurity being moved outside of CSD while other projects whose names suggest they have a significant content that does not concern cybersecurity being moved into a new CSD with a new name.

Note, the two elements are largely independent.

The first element, having CSD report-in higher-up the management chain, seems wise and even prescient, given the growing need for services that CSD now provides or will need to be providing in the near future. Higher-levels of NIST's management will have to understand and champion the activities of CSD, to ensure sufficient resources are available to support cybersecurity efforts and to provide guidance to other federal and civilian decision-makers in a world where cybersecurity matters are growing pervasive. Notice, also, that this first element of the proposed reorganization directly impacts a small number of people but offers enormous leverage.

The second element of the proposed reorganization affects a much larger number of people—all those involved in CSD projects plus some others within ITL. Any reorganization that potentially affects many people tends to be disruptive (and this one already seems to have had a significant impact on the esprit de corps within CSD), so such change is best contemplated and undertaken only when there are significant

gains to be had. In evaluating any proposed reorganization of CSD, I think that we should want to know:

- To what extent does the proposed reorganization leverage investments and personnel? For example, what is the overhead for management and for communication within the proposed reorganization, as compared with the current organization?
- To what extent does the proposed reorganization facilitate or impede inefficiencies, collaborations, synergies, and informed trade-offs by virtue of shared management. For example, how would changing which projects share mangers benefit or harm each effort as it competes for budget, other resources, ratings, promotions, etc.
- Does the proposed reorganization change the visibility of CSD activities to NIST management (which must make budget trade-offs and advocate for CSD outside of NIST) or to CSD customers (Federal Government civilian agencies and the private sector).
- Does the proposed reorganization facilitate better accountability for budget appropriations intended to enhance activities in computer security?
- Does the proposed reorganization better position NIST to support expected future needs (such as changes to FISMA to require continuous monitoring of systems and improved security metrics, the Administration's new smart grid and health care initiatives, and our nation's ever-increasing dependence on networked systems both within the government and private sectors)?

Yet I am aware of no analysis that answers the above questions. I myself am not familiar enough with the details of ITL and CSD to attempt such an analysis. But I can offer some general guidelines for designing a good CSD organizational structure.

The CSD brand is a valuable asset. It serves as a clear and obvious point of engagement for customers. That both (i) increases the efficiency of interactions between CSD and customers and (ii) increases the chances that those in need will know to seek CSD expertise and to embrace CSD standards and other guidance.

The CSD brand also means that

(1) CSD accomplishments,

(2) the unique role and impact CSD has on the computer security landscape internationally (through encryption standards) as well as domestically (through other standards and guidance, too), and

(3) the problems CSD addresses

together make CSD an exciting place to work. This, in turn, has enabled CSD to recruit an outstanding staff, despite the scarcity of computer security experts and despite competition for their services (with considerably better compensation) from the private sector. A CSD reorganization that erodes the CSD brand by eliminating the name or by diffusing the organization's efforts into a larger pool of computer science activities should therefore not be undertaken lightly.

In addition, mixing computer security activities and other computer science efforts complicates accountability of computer security budget appropriations. Creating decreased management visibility into how budget is divided seems unwise, as we enter an era where Congress will doubtless be providing increased budgets to NIST in order to serve the ever growing computer security needs of our nation.

Finally, I see no benefits from dividing cybersecurity activities, locating some in an organization that is mostly populated by cybersecurity experts but others in an organization that is not.

- I can see no intellectual basis that could be used to decide today on such a partitioning of cybersecurity projects, much less to decide on a partitioning that is likely to remain sensible for a future where our understanding of cybersecurity will almost certainly have evolved. To give an extreme case, there once was a time when it made sense for those studying privacy and other policy matters to be organizationally separated from technologists. That separation is no longer sensible, however—technologies are typically useless when developed by people ignorant of policy, and policy developed by people who don't understand technology is often damaging to innovation and growth. So CSD ought to include both, yet the proposed new reorganization seems to be considerably narrower and includes only a subset of the technologists.
- There is also a matter of styles. Some members of CSD engage in research, and some engage in activities that have a very different character-writing standards, compiling best practices, etc. The rest of ITL is primarily con-

cerned with research. If all computer security activities were located in CSD, then this difference would be accommodated by the organizational structure. In contrast, diffusing the one kind of activity within the other will likely lead to an organization that is difficult to manage and has various different classes of citizens.

From my analysis and the guidelines I proposed above, I conclude that NIST management would be wiser to be contemplating a new laboratory—CSL (instead of CSD)—in parallel to ITL, instead of making changes to the organization of ITL. Choosing which specific projects to place in CSD, as advocated by the second element of the proposed reorganization, simply offers no leverage but has the potential to create problems. A new CSL structure, however, would satisfy all of the requirements I noted above: (i) the director would report higher-up in the NIST management chain, (ii) CSD function would be even more visible and have a stronger identity, (iii) budget control and accountability is facilitated, and (iv) there is no need to separate projects that are closely related.

Question: *Given the current emphasis on information assurance and cybersecurity, what recommendations do you have on how ITL might improve its effectiveness or expand the scope of its activities and their impact?*

Looking to the future, the functions performed today within CSD will play a bigger and bigger role in how the Federal Government and the private sector protect their computer systems. Smart grid and computerized support for health care, for example, raise new computer security questions. The current discussion about "accountability of action" for enforcing security on our networks raises numerous issues involving both technology (e.g., how to attribute packets in transit) and policy (e.g., how to manage trade-offs with privacy)—topics that fall squarely in the expertise of CSD. And no matter what happens with a U.S. universal identity card, questions about federated identity still need to be sorted out as various public sector and private sector organizations create identity management systems on the Internet.

In short, the need is there today for a CSD that is much larger than its current size; and the needed work cannot be done in the private sector, because of inherent conflicts of interest and commitment. I conclude that CSD will have to grow in size significantly over the next five to ten years.

But CSD growth raises another issue about the recently proposed efforts to reorganize ITL and CSD. The proposed reorganization does not group all cybersecurity efforts together in a single CSD presumably because that division would be too large. So yet another reorganization would be required to accommodate significant growth in CSD activities. If, instead, a CSL is created today, then we would be putting in place an organization that not only satisfies its requirements for today but would continue to meet its requirements for a long time to come. And that strikes me as by far the more sensible course.

BIOGRAPHY FOR FRED B. SCHNEIDER

Fred B. Schneider is Samuel B. Eckert Professor of Computer Science at Cornell University. He joined the Cornell faculty in Fall 1978, having completing a Ph.D. at Stony Brook University, preceded by a B.S. in Engineering from Cornell in 1975. Schneider currently also serves as the Chief Scientist for the NSF-funded TRUST Science and Technology Center, which brings together researchers at U.C.–Berkeley, Carnegie-Mellon University, Cornell University, Stanford University, and Vanderbilt University.

Schneider's research has focused on various aspects of trustworthy systems—systems that perform as expected, despite failures and attacks. His early work concerned formal methods to aid in the design and implementation of concurrent and distributed systems that satisfy their specifications; he is author of two texts on that subject: *On Concurrent Programming* and *A Logical Approach to Discrete Mathematics* (co-authored with D. Gries). He is also known for his research in theory and algorithms for building fault-tolerant distributed systems. For example, his paper on the "state machine approach" for managing replication received an SOSP "Hall of Fame" award for seminal research. More recently, his interests have turned to system security. His work characterizing what policies can be enforced with various classes of defenses is widely cited, and it is seen as advancing the nascent science base for security. He is also engaged in research concerning legal and economic measures for improving system trustworthiness.

Schneider was elected Fellow of the American Association for the Advancement of Science in 1992, the Association of Computing Machinery in 1995, and the Institute of Electrical and Electronics Engineers in 2008. He was named Professor-at-

Large at the University of Tromso (Norway) in 1996, and was awarded a Doctor of Science *honoris causa* by the University of NewCastle-upon-Tyne in 2003 for his work in computer dependability and security.

Schneider has served since Sept. 2006 as a member of the Information Security and Privacy Advisory Board (ISPAB), which advises NIST, the Secretary of Commerce, and the Director of OMB on information security and privacy issues pertaining to Federal Government Information Systems. He chaired the National Academies CSTB study on information systems trustworthiness that produced the 1999 volume *Trust in Cyberspace*. He also served as a member of CSTB from 2002–2008 and served from 2004–2007 on the CSTB study committee for improving cybersecurity research. Schneider was a member of the NSF CISE advisory committee 2002–2006. And in Fall 2001, he chaired the United Kingdom's pentennial external review of research funding for academic Computer Science.

In 2007, Schneider was elected to the Board of Directors of the Computing Research Association (CRA) and appointed to the steering committee of CRA's Computing Community Consortium. CRA is an association of more than 200 North American academic departments of computer science, computer engineering, and related fields; part of it's mission is to strength research and advanced education in the computing fields and to improve public and policy-maker understanding of the importance of computing and computing research in our society.

Schneider is a frequent consultant to industry, believing this to be an efficient means of implementing technology transfer as well as learning about the real problems. He is Co-Chair of Microsoft's Trustworthy Computing Academic Advisory Board, which comprises outside technology and policy experts who meet periodically to advise Microsoft about products and strategy. He also provides technical expertise in fault-tolerance and computer security to a variety of firms, including: BAE Systems, Fortify Software, Lockheed Martin, and Microsoft.

Chairman WU. Thank you very much, Dr. Schneider. And Mr. Bohannon, please proceed.

STATEMENT OF MR. MARK BOHANNON, GENERAL COUNSEL AND SENIOR VICE PRESIDENT FOR PUBLIC POLICY, SOFTWARE & INFORMATION INDUSTRY ASSOCIATION (SIIA)

Mr. BOHANNON. Thank you, Mr. Chairman, Ranking Member Smith, Congresswoman Edwards. It is a pleasure to be here today on behalf of the more than 500 members of SIIA, the principal association of software companies, to discuss with you NIST's cybersecurity activities in the context of the 60-Day Review.

As has already been indicated by the panel, that review was quite comprehensive in its outlook. Even by its own statement, it touched virtually everyone and everything we do in our society, and I think I certainly share with my colleagues the anticipation that the cyber coordinator will be announced soon.

But I think you can boil down the thrust of that review into three things. First, that we have got to take action to enhance the security of our Federal Government systems; second, that we need to continue to enhance the public/private partnership to make sure our infrastructure is secure; and third, that we need to partner effectively with the international community since this is a global problem, not just a U.S. problem.

And in our view, the challenges, these three challenges, mean that NIST and thereby the Secretary and Department of Commerce have an absolutely essential and critical mission and contribution to make to seeing where the 60-Day Review goes.

To be more precise—and I welcome Ms. Furlani's update on what is going on with the ITL. I have known her for many years and look forward to working with her on where this could possibly go once they have stepped back from this program. The reality is that this change in NIST review comes at a very critical time about the

direction I think we are going to take with the cybersecurity review, and one of the key questions is whether its implementation is going to be informed predominantly by the military intelligence framework on cybersecurity or whether it is going to be able to adapt across a wide-variety of sectors and parts of our economy.

Our view, based on the experience so far, is that you have got to have that blend of perspectives for it to work, and if it is going to be effective, it means that NIST must be enhanced and reinvigorated in its role, and thereby the Department and the Secretary must play a leadership role in where the 60-Day Review is going to be carried out.

So therefore, we think rather than looking at what are the merits or non-merits of the ITL reorganization, this is a great time to look at really where the future of NIST and its cybersecurity activities need to go.

Mr. Chairman, in our testimony we make a number of recommendations and ask some key questions which I assume have been submitted for the record. Let me try to summarize those here.

First, we urge the Committee as it has done for decades to make sure that NIST does not become a regulator of private-sector actions. You all have been very consistent in making sure that NIST remains a first-class laboratory, not a fifth-class regulator. NIST does best and carries out its mission when it collaborates with the private sector, not try to impose government-defined standards or technologies on the private sector, and my testimony goes through some examples where they have come very close to that line without a great deal of success, and in my view some negative consequences.

The second thing we would urge, and is consistent with some of the other panelists, is that we would urge serious consideration to making the Computer Security Division a stand-alone laboratory. We have heard three key challenges facing the Computer Security Division. One is funding, one is staffing and recruiting and retaining good staff, and the third is enhancing and reinvigorating the global brand. We think that currently the CSD, being one of six divisions inside of ITL, and ITL being one of ten laboratories inside of NIST, is not really the right framework in which that can occur. And so again, we know that there are issues involved in doing any reorganization, but we think that there needs to be serious consideration given to this. Creating a cyber information security, information assurance lab, I don't want to get hung up on the name. We think it would send a very important signal to the private sector and to the world that the United States Government is taking its role very seriously in this regard.

The third recommendation we would make is that NIST needs to make sure that its primary customers, agencies of the Federal Government, are the focus of its efforts, and the committee is well-aware of its responsibilities in that regard.

The fourth recommendation we would make is that NIST needs to continue to work with the private sector and the political leadership of the Commerce and USTR (United States Trade Representatives) among others as we work to roll back some of the ridiculously stringent regimes that we are seeing from other govern-

ments which are trying to impose indigenous or unique standards in this area.

I was not able to appear in the June hearing, Mr. Chairman, because I was in China personally working to try to roll those back, and while we certainly depended on the leadership of Ambassador Kirk and Secretary Locke in getting that done, NIST was an absolutely essential partner because of its perceived global reputation as an independent assessor, independent evaluator, credible place where we could talk about legitimate ways of approaching these issues globally. That is going to become more important as we see countries like India and Russia also beginning to take on those efforts.

So with that, Mr. Chairman, I just want to say that we think that NIST and the Department of Commerce have an absolutely essential role. We are very pleased to see that Secretary Locke in particular has brought some terrific people in who are really beginning to focus on these issues. We commend those steps. We commend this hearing, and we look forward to working with you and the executive branch to carry out these goals. Thank you.

[The prepared statement of Mr. Bohannon follows:]

PREPARED STATEMENT OF MARK BOHANNON

Chairman Wu, Ranking Member Smith, Members of the Committee, on behalf of the more than 500 members of the Software & Information Industry Association (SIIA), the principal association of the software and digital content industry, we appreciate the opportunity to discuss the current cyber and information security activities of the National Institute of Standards and Technology (NIST) and how they fit into the action plan of the Cyber Space Policy Review (60-Day Review). As the Committee is aware, I also served as an official at the Department of Commerce during the 1990's working with NIST on computer security issues.

The 60-Day Cyber Space Review was an extraordinarily comprehensive document, recognizing that "cyberspace touches practically everything and everyone."[1] We are not alone in awaiting the appointment of a White House coordinator to undertake the many and varied 'next steps' that the Review identified.

Among the central thrusts of the Review is that action must be taken, first, to enhance the security of the Federal Government's systems; second, to continue and enhance the public private-partnership that is essential to securing our nation's infrastructure; and, third, to partner effectively with the international community.

In each of these vital challenges, NIST—and thereby the Secretary and Department of Commerce—has an essential and critical mission and contribution to make.

We read news reports of a possible reorganization of NIST's computer security areas of competence. I must emphasize that I am relying entirely on published reports on this matter. However, we are concerned about these reports regarding the future of NIST's Computer Security Division (CSD).

If this proposed reorganization would separate—some would say bifurcate, some would say disperse—the activities of NIST's basic research functions from those of its applied-external activities (which include its evaluation processes and engagement internationally), this would be in our view a serious detriment to the ability of NIST and the Department to step up to the plate if and when the Cyberspace Review is undertaken systematically.

This potential change in NIST computer security functions is taking place as the 60-day Review—and the direction it will take—remains a work in progress. One key question is whether its implementation will be informed predominantly by a defense-intelligence framework and the related assumptions about cybersecurity. If the follow-on to the 60-day Review is going to be meaningful across a variety of commercial sectors and viable economically, there must be strong leadership from the Department of Commerce—and that cannot occur without an effective and enhanced role of NIST.

It is also occurring as we face mounting global challenges, which include efforts by other governments to undertake stringent cybersecurity regimes outside of global

[1] Preface, Cyberspace Policy Review, p. i.

norms. There are also important efforts underway to focus on the next generation of international frameworks for assuring cross-border analyses of vulnerabilities and bases for product evaluation.

Therefore, it is an opportune time to look at how to make sure NIST—and the Department—are prepared and ready to engage the interagency process, the public and our international partners with a view to the future.

In Appendix A, we outline a number of questions that we believe are timely and essential to NIST's role in cyber and information security, and very relevant to the 60-day Review objectives. Let me summarize them here.

First, we urge the Committee, as it has consistently done by decades, not to make NIST a "regulator" of private sector actions. NIST has effectuated its mission best through long-standing collaboration with the private sector. This collaboration, which is not replicated to the same degree by any other agency of the Federal Government, has benefited not only government agencies (which are the first line customers of NIST's work), but also our nation's infrastructure, innovation environment and competitive strength.

When NIST has ventured away from this mission and collaborative approach, the result has been injurious. For example, in undertaking Federal Information Processing Standards for federal agencies, NIST has recognized (including making mandatory) controversial cryptographic implementations like Clipper Chip and Skipjack (which are still identified for government use). The controversies around these approaches are enormous.[2] NIST is not equipped to become a regulatory body which proscribes specific standards for the private sector, nor would it be desirable to make it such, as it would inherently distract from its core competencies and mission. Instead, it is critical to look ahead to the next generation of challenges, which require NIST to remain the globally recognized forum for reaching consensus on key issues (as it did with the highly successful competition to identify the Advanced Encryption Standard), and reinvigorating its recognition as a world-class laboratory.

Second, we would strongly urge consideration to making the Computer Security Division a separate lab within NIST should be a priority. The CSD is one of currently six Divisions within the Information Technology Laboratory (ITL), which is itself one of 10 laboratories within the NIST organization. This action—creation of a stand alone Cyber and Information Security Lab—would send an important signal, both to Government agencies and to the private sector, and enhance the NIST 'brand' in this important area. As a Division within one of 10 competing Labs at NIST, the Division is, for example, handicapped in its recruiting and retention of quality employees. For example, the Division Chiefs are *not* Senior Executive Service (SES) position.

To state the obvious, this recommendation is in direct contrast to any suggestion of dispersing or bifurcating the computer security functions of NIST, which would present serious risks to the funding and global branding of NIST in cybersecurity work. It would also compound the problems that NIST has been facing in recent years.

On the one hand, NIST—specifically the Computer Security Division—has been handed in recent years a number of legislative mandates, including some that have not been funded.[3] This compounds the on-going funding paradigm of the Division (which is shared by other NIST Labs) that requires it, except in rare years, to get up to 40 percent of its funding from other agencies (or engage in cost-reimbursement work through CRADAs), since appropriation funds may account for as little as half of the year's program.

On the other, the work of the Division on broad-based research, including those initiatives that benefit both the public and private sectors, is increasingly under pressure due to the demands of other agencies, including the Office of Management and Budget (OMB), for assistance to other Federal agencies in computer security. These demands are compounded by the growing mandatory imposition of NIST work—whether in the form of FIPS or guidance—on government agencies (a consequence of OMB implementing the requirements of FISMA, and no longer allowing "waivers").

These conflicting pressures—as well as the challenge of keeping quality staff—have impacted a number of key areas of work that NIST collaborates on with the private sector, particular improvements in conformity assessment.

---

[2] See "The Clipper Chip" (*http://www.epic.org/crypto/clipper*).

[3] See, e.g., *Cybersecurity R&D Act* (2002).

Third, make sure that NIST's primary customers—agencies of the Federal Government—are the focus of its efforts through effective implementation of NIST's mandated responsibilities which include:

- Raising awareness of IT risks, vulnerabilities and protection requirements, particularly for new and emerging technologies;
- Researching, studying, and advising agencies of IT vulnerabilities and devising techniques for the cost-effective security and privacy of sensitive federal systems;
- Developing standards, metrics, tests and validation programs:
  - to promote, measure, and validate security in systems and services
  - to educate consumers and
  - to establish minimum security requirements for federal systems
- Developing guidance to increase secure IT planning, implementation, management and operation.

Fourth, work with the private sector and the leadership of the Department of Commerce and other agencies of the Federal Government in taking on the global challenge of other governments' stringent cybersecurity regimes. We were very pleased to see the recognition in the 60-day Review that it will be essential to partner effectively with the international community. We are seeing efforts in several countries—China, Russia, India, just to name a few—to impose stringent, potentially trade-restrictive frameworks that require mandatory evaluation of U.S. IT products against locally developed, indigenous information security standards. This is not only bad security practice; it is potentially adverse to our nation's technology base and economic security.

As we have worked to roll back these regimes, the U.S. Government has been a critical partner. NIST, in particular, has played an essential role based on its status as a world class laboratory that is respected for its independent assessments and solid work. There is no other entity like NIST anywhere in the world. When we engage other governments, the officials sitting on the other side are almost entirely from their defense, intelligence and national security operations.

In closing, Mr. Chairman, I reiterate the need for an engaged and prepared Department of Commerce in taking up the challenge of our nation's cybersecurity strategy, and playing a key role in the direction of the 60-day Review. NIST is essential to that role, and the recommendations and questions we have posed here chart what we believe is a path for a renewed and reinvigorated cyber and information security function of NIST. We also note that, in the few short months since Secretary Locke has taken over the leadership of the Department, we are seeing a more focused and engaged team at the top levels of the Department. This is a very positive development which we commend and look forward to working with.

Again, thank you for the opportunity to appear today. I will be glad to take any questions from the Committee.

APPENDIX A

- In the context of NIST's overall mission and its existing paradigm for research, what is the most effective way to ensure that the CSD is able to carry out its mission and work collaboratively with the private sector to achieve its goals?
- What is the process for developing a strategic plan for CSD to carry out its mission?
- Is the current budgetary process for CSD—which relies on appropriate monies, but also requires each group within CSD to contract for specific monies with particular agencies—consistent with CSD's mission and consistent execution of long-term programs?
- In a highly competitive environment for skilled talent in this area, how is NIST supporting the CSD in this regard and what can be done to both attract and keep these individuals to the CSD?
- The *Cybersecurity Research & Development Act* included a number of "grand challenges." How has NIST/CSD responded and what can be done to enhance the capacity of the agency to carry out these challenges?
- What has been the experience with the National Infrastructure Assurance Program (NIAP) and should NIST continue to have a key role in its implementation?

- With the Common Criteria now a broadly accepted basis for conformity assessment, how is the CSD looking to ensure its continued effectiveness and relevance to the dynamic challenges of combating information security?
- How is NIST preparing to support, working with the private sector, the development of the next generation of Common Criteria arrangements, including improvements in the development of protection profiles?
- Has the Special 800 series been effective in providing guidance, and how can the process be updated and improved? How is NIST working to avoid inappropriate use of the Special 800 series which are now being used as legal standards imposed on private sector companies when they were never designed to be used in that way?
- With the adoption of data encryption playing a larger role in data security, is NIST's FIPS 140–2 validation program effective at ensuring timely and effective evaluations? Does the program encourage use of validation?
- There are several efforts to redefine what are "national security" and "non-national security systems." How does this discussion affect NIST's role and what are can be done to avoid unnecessary duplication and complexity?
- How can the work of the CSD in implementing FISMA be highlighted and reinforced and how can its role be made more effective?

BIOGRAPHY FOR MARK BOHANNON

Mark Bohannon is the General Counsel and Senior Vice President Public Policy for the Software & Information Industry Association (SIIA).

As the principal trade association of the software code and information content industry, the more than 500 members of the Software & Information Industry Association (SIIA) develop and market software and electronic content for business, education, consumers and the Internet. SIIA's members are software companies, e-businesses, and information service companies, as well as many electronic commerce companies. Its membership consists of some of the largest and oldest technology enterprises in the world as well as many smaller and newer companies.

Mr. Bohannon is responsible for the legal and public policy agenda of SIIA. Mr. Bohannon's experience includes engagement with hundreds of companies developing online services for the business, consumer and government markets.

Prior to joining SIIA, Mr. Bohannon was a senior official of the U.S. Department of Commerce where he served as Chief Counsel for Technology and Counselor to the Under Secretary for Technology. During his tenure, his responsibilities included a number of technology policy initiatives, fighting against technical barriers to trade, and promoting effective e-Commerce, intellectual property and Internet policies. Mr. Bohannon also served on numerous USG delegations to bilateral talks and negotiations with major trading partners and multilateral fora such as the Hague, OECD, UNCITRAL and WTO.

A native of Austin, Texas, Mr. Bohannon is a graduate of the Edmund A. Walsh School of Foreign Service at Georgetown University and of the George Washington University Law School in Washington, D.C.

DISCUSSION

Chairman WU. Thank you very much, Mr. Bohannon, and now it is in order for the panel to ask questions, and the Chair recognizes himself for five minutes. I hope to be able to address both the international cooperation issues and also the reorganization issues in five minutes, but it may stretch out a little bit.

Mr. Bohannon, you cited the Chinese incidents, and I would like to expand on that a little bit, and also I would like to ask the rest of the panel about the appropriate role that you see for NIST playing in development of international standards, what has gone well and what can be improved going forward. Mr. Bohannon, would you care to go first?

Mr. BOHANNON. Sure. The developments in China are complex. Let me try to summarize them the best I can.

Starting several years ago, China began to develop a series of standards for evaluating IT products in a wide range of areas. Not surprisingly they include areas in which the U.S. IT industry is dominant or has very superior products to the rest of the world. Those standards are based in large part on indigenous standards that were developed by indigenous standards organizations without really input from anyone outside of China, to be honest with you. They would require evaluation of products through laboratories that are at best loosely associated with the Chinese government.

These kinds of evaluations are very sensitive. NIST has handled these issues very carefully and has a long-time history of working in this area. Those Chinese standards would have prevented market access for many IT products. Working with the Secretary of Commerce and USTR, we have been able to roll them back. They are still quite broad in scope, however, and we are looking forward to continuing to work with the United States Government.

But the implications were that China would develop very indigenous, very unique standards for security in products that are widely used and that would be detrimental not only to the security of China in terms of its practices but also our technology base and our innovation base.

Chairman WU. Mr. Bohannon, I think we are familiar with the scope of the problem, but if there are any further comments you want to make about NIST's role and why that was important.

Mr. BOHANNON. Sure. NIST's role—they were very important because the Chinese see NIST as a truly world-class laboratory from which NIST can provide an independent view about things. Its role in developing advanced encryption standard is well known, but that is only the tip of the iceberg. It is not only China but other governments see NIST as a place where it can go for unbiased, professional independent assessments of what are good security practices and how they can be implemented in a meaningful way.

And so we were very pleased when the NIST team were willing to have late-night videoconferences with their counterparts explaining to them why the United States Government doesn't do things like ask for source code or why other governments don't ask for source code. That was a very important message. It was a different message than could come from the trade route with the Secretary of Commerce. It came from the best in world-class experts in this area to explain why that is not good security practice based on global norms. And those are making a big difference.

Chairman WU. Thank you very much, Mr. Bohannon. Would any of the other witnesses like to comment on what has been occurring well or not well and what could be improved going forward on international standard setting?

Dr. LANDAU. I would just like to say, and this is an old example but it contrasts with a previous failed example or an example that was not so successful. The advanced encryption standard was done extremely openly, extremely transparently. Not only were the submissions open but in fact, the comments on the proposed specifications were given out, that is, the proposed specs were put out and NIST asked for comments, and then the proposed specs were changed in accordance with comments it received internationally. The result was a very open competition, and when the standard

was chosen, and it was a standard designed by two Belgians, the acceptance was immediate internationally which created a much better situation for industry, it created a much better situation for security, and it created a situation in which the United States Government has approved the use of the advanced encryption standard for top-secret implementations. The NSA has approved of it, and I think it is a tremendous success and it has to do with the transparency of the process, the scientific integrity with which it was carried out.

Chairman WU. Mr. Starnes.

Mr. STARNES. Thank you. A couple things on the international standards front that relate to this discussion about brand, the primary brand at NIST is NIST, and it is a significant brand. And as NIST doesn't have regulatory authority, they are very good in these kinds of technology and standards discussions across border.

There is a movement, a broad movement that we are watching carefully to this notion of trusted platform. How do I know that this device is trusted? That involves both hardware and software systems. So there is deep concern that our definition of trust is not consistent. We can describe technical trust, but social trust is a little bit more interpretive. So there is work being done against some particular elements, fundamental elements in the platform, things called Trusted Platform Modules (TPMs) where China, for example, would like to build their own based on their definition of trust. And I think we do have to look carefully at some of these formative issues, and NIST can play an extremely important role in creating an adopted international standard at the core basis of the evolution of this trusted platform movement.

Chairman WU. Thank you very much, Mr. Starnes, and my time is expired, but Dr. Schneck, perhaps we can come back in the next round. Mr. Smith, five minutes.

Mr. SMITH. Thank you, Mr. Chairman. Dr. Schneider, you stated in your testimony the need to revise FISMA. Could you elaborate? What do you see as the problems and what you believe should be done about them especially as it relates to NIST?

Dr. SCHNEIDER. Yes, thank you. So I suppose I am an outsider. I am not working for a federal agency, and therefore I don't have to follow FISMA guidelines periodically to establish the security of my computing systems.

But I have heard people who do this in my capacity on the ISPAB, and it strikes me as a very expensive madness, an annual ritual where IT managers have to compile an enormous amount of paper certifying a number of things that is only loosely correlated with the security of their systems.

When the Federal Government didn't require our agency computer systems to be very secure, there was much distance to cover, and the sort of initial inventorying that FISMA reviews are about were a very good way to get started. We are now way down that path, and we understand much better about vulnerabilities and about how to address them, and the current FISMA requirements are not about that. They should be continuous, they should involve monitoring, they should be focused much more on technical issues and much less on inventory-style documentation. They should be much less legalistic exercise between some sort of auditor and

agency management, and I think that lots and lots of resources are being spent trying to accommodate a set of guidelines without getting much security gain.

Mr. SMITH. Okay. Thank you. Ms. Furlani, you noted in your testimony about OMB talking about outcome-focused rather than compliance-focused metrics in cybersecurity. What type of products do you expect to emerge from that effort and what is the timeline associated with that?

Ms. FURLANI. The effort has just begun, so I am not prepared—I really don't know a timeline. But there is an energy assigned to it to try to make the changes as quickly as possible.

The focus is to understand some of the issues that Fred—Dr. Schneider has mentioned and how the changes might be implemented that metrics could be more realistic in today's environment.

Mr. SMITH. Okay. Thank you. Dr. Landau, you mentioned in your testimony the emerging security needs in the area of cloud computing. Could you explain exactly what that is and how it is used on federal computer networks and what unique security needs accompany it?

Dr. LANDAU. When you have a system that is in your office or in your IT center, you own it, you manage it. When the data is instead held somewhere else on Google documents, or Gmail should be examples that people tend to be familiar with, then you are no longer managing the security of your system or your IT managers are no longer managing the security of your system. I don't know exactly how the Federal Government is using cloud computing. I know that NIST has been preparing documents about security risks and security definitions for cloud computing, and I would defer to Cita for that.

But you raise a whole set of security risks and a whole set of policy risks and legal risks when you move to cloud computing, and those have to be addressed, whether it is in business, whether it is in government, whether it is in education. As you shift where the data is being held, what is the backup policy, who has access to it, what are the legal policies? If the data is being held in the United States, that is one thing. Is the data being held in Canada? Is the data being held in the UK? What is the backup policy? So it is a new set of security risks that are being introduced.

Mr. SMITH. Thank you very much.

Dr. LANDAU. Sure.

Chairman WU. Thank you very much, Mr. Smith. Ms. Edwards?

Ms. EDWARDS. Thank you, Mr. Chairman, and thank you to each of our witnesses. I am in the 4th Congressional District in Maryland. We are really proud to be the home of the NIST labs. I know I have had a chance to visit and meet with all of our partners, friends in NIST and am incredibly impressed by the work that is done there, and I appreciate your testimony.

Ms. Furlani, I have a question because I don't quite understand the argument around concerns raised about reorganization if there isn't a deep impact on the actual work that takes place and NIST's responsibilities. And so I wonder if you have any comments about some of the testimony that you have heard here today regarding NIST's capacity to take on these responsibilities and also maintain what I think is a really high standard for cooperation and work

with private industry and trusted work with private industry in so many other areas. And why would a reorganization actually impact that trust that has been well-established?

Ms. FURLANI. Thank you for the opportunity to speak. The energy that was applied to rethinking how we could better use the resources that are ours to manage to address all the incoming opportunities to succeed was the driver behind the proposal—the initial thinking of how we might consider restructuring to be better prepared to address the future, the perception that somehow we would be diminishing what we were already—the great things that are already being accomplished was misplaced. And so what we were trying to do is make sure that we could address the new requirements with the resources that we have and bring the broader perspectives that are available across the laboratory to that focus.

Ms. EDWARDS. Thank you, and I have a couple of other questions that are actually related more to this concern that the absorption of cybersecurity responsibilities and standard setting in the Homeland Security, national security arena, apart from NIST's role—and I wonder if any of the witnesses have some thoughts about as to the value of maintaining a somewhat independent standard setting for cybersecurity that isn't completely folded into a national security framework. I am thinking about areas like healthcare and, you know, some things that seem a little bit of a distance from national security concerns.

Dr. SCHNECK. Thank you and thank you for the opportunity to address that. As a McAfee employee and as a citizen with a background of high-performance computing and actually a founder of the Georgia Tech Information Security Center, I look at the development of cybersecurity standards as a collaborative effort, a necessarily collaborative effort with academia, with private sector and with NIST's scientific guidance as has been mentioned by the other panelists. And we look at that because we are up against an enemy, an international enemy. We are all connected, and we all face the same threat. And this enemy is collaborative, and this enemy works fast. So if we were to have an only-government or a very regulatory standards body for cybersecurity, you not only stifle the market or innovation as we have mentioned, but you set back the implementation of standards of stronger cybersecurity for two to three years, and by the time we are able to meet those standards in the networks that keep the lights on, we are three years behind what the market has developed to do better than the enemy, and we lose that war.

So I feel strongly that cybersecurity standard setting needs to be a very collaborative exercise with the private sector, with academia, with many experts from government with different agencies and certainly with NIST's scientific guidance bringing crucial guidance into that process.

Ms. EDWARDS. And does that mean, in your view does that mean that the coordination for that has to take place out of the White House or is there some sort of other interagency coordination at the federal level with private industry and academia that should be set up that is at the whims of one administration's focus or not?

Dr. SCHNECK. The focus is how we set standards for cybersecurity, not overall cybersecurity strategy but simply stand-

ards. The view I would put here today and on behalf of BSA is it is collaborative. It is private sector and academia but with strong respect for and inclusion of that crucial role that NIST plays, and the China example is a great point of bringing the science back into the equation because the science is what will help us win that war against that threat.

Ms. EDWARDS. Thank you, Mr. Chairman.

Chairman WU. Thank you very much. I believe we have just commenced a series of nine votes, and I think it would be inhumane to ask the panel to wait that long through the votes, so it is my intent to move as expeditiously as possible. And we probably have ten more minutes for questions.

Dr. Schneck, I know that you wanted to make a comment about international issues, but perhaps we could submit a series of written questions and look forward to your response.

Dr. Landau, you distinguish between security issues, identity issues and privacy issues. How does that affect the framework of security standards that we should be developing?

Dr. LANDAU. Well, up until now, NIST has focused on the security standards, and anytime that I was on the ISPAB and we discussed NIST addressing privacy standards, NIST had stayed very far away. I am delighted to hear that it is beginning to move in that direction. I would urge the Committee to give NIST even more authority to do so because I think there is a crying need as we see the accumulation of data in private hands and the need for a good set of standards.

Identity management is a very complicated issue, and we have seen some fledgling efforts. I think that NIST has a very good understanding of the difficulties of doing identity management, and I am sorry that NIST was not pulled more into the discussions earlier this summer as well. It produced the levels of assurance document, that is part of the 800-series, but it wasn't as involved as I think it ought to have been in the policy implications of making decisions about identity management systems for different levels of assurance. And that is a place where I had said earlier I thought that NIST should be providing more policy guidance and should be somewhat more independent.

Chairman WU. So if I am simplifying this incorrectly, please correct me, that there has been a fair amount of activity on the privacy side and that more activity is needed—I am sorry, on the security side and more activity is needed on the privacy and identity side?

Dr. LANDAU. More activity is needed on the privacy side and I would say on the policy side, on the policy side where it is closely allied to technical issues, and one particular example of that is the identity management.

Chairman WU. Very good. And I wanted to ask the panel whoever wants to respond that, you know, we have been talking about standards and focused on that. Is there some low-hanging fruit here if one of the federal entities, NIST or otherwise, developed better education programs so that people up and down the food chain, but especially end-users, became more aware of what they could do. Would that help the overall privacy assurance security issues, you know, outside of standard setting?

Dr. LANDAU. So I would like to say here that while I think a lot of the Computer Security Division, the one place that I think it has not handled things well is in outreach and in particular inability to find the information. If you know the information is there and you look for it, you can find it. But if you are not determined, it is somewhat hard to do. And I would like to see better outreach, better development of its website, more usable access to information.

Chairman WU. What kinds of mechanisms could we use to push that out as opposed to having it as a pool that people reached into?

Dr. LANDAU. I know that NIST had a program in which it advised small business, but it was a very small program. I mean, there is the answer, it is a very small program. It doesn't reach very many people. I think NIST should be doing that work and not the FBI.

Chairman WU. Would the ag extension or manufacturing extension sort of mechanism or model apply in this case?

Dr. LANDAU. I don't know what the ag extension model is well enough. I am sorry.

Chairman WU. Mr. Furlani and then Mr. Starnes, we will come back to you.

Ms. FURLANI. Yes, we have been planning and working historically with our Manufacturing Extension Partnership and with our new YouTube video. We are hoping to leverage that capability to get to the small manufacturers. Of course—it is addressing all small businesses. We were hoping that maybe some of your newsletters might refer back to our YouTube video and make it more available to your constituents as well.

Chairman WU. Mr. Starnes.

Mr. STARNES. Yes, traditionally in information security, we have, to your observation, Representative Edwards, pulled the collective knowledge and talent across multiple parts of industry and government, and I think this is a clear case where we need to do that again and are doing that. So we have to differentiate between standards, which NIST is very good at, and methods and best practice which are putting standards into action. And there are some very good technical solutions that are coming, multilaterally as I mentioned, from government that move us from just certification and accreditation. We spent $1.31 billion on certification and accreditation last year. Many of those dollars should be spent with these new tools and techniques for continuous monitoring of information technology systems using all of the intelligence of all of our federal agencies and commercial entities.

Chairman WU. Thank you very much, Mr. Starnes. My time has about expired. Mr. Smith, further questions?

Mr. SMITH. I think just briefly. Mr. Bohannon, you emphasized in your testimony that Congress should avoid making NIST a regulator of private-sector actions. Could you elaborate and maybe touch on how the government procurement is de facto an approach to regulation, whether on purpose or not?

Mr. BOHANNON. That is a very good question. Obviously government procurement is where the rubber hits the road, when it comes to NIST work. The approach with NIST, though, is consistent with trying to figure out how to walk that fine line because with a few

exceptions, some of which I talk about in my testimony, on the whole where NIST has developed federal information processing standards, it has done so in an open, transparent and collaborative way so that when FIPS (Federal Information Processing Standard) are in fact referenced for government use, they are the product on the whole of working with the stakeholders, the technology providers, and the users to make sure there is a standard that as much as possible conforms to general commercial practice. And notably the government has its needs. Those are taken into account, but that is a fine line and one that, going back to Congresswoman Edwards' question, you know, some of us have short memories. But it was just seven years ago that when the Department of Homeland Security was going to be created, the proposal was to move the Computer Security Division to DHS. Thanks to the leadership of this Committee, on both sides of the aisle, that did not happen. I think we would be in a very different situation today if the Computer Security Division had moved. I think its work on the special 800-series, I think its work on AES (Advanced Encryption Standard), I think the work where it needs to go would have been fundamentally different because it would have come out of an agency that had very specific law enforcement and regulatory mission stakes, and the credibility of that work would have been dramatically differentiated.

So Mr. Smith, you are absolutely right. It is a fine line, but as we pointed out, the way NIST does its business in a collaborative way means that on the whole, it doesn't always get it perfect, but on the whole, the results are consistent with commercial goods, commercial practice, taking into account stakeholders, and try to reflect the best of what should be in that standard.

Mr. SMITH. Thank you. Thank you, Mr. Chairman.

Chairman WU. Thank you very much, Mr. Smith. Ms. Edwards? No further questions. Okay.

Ms. Furlani, there have been numerous suggestions for about what you might do, what your agency might do and so on. I wanted to give you an opportunity to respond to any of the suggestions that you want to respond to, but in particular, I would very much like you to respond to—I mean, it is not as simple as should CSD become a laboratory on its own, but that is—let us reduce it to that simplicity, and could you respond to that and any other comments, suggestions that you would like to respond to?

Ms. FURLANI. Thank you, Chairman Wu. Certainly we have had a lot of input, and as I have said, both support and concerns. We are going to go back to the drawing board essentially and revisit what might make the best next proposal. The idea of separating cybersecurity from information technology is difficult for me to understand because of the intertwined nature of the two, but the decision of course would be Dr. Gallagher's, not mine. So we have lots to consider, many from the panel members which I greatly appreciate and others. And we have a lot of rethinking—and of course the original goal, which I want to go back to and make sure that we have the full input from my staff which is where we all started with just trying to get the staff's input. We are back to revisiting the entire setup, and we will hopefully come out with something

that enables us to move forward in the future, meet our new opportunities and challenges in a much more robust capable way.

Chairman WU. Thank you very much, Ms. Furlani. And for the entire panel, we will submit some additional written questions. But you all have put a lot of work into the prepared written materials, into preparing for the oral testimony, and some of you have traveled a decent distance to get here. So at the risk of shortening up my thank-yous in person at the table, I want to give each of you who has something that you want to contribute to this discussion but you haven't had an opportunity to put that either in your oral testimony or you haven't been asked that question. Please, at this time, for as much time as we have, if you want to add that last point, this is your chance.

Dr. LANDAU. I would like to just make a brief comment which I do have in my written testimony about the importance of usability work in security, and I know that the Computer Security Division has begin work on this, and I think it is an important, new direction. I would like to see the Committee strongly support that work because of course, it increases security. Thank you.

Chairman WU. Thank you. Anyone else?

Dr. SCHNECK. Thank you. One opportunity—we talk a lot about cybersecurity and the threats and the scariness of it and the work that we need to do. The issue of awareness was raised before, and that is a very positive point, and I think there is a huge opportunity for NIST to work with the National Cybersecurity Alliance. Part of this is in my written testimony, but when you visualize that, this group, what they do is they take the message and they bring it to the street, from the federal to the State, local, tribal community level and to homeowners' associations and to schools so that our youngest citizens all the way on up are learning not just what to be careful of but how to responsibly build security and privacy as Dr. Landau has referred to today into their daily lives and to our use of cyber, because it is going to affect our entire way of life forward.

Chairman WU. Thank you very much. Anyone else?

Mr. STARNES. Thank you, Chairman, but I would like to put just a punctuation mark on my C&A (Certification and Accreditation) comments of earlier. If we took just 30 percent of the C&A dollars that were spent in 2008, that would be more than we spent on cybersecurity research in the entire year. So I encourage the Committee to focus legislatively on these processes as well and help government agencies and industry do zero-based implementation of important new methods around continuous monitoring.

Chairman WU. Thank you very much, Mr. Starnes. And since Mr. Smith and I are at risk of missing some of these votes, Dr. Schneider, Mr. Bohannon, your indulgence in perhaps providing us comments and answering other inquiries as we go. I want to again thank you all very, very much for your testimony, and no guarantees in life, but I think there is a high probability that we will try to pitch in with relevant legislation to try to improve the situation, and we look forward to your comment on that effort also. So thank you very much. The record will remain open for two weeks for additional statements from Members and for answers to follow-up ques-

tions. The witnesses are excused, and the hearing is now adjourned. Thank you.

[Whereupon, at 3:17 p.m., the Subcommittee was adjourned.]

Appendix:

Answers to Post-Hearing Questions

ANSWERS TO POST-HEARING QUESTIONS

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

Questions submitted by Chairman David Wu

Q1. What are the current limitations and flaws of FISMA and what parts of FISMA policy must change to improve the security of federal information technology systems? What role should NIST play in an effective FISMA framework?

A1. The Federal Information Security Management Act (FISMA) Act of 2002 tasked the National Institute of Standards and Technology (NIST) with the responsibility to establish security standards and guidelines for the Federal Government and charged the Office of Management and Budget (0MB) with enforcement of FISMA.

NIST developed two standards, Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems and FIPS 200, Minimum Security Requirements for Federal Information and Information Systems and associated guidelines including Special Publication 800–53, Recommended Security Controls for Federal Information Systems and Organizations to provide a foundation for federal agency security.

Since FISMA's release, agencies' security capabilities have been maturing, and it is time to shift the focus from compliance to improving the implementation of their enterprise security. The existing NIST work in developing standards and guidelines and in creating tools for monitoring the status of security settings enables this shift. NIST is prepared to develop additional security automation tools to further optimize system security configurations and report status of system components. NIST is poised to ensure its standards and guidelines address new security technologies that can be used to mitigate the ever changing threat environment. In addition, NIST is working with 0MB and others to develop security metrics that will better quantify the improvements that agencies make to their security implementations and provide more robust methods for assessment of agencies' security posture.

ANSWERS TO POST-HEARING QUESTIONS

Responses by Susan Landau, Distinguished Engineer, Sun Microsystems, Burlington, MA

Questions submitted by Chairman David Wu

Q1. What are the current limitations and flaws of FISMA and what parts of FISMA policy must change to improve the security of federal information technology systems? What role should NIST play in an effective FISMA framework?

A1. I am speaking from my experience on ISPAB; since I retired from the board in January 2008, this information is a bit dated. I have just three points to make.

- In its early years, FISMA increased security awareness. However, after multiple times of agencies filling in the FISMA reports, it appears—at least from the outside—that FISMA has become more of an exercise in paperwork than a schema for enforcing good security practices.
- The problem is incentives and this is not a NIST issue, but a Federal Government one. Unless the cost for failure to have a good security posture and a good recovery plan is high, it is difficult to incentivize the agencies to treat cybersecurity with the appropriate attention.
- Backup and disaster recovery are two issues not covered by FISMA; they should be part of any cybersecurity plan (and continuity of operations should be updated with each technology enhancement).

I hope this is useful to you.

ANSWERS TO POST-HEARING QUESTIONS

Responses by Phyllis Schneck, Vice President, Threat Intelligence, McAfee Corporation

Questions submitted by Chairman David Wu

Q1. What are the current limitations and flaws of FISMA and what parts of FISMA policy must change to improve the security of federal information technology systems? What role should NIST play in an effective FISMA framework?

A1. We believe Congress needs to reform FISMA, to close the gap between compliance and security. Congress needs to legislate to empower officials in charge of the security of agencies' computer networks:

* First, they need authority to actually enforce security requirements over their agencies' networks and systems. It would be appropriate for OMB to develop some additional incentives to push agencies to comply with their FISMA requirements, including having some percentage of cyber budgets of agencies withheld in the event that they do not show good progress toward meeting their compliance obligations. Alternatively, agencies could be rewarded with larger budget growth rates for their cyber security programs when they show actual progress in improving the security postures of their operations.

* Second, they need the technical and human resources necessary to perform these tasks, such as network monitoring and automated security policy compliance monitoring and enforcement capabilities. This in particular is where NIST efforts will be most needed. Network monitoring and automated security policy compliance monitoring should be done across the government on the basis of common standards. This would allow a government-wide security center to have a consistent view of federal networks' security.

We also need the legislation to ensure these officials are accountable for identifying and addressing the threats and vulnerabilities that their networks actually face. We can do this in particular by having "red teams" test the effectiveness of the security measures in place against real-life attacks, and by having this serve as a feedback loop that leads to system and network security improvements.

ANSWERS TO POST-HEARING QUESTIONS

Responses by William Wyatt Starnes, Founder, CEO, and President, SignaCert, Inc.; Founder, Tripwire, Inc.

Questions submitted by Chairman David Wu

Q1. What are the current limitations and flaws of FISMA and what parts of FISMA policy must change to improve the security of federal information technology systems? What role should NIST play in an effective FISMA framework?

A1. FISMA is a broad methodology that seeks to normalize the IT compliance and reporting for Federal IT infrastructure. Generally the method encourages "periodic testing" of IT devices and infrastructure against a range of configuration, vulnerability and usage best practices.

There are several problems with this approach.

- Specifically, it is questionable whether the FISMA report card actually properly and correctly reflects the actual security, compliance and readiness of the Civilian Agency reporting the results.
- Also, FISMA largely is viewed as a Certification and Accreditation (C&A) process, and the C&A processes are "point in time" current state of the IT devices. This "IT Audit" mentality:
  - creates periodic "peak load" human resource drain by the Agencies to do the FISMA reporting
  - generates tremendous paperwork, much of which goes largely unused past the summary reporting for the actual roll-up to the OMB
  - as it is point in time and periodic, there is large time gap between the audits where a actual and problematic security and compliance issues can emerge, causing increased risk and disruption.

There is a lot of emerging consensus that we should change or update the methodologies and technologies used for FISMA, as well as changing driving legislation, to deal with the aforementioned risks and weaknesses.

NIST/NSA/DHS and others have been in close collaboration for several years on best practices, method and technologies that address many of the FISMA gaps. Called the Security Content Automation Protocol, or SCAP, these methods are very well suited to all IT management needs, and we recommend that the full extended version of SCAP be establish as the technical pillar for FISMA 2.0 usage.

In concert, we strongly urge Congress, through all of the committees activities, to begin to shift "C&A" requirements (and the thus the dollars allocated for C&A), to SCAP CONTINUOUS MONITORING.

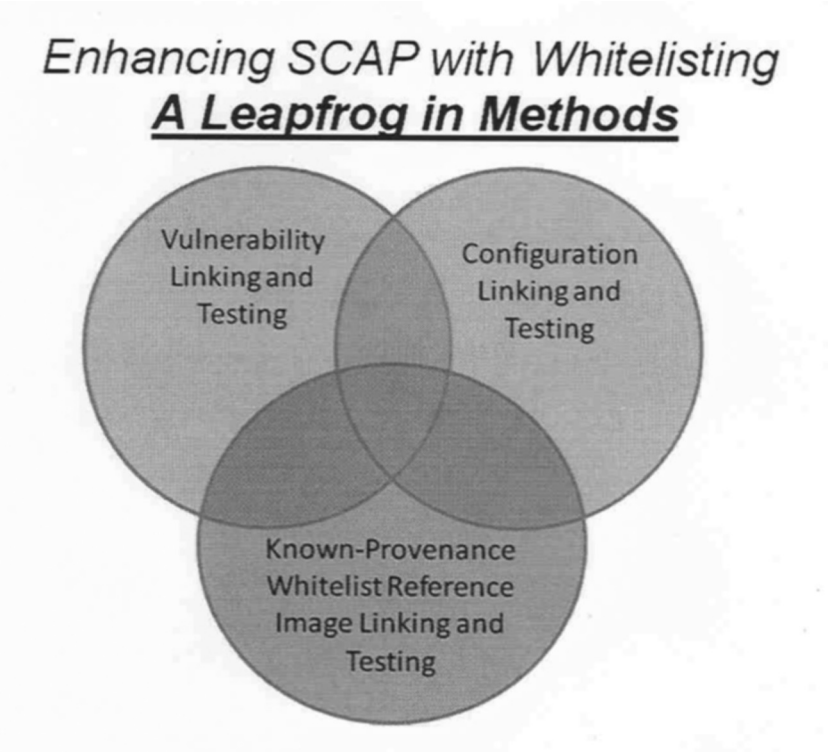
IT compliance, done well, should be largely transparent to the users and even the IT staff. Good systems hygiene should be complete, intrinsic and continuous, not just scorecard driven period process. Legislated FISMA processes should fully embrace this concept.

With the SCAP framework, the following key IT issues can be continuously addressed in a consistent form at all Agencies, and ultimately across the broader DOD and even commercial IT enterprise:

1. It devices are configured with the *right software components* (including **supply chain** provenance) not only at the time and point of deployment, but actively and continuously across their usage lifetime.
2. The deployed software can be *configured correctly* at point of deployment, and maintained in the correct, secure and most stable configuration throughout their usage lifetime.
3. The *presence of vulnerabilities can be actively tested and validated* in a consistent and complete way across the entire IT infrastructure on an active, real time and continuous basis.

See the diagram below for a simple view of the core SCAP test areas.

Another benefit of these methods is that we can use the SCAP protocol to aggregate and automate "best practices" knowledge against all three of the areas above so that IT operational readiness (AS A NATION) gets better based on the collective knowledge and experience of the best IT expertise that we have, and we can immediately apply that knowledge—reducing our cyber vulnerabilities across all industry sectors.


Enhancing SCAP with Whitelisting
A Leapfrog in Methods
Vulnerability Linking and Testing
Configuration Linking and Testing
Known-Provenance Whitelist Reference Image Linking and Testing

ANSWERS TO POST-HEARING QUESTIONS

Responses by Fred B. Schneider, Samuel B. Eckert Professor of Computer Science, Cornell University

Questions submitted by Chairman David Wu

Q1. What are the current limitations and flaws of FISMA and what parts of FISMA policy must change to improve the security of federal information technology systems? What role should NIST play in an effective FISMA framework?

A1. I do not have direct experience with FISMA and I have not read the legislation. But I am a member of NIST's Information Security and Privacy Advisory Board (ISPAB), and our board has heard a good deal from officers at civilian Federal agencies that must comply with FISMA as well as from the Inspector General (IG) community, which is responsible for auditing FISMA compliance. These comments are based on what I have heard from those communities.

I believe that we should strive to have FISMA compliance for an agency mean that the agency's computing systems are secure enough, given the tasks they perform, the data they store, and the information and services they can access. I fear that the way FISMA is interpreted today does not succeed at this.

FISMA compliance should embody a philosophy of risk management rather than one of absolute security. Risk management requires understanding the consequences of system compromise, including loss of functionality, ex-filtration of confidential data, corruption of information, and even possible use by an attacker as a stepping-stone to other systems. This is multi-dimensional and, therefore, attempting a simple categorization of all systems within an agency or across agencies is unlikely to be useful. Only with richer kinds characterizations, can we portray system weaknesses in a sufficiently useful way for decision-makers. And only richer characterizations will incentivize corrective measures that address the real problems in context (as opposed to incentivizing measures that merely sound impressive on paper).

There needs to be a strong coupling between FISMA compliance and security of a system in its deployed context. Today that coupling is weak. A system that has been deemed compliant today might still be easy to attack; a system that today implements sufficient defenses for its role will not necessarily be deemed FISMA compliant.

This disconnect between FISMA compliance and real security partly results from

- an absence of good metrics for security,
- FISMA compliance being dominated by documenting defenses rather than by exercising them, and
- FISMA compliance being seen as a periodic obligation discharged by negotiating with an auditor rather than a continuous one concerned with eliminating system vulnerabilities as they become known.

The first of these—the absence of metrics—is an open research question; the other two are inherent in the way FISMA compliance is interpreted and evaluated.

NIST is an obvious place to undertake research in security metrics. That said, I am doubtful that anyone will ever devise a way to measure whether a system is secure (because security is relative to attacks, and new attacks are being discovered every day). But it does seem reasonable to expect better ways than practiced today for evaluating a system and ascertaining whether it is secure against some set of known attacks. And NIST is a reasonable place to develop and codify as metrics these better ways; FISMA compliance assessments should adopt such improved metrics as they become available.

NIST has in the past done a good job of developing and documenting security best practices for civilian Government agency computing systems. Best practices bring good security, so we should want NIST to continue that work. And a security evaluation of a system for FISMA compliance should ascertain whether current best practices are being followed. I would urge, though, that "best practices" be expanded to include the obligation that a system is checked against lists of known vulnerabilities. That is, we need to check that certain desirable features and processes are present but also check that undesirable ones are absent.

Finally, FISMA compliance needs to require more than documenting what a system is. We don't evaluate the efficacy of a weapons system or a military unit only by evaluating metrics—we run exercises in the field and force engagement with realistically simulated attackers. FISMA compliance needs to adopt that approach for our computing systems. Some of this can be accomplished with existing automated tools, but some will require building new tools. We should also contemplate requir-

ing periodic random surprise red-team attacks and simulated natural disasters, because this evaluates system trustworthiness in a way that incentivizes continuous readiness. The key point is to promote the view that system defense a continuous obligation and is results-oriented, rather than being documentation-oriented. Documentation is a useful basis for determining accountability after a system is found wanting, but documentation does little to defend against attacks.

ANSWERS TO POST-HEARING QUESTIONS

Responses by Mark Bohannon, General Counsel and Senior Vice President for Public Policy, Software & Information Industry Association (SIIA)

Questions submitted by Chairman David Wu

Q1. What are the current limitations and flaws of FISMA and what parts of FISMA policy must change to improve the security of federal information technology systems? What role should NIST play in an effective FISMA framework?

A1. As the Committee is well aware, the *Federal Information Security Management Act* (FISMA), enacted in 2002, sets forth a comprehensive framework to ensure the effectiveness of security controls over information resources that support federal operations and assets. FISMA assigns specific responsibilities to federal agencies, the Office of Management and Budget (OMB), and the National Institute of Standards and Technology (NIST). It also requires agencies and OMB to annually report on the adequacy and effectiveness of agency information security programs and compliance with the provisions of the Act. To help meet these requirements, OMB established a uniform set of information security measures that all federal agencies report on annually. NIST produces important guidance and publications related to FISMA implementation.

In reviewing the current limitations and flaws of FISMA, recent investigations by the General Accounting Office (GAO) are useful inputs. As the GAO has stated,[1] leading organizations and experts have identified different types of measures that are useful in helping to achieve information security goals. While it found that officials categorized these types using varying terminology, GAO concluded that they generally fell into three types: (1) compliance, (2) control effectiveness, and (3) program impact. These types are consistent with those laid out by NIST in its information security performance measurement guide.[2] The GAO found that, while information security measures can be grouped into these three major types, organizations and experts reported that all such measures generally have certain key characteristics, or attributes. These attributes include being (1) measurable, (2) meaningful, (3) repeatable and consistent, and (4) actionable.[3]

Using this framework, GAO determined—and we concur—"that federal agencies have not always followed key practices identified by leading organizations for developing information security performance measures. While agencies have developed measures that fall into each of the three major types (i.e., compliance, control effectiveness, and program impact), on balance they have relied primarily on compliance measures, which have a limited ability to gauge program effectiveness. Agencies stated that, for the most part, they predominantly collected measures of compliance because they were focused on measures associated with OMB's FISMA reporting requirements. In addition, while most agencies have developed some measures that include the four key attributes identified by leading organizations and experts, these attributes were not always present in all agency measures. Further, agencies have not always followed key practices in developing measures, such as focusing on risks."

GAO focused on the inadequacies of OMB's measures which "did not address the effectiveness of several key areas of information security controls, including, for example, agency security control testing and evaluation processes. There is no measure of the quality of agencies' test and evaluation processes or results that demonstrate the effectiveness of the controls that were evaluated."

As a starting point, the most recent five recommendations GAO made to OMB to assist federal agencies in developing and using measures that better address the effectiveness of their information security programs are worth considering:

- "issue revised guidance to chief information officers for developing measures," which we would add should follow and build on the relevant work and publications produced by NIST;

---

[1] See GAO report number GAO–10–159T, entitled 'Information Security: Concerted Effort Needed to Improve Federal Performance Measures' which was released on October 29, 2009.

[2] National Institute of Standards and Technology, Performance Measurement Guide for Information Security, NIST Special Pub. 800–55 Revision 1 (Gaithersburg, Md.: July 2008).

[3] Although we focused on identifying attributes and practices for measuring the performance of information security programs, our findings conformed closely to our prior work on effective performance measurement and reporting practices for the Federal Government in general. See, for example, GAO, Managing for Results: Enhancing Agency Use of Performance Information for Management Decision Making, available at *www.gao.gov/cgi-bin/getrpt?GAO-05-927*, Sept. 9, 2005.

- "direct chief information officers to ensure that measures exhibit key attributes";
- "direct chief information officers to employ the key practices for developing a measure as identified by leading organizations," again taking into account the work and publications produced by NIST;
- "revise annual FISMA reporting guidance to agencies"; and:
- "revise the annual FISMA report to Congress to provide better status information on the security posture of the Federal Government."

In addition, we would note that implementation of FISMA, with the continued leadership of NIST working with OMB, would benefit from:

- Requiring that federal agency CIOs and CISOs are appropriately positioned within their agencies management structure to promote "top down" priority of information security.
- Agencies sometimes use FISMA compliance as an excuse to reject innovations simply because they are new and not explicitly reflected in the FISMA checklists. FISMA should actively encourage government agencies to be more open to deploying cutting edge solutions.
- Audit and oversight methods should be harmonized to the greatest degree possible using NIST work and publications. There also needs to be work to establish consistency in IG examinations, recognizing that IG offices are not necessarily staffed with requisite skill sets.
- Agencies should conduct at least annual risk assessments that incorporate classified information and input from the private sector. Those risk assessments should also incorporate the work and outcome of NIST as well as other sources, including the Department of Homeland Security's US–CERT.