ASSESSING CYBERSECURITY ACTIVITIES AT NIST AND DHS

HEARING

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY AND INNOVATION

COMMITTEE ON SCIENCE AND TECHNOLOGY

HOUSE OF REPRESENTATIVES

ONE HUNDRED ELEVENTH CONGRESS

FIRST SESSION

JUNE 25, 2009

Serial No. 111–39

Printed for the use of the Committee on Science and Technology

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

U.S. GOVERNMENT PRINTING OFFICE

50–325PDF WASHINGTON : 2009

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

COMMITTEE ON SCIENCE AND TECHNOLOGY

HON. BART GORDON, Tennessee, *Chair*

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

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

SUBCOMMITTEE ON TECHNOLOGY AND INNOVATION

HON. DAVID WU, Oregon, *Chair*

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

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

RALPH M. HALL, Texas

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

CONTENTS

June 25, 2009

ASSESSING CYBERSECURITY ACTIVITIES AT NIST AND DHS

THURSDAY, JUNE 25, 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 [Chair of the Subcommittee] presiding.

VerDate 11-MAY-2000 20:17 Dec 19, 2009 Jkt 050325 PO 00000 Frm 00005 Fmt 6633 Sfmt 6633 C:\DWORK\T&I09\062509\50325 SCIENCE1 PsN: SCIENCE1

BART GORDON, TENNESSEE
CHAIRMAN

RALPH M. HALL, TEXAS
RANKING MEMBER

U.S. HOUSE OF REPRESENTATIVES

COMMITTEE ON SCIENCE AND TECHNOLOGY

SUITE 2320 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6301
(202) 225–6375
TTY: (202) 226–4410
http://science.house.gov

Subcommittee on Technology and Innovation

Hearing on

ASSESSING CYBERSECURITY ACTIVITIES AT NIST AND DHS

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

Witness List

Mr. Greg Wilshusen
Director, Information Security Issues, Government Accountability Office (GAO)

Mr. Mark Bregman
Executive Vice President and Chief Technology Officer, Symantec Corporation

Mr. Scott Charney
Corporate Vice President, Trustworthy Computing, Microsoft Corporation

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

HEARING CHARTER

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

Assessing CyberSecurity Activities at NIST and DHS

THURSDAY, JUNE 25, 2009
2:00 P.M.–4:00 P.M.
2318 RAYBURN HOUSE OFFICE BUILDING

I. Purpose

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

II. Witnesses

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

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

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

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

III. Overview

In January 2008, the Bush Administration established, through a series of classified executive directives, the Comprehensive National Cybersecurity Initiative (CNCI). While the goal of the initiative was to secure federal systems, a number of security experts have expressed concern that the classified nature of the CNCI has inhibited active engagement with the private sector despite the fact that 85 percent of the Nation's critical infrastructure is owned and operated by private entities. While experts are concerned by the lack of transparency and public-private cooperation under the CNCI, they have also urged President Obama to build upon the existing structure of CNCI. In February 2009, the Obama Administration called for a 60-day review of the national cybersecurity strategy. The President's review required the development of a framework that would ensure that the CNCI was adequately funded, integrated, and coordinated among federal agencies, the private sector, and State and local authorities.

On May 29, 2009, the Administration released its *Cyberspace Policy Review*. The review recommended an increased level of interagency cooperation amongst all departments and agencies. The active exchange of information concerning attacks, vulnerabilities, research, and security strategies is essential to the efficient and effective defense of federal computer systems. The review team also emphasized the need for the Federal Government to partner with the private sector to guarantee a secure and reliable infrastructure. Furthermore, it highlighted the need for increased public awareness, the education and expansion of the Information Technology (IT) workforce, and the importance of advancing cybersecurity research and development.

The hearing will address recommendations made in the *Cyberspace Policy Review* and a recent report from the GAO.[1] DHS currently monitors the federal civilian networks for cyber attacks and coordinates the gathering and dissemination of information on cyber attacks to federal agencies and private industry. The policy review and GAO report highlight deficiencies in both the operations and coordination roles. The policy review also calls on a more proactive plan for collaboration with international standards bodies and an end to the cybersecurity distinctions between national security and other federal networks. NIST currently develops and promulgates standards to help secure the federal civilian network systems. Finally, both reports call for an increase in effective public/private partnerships, despite a current high number of coordination councils and advisory boards. The policy review states that the high number of coordinating groups has left some participants frustrated with unclear roles and responsibilities and an excess of plans and recommendations.

IV. Issues and Concerns

Operations

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

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

Standards

A major recommendation from industry experts indicates the need to end the bifurcation of minimum cybersecurity standards amongst military, national security, and federal civilian networks. A recent draft report from NIST proposes a unified set of standards that meet this recommendation.[2] The use of a single set of basic standards and minimum security requirements will simplify acquisition of network components and ease the assessment of cybersecurity performance.

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

Critical Infrastructure

Critical infrastructure represents a challenge because much of it is privately-owned, yet could represent a major vulnerability to the security of the Nation. The *Cyberspace Policy Review* called for increased coordination and integration of current efforts among all federal departments and agencies, and with private industry to assist in securing critical infrastructure. Currently, an assortment of public-private partnerships, advisory boards, and information sharing mechanisms exists across the Federal Government, such as the Critical Infrastructure Partnership Ad-

---

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

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

visory Council (CIPAC), IT–Sector Coordinating Council (IT–SCC), National Infrastructure Advisory Council, and Information Security and Privacy Advisory Board (ISPAB).

Metrics

Throughout its recommendations, the review team highlights the need for the increased use of performance metrics to guide strategies and to make key planning decisions. Cybersecurity efforts are traditionally assessed by detailing the number of initiatives and funding spent on these initiatives. A set of metrics based on actual outcomes of efforts, instead of output of initiatives and funds would better assess the current activities and identify areas for improvement. They recommend the development of a formal program assessment framework that would guide departments and agencies in defining the purpose, goal, and success criteria for each program. This framework could then be used as a basis for implementing a performance-based budgeting process, setting priorities for research and development initiatives, and assisting in development of the next-generation networks.

V. Background

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

Department of Homeland Security

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

National Cybersecurity Division

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

- **United States Computer Emergency Readiness Team**

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

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

- **National Cyber Response Coordination Group**

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

- **Cyber Storm**

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

- **Software Assurance Program**

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

National Cyber Security Center

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

Cyber Security Research and Development Center

Cyber security research within DHS is planned, managed, and coordinated through the Science and Technology Directorate's Cyber Security Research and Development Center. This center supports the research efforts of the Homeland Security Advanced Research Projects Agency (HSARPA), coordinates the testing and evaluation of technologies, and manages technology transfer efforts. The FY 2010 budget includes $37.2 million for cyber security R&D at DHS; this is an increase of $6.6 million over FY 2009.

National Institute of Standards and Technology

NIST is tasked with protecting the federal information technology network by developing and promulgating cybersecurity standards for federal civilian network systems (Federal Information Processing Standard [FIPS]), identifying methods for assessing effectiveness of security requirements, conducting tests to validate security in information systems, and conducting outreach exercises. These tasks were appointed to NIST in the *Computer Security Act of 1987.* In the *Federal Information Security Management Act of 2002,* OMB was tasked to develop implementation plans and enforce the use of the FIPS developed by NIST. Cybersecurity activities are conducted through NIST's Information Technology Laboratory which has a budget request of $72 million for FY 2010, including $15 million in support of the CNCI and $29 million for Computer Security Information Assurance (CSIA) R&D.

Computer Security Division

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

- **Security Technology**

  The Security Technology group focuses on cryptography and online identity authentication. These foci ensure that access to information is only granted to the appropriate users and done so in a secure manner using technologies such as: cryptographic protocols and interfaces, public key certificate management, biometrics, and smart tokens.

- **Systems and Network Security**

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

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

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

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

- **Security Management and Assistance**

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

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

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

- **Security Testing and Metrics**

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

Chair WU. Good afternoon. I would like to welcome everyone to today's hearing on the cybersecurity activities of the National Institute of Standards and Technology (NIST) and the Department of Homeland Security (DHS). This is the third hearing the Science and Technology Committee has held on this very, very important issue.

The prior hearings discussed the research and development needs for improved cybersecurity and federal agencies' responses to recommendations made in the *Cyberspace Policy Review*.

All of us, in both public and private sectors, rely on IT (Information Technology) networks to manage a great many things ranging from online bank accounts to the power grid. With this increased reliance on networks, we have become more sensitive to the security of these networks. To support cybersecurity efforts, the prior Administration implemented an estimated $40 billion Comprehensive National Cybersecurity Initiative in January of 2008.

This year alone, DHS and NIST have requested over $500 million for their cybersecurity efforts, with an additional $340 million requested for research through the Networking and Information Technology Research and Development (NITRD) Program. Even by government standards, almost $850 million is a fair amount of money.

Despite the substantial funding levels and many hours spent by federal employees on this issue, the assessment remains the same: overall, our cybersecurity remains poor.

The Administration's *Cyberspace Policy Review* emphasized the recommendations made in previous reports: first, bolster cybersecurity operations protecting the federal network systems; second, improve interagency and private sector coordination; third, modernize and coordinate the research agenda; and fourth, enhance public education on cybersecurity. This committee wants to understand the impediments that have prevented similar recommendations from being successfully implemented in the past.

I believe one key recommendation made in the *Cyberspace Policy Review* is the need for objectives and metrics to accurately measure cybersecurity performance. The development of these metrics would provide a base from which we could improve program assessment, budgeting, research and development prioritization, and strategic planning.

This recommendation mirrors the Subcommittee's belief that agencies should be accountable for real-world outcomes, rather than outputs measured in terms of money spent, projects supported, and interagency meetings, which is how the agencies categorized their success at a Subcommittee hearing last week.

As is generally the case, we have many recommendations, but the devil is in the details. I hope that in addition to making suggestions on this hearing's issues, our witnesses can tell us what is required to implement their recommendations.

I want to thank our witnesses for appearing before us today, and now I would like to recognize my friend and colleague, Mr. Smith from Nebraska, for his opening statement.

[The prepared statement of Chair Wu follows:]

PREPARED STATEMENT OF CHAIR DAVID WU

Good afternoon. I want to welcome everyone to today's hearing on the cybersecurity activities of the National Institute of Standards and Technology and the Department of Homeland Security. This is the third hearing the Science and Technology Committee has held on this critical issue.

The previous hearings discussed the research and development needs for improved cybersecurity and federal agencies' responses to recommendations made in the *Cyberspace Policy Review*.

All of us, in both public and private sectors, rely on IT networks to manage everything from online bank accounts to the power grid. With this increased reliance on networks, we have become more sensitive to the security of these networks. To support cybersecurity efforts, the previous administration implemented an estimated $40 billion Comprehensive National Cybersecurity Initiative in January 2008.

This year alone, DHS and NIST have requested over $500 million for their cybersecurity efforts, with an additional $340 million requested for research through the Networking and Information Technology Research and Development Program. Even by government standards, almost $850 million is a lot of money.

Despite the substantial funding levels and many hours spent by federal employees on this issue, the assessment remains the same: our cybersecurity is poor.

The Administration's *Cyberspace Policy Review* re-emphasized the recommendations made in previous reports: first, bolster cybersecurity operations protecting the federal network systems; second, improve interagency and private sector coordination; third, modernize the research agenda; and fourth, enhance public education on cybersecurity. This committee wants to wants to understand the impediments that have prevented similar recommendations from being successfully implemented in the past.

I believe one key recommendation made in the *Cyberspace Policy Review* is the need for objectives and metrics to accurately measure cybersecurity performance. The development of these metrics would provide a base from which we could improve program assessment, budgeting, research and development prioritization, and strategic planning.

This recommendation mirrors the Subcommittee's belief that agencies should be accountable for real-world outcomes, rather than outputs measured in terms of money spent, projects supported, and interagency meetings, which is how the agencies categorized their success at a Subcommittee hearing last week.

As is generally the case, we have many recommendations, but the devil is in the details. I hope that in addition to making suggestions on this hearing's issues, our witnesses can tell us what is required to implement their recommendations.

Mr. SMITH. Thank you, Mr. Chair, for calling the hearing today on cybersecurity, the third in a series of hearings held by the Committee this month.

While the Committee's jurisdiction on cybersecurity issues is generally limited to two agencies, DHS and NIST, because of their broad roles and responsibilities, the activities of both agencies directly impact not only the entire Federal Government but also many private sector computer security stakeholders. Accordingly, we have the benefit of being able to examine cybersecurity through a very broad lens and the opportunity to influence the debate on the Government's actions in the most important and pressing policy areas.

To this end, I would like to briefly outline what I see as the key, high-level, outstanding questions which drive the direction of cybersecurity policy for this committee and Congress as we do go forward.

First, as we explored last week with respect to protection of government networks, are we confident the reported $30 billion effort comprising the Administration's Comprehensive National Cybersecurity Initiative, CNCI, is appropriately focused, and will DHS's centerpiece EINSTEIN program provide effective and lasting security? If not, what are the best alternatives to this investment and focus area, and perhaps more importantly, how do we do a bet-

ter job at measuring cybersecurity so we can more systematically evaluate technology and policy options and perhaps even fit in a hearing between votes?

The largest outstanding questions, however, revolve around the nature of the relationship between the government and the private sector and efforts to secure non-government systems. Stakeholders on all sides place a great deal of emphasis on strengthening public-private partnerships to secure critical infrastructure, but beyond the well-established goals of improving information sharing and policy dialogue, the precise features of the desired partnerships as well as the scope of what constitutes critical infrastructure have remained largely undefined. Does this entail a new regulatory regime at DHS or NIST, new liability protections, or incentives for private sector actors or some combination thereof? Are there other innovative partnership models which could be explored?

These are all weighty questions which will not be answered at this hearing or in the immediate future, but I believe they require the careful attention of Congress going forward as we consider legislative options to improve network security.

I thank the Chair for assembling an excellent panel today. Thank you for being here, and I look forward to the productive discussion.

[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 third in a series of hearings held by the Committee this month.

While the Subcommittee's jurisdiction on cybersecurity issues is generally limited to two agencies—DHS and NIST—because of their broad roles and responsibilities, the activities of both of these agencies directly impact not only the entire Federal Government but also many private sector computer security stakeholders.

Accordingly, we have the benefit of being able to examine cybersecurity through a very broad lens, and the opportunity to influence the debate on—and the government's actions in—the most important and pressing policy areas.

To this end, I would like to briefly outline what I see as the key, high-level outstanding questions that should drive the direction of cybersecurity policy for this committee and for Congress as we go forward.

First, as we explored last week with respect to protection of government networks, are we confident that the reported $30 billion effort that comprises the Administration's Comprehensive National Cybersecurity Initiative (CNCI) is appropriately focused, and will DHS's centerpiece "EINSTEIN" program provide effective and lasting security? If not, what are the best alternatives to this investment and focus area? And perhaps more importantly, how do we do a better job at measuring cybersecurity so we can more systematically evaluate technology and policy options?

The largest outstanding questions, however, revolve around the nature of the relationship between the government and the private sector in efforts to secure non-government systems. Stakeholders on all sides place a great deal of emphasis placed on strengthening "public-private partnerships" to secure "critical infrastructure," but beyond the well established goals of improving information sharing and policy dialogue, the precise features of the desired "partnerships"—as well as the scope of what constitutes "critical infrastructure"—have remained largely undefined. Does this entail a new regulatory regime at DHS or NIST, new liability protections or incentives for private sector actors, or some combination thereof? Are there other innovative "partnership" models that should be explored?

These are all weighty questions that will not be answered at this hearing or in the immediate future, but I believe they require the careful attention of Congress going forward as we consider legislative options to improve network security.

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

Chair WU. Thank you, Mr. Smith. And as you all probably noticed from the bells, votes have been called. This will be a substan-

tial series of votes. I want to apologize to the witnesses and all the participants here for the inconvenience, but I just want to note that these votes are called without consideration for any of the individual Members and rarely of any individual Committee. But what I intend to do is proceed to introduce the witnesses, and we may be able to get through the testimony of one or two witnesses before Mr. Smith and I and the other Members who come here will have to leave to vote, and then we will recess this hearing until after the last vote at which time we will reconvene and finish the testimony and proceed to questions.

[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 be discussing the cybersecurity efforts of the Department of Homeland Security (DHS) and the National Institute of Standards and Technology (NIST).

Specifically, we will be learning more from the private sector on how federal cybersecurity activities can enhance privately-owned critical infrastructure, better monitor federal networks, and more clearly define cybersecurity performance with metrics and success criteria.

I look forward to hearing more from our witnesses on how the Federal Government can partner with the private sector to guarantee an effective and secure cyberspace policy.

I yield back.

Chair WU. And with that, it is my pleasure to introduce our witnesses. Mr. Greg Wilshusen is the Director of Information Security Issues at the Government Accountability Office (GAO). Mr. Mark Bregman is the Executive Vice President and Chief Technology Officer of Symantec Corporation. Mr. Scott Charney is the Corporate Vice President of Microsoft's Trustworthy Computer Group, and Mr. Harper is the Director of Information Policy Studies at the Cato Institute.

You each will have five minutes for your spoken testimony. Your written testimony will be included in the record in its entirety. And when you complete all of your testimony, we will start with questions. At that point, each Member will have five minutes to ask questions.

Mr. Wilshusen, please proceed.

STATEMENT OF MR. GREGORY C. WILSHUSEN, DIRECTOR, INFORMATION SECURITY ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Mr. WILSHUSEN. Chair Wu, Ranking Member Smith, thank you for the opportunity to testify at today's hearing on the cybersecurity activities performed by the Department of Homeland Security and the National Institute of Standards and Technology.

Federal laws and policy have assigned important roles and responsibilities to DHS and NIST with securing computer systems and networks. DHS is charged with coordinating the protection of cyber-critical infrastructures, much of which is owned by the private sector, and securing its own computer systems, while NIST is responsible for developing standards and guidelines for implementing security controls over computer systems and information.

Today I will describe cybersecurity efforts at DHS and NIST, including partnership activities with the private sector and the use of cybersecurity performance metrics in the Federal Government.

Over the past three years, GAO has consistently reported that DHS has yet to fully satisfy its key responsibilities, including those for coordinating and protection of cyber-critical infrastructures in serving as the primary federal focal point for cybersecurity efforts. While the department has achieved some successes, shortcomings exist in key areas including bolstering cyber analysis and warning capabilities, improving the security of infrastructure control systems, strengthening its ability to help facilitate recovery from Internet disruptions, reducing organizational inefficiencies, completing actions identified during cyber exercises, and securing internal information systems.

We have made about 90 recommendations to assist DHS in addressing these shortcomings. The department has implemented some of our recommendations but still has not fully satisfied most of them and thus needs to take further action to address these areas.

Pursuant to its responsibilities under the *Federal Information Security Management Act*, or FISMA, NIST has developed a suite of mandatory standards and guidelines that are intended to assist agencies in developing and implementing information security programs and in managing risk to agency operations and assets. In addition, NIST has worked with both public- and private-sector entities to enhance its cybersecurity products. The resulting guidance and tools provided by NIST serve as important resources that federal agencies can apply to their information security programs.

Mr. Chair, as the old adage goes, what gets measured gets done, and so it is with the security measures that agencies use to report on their progress implementing the requirements of FISMA.

According to the performance metrics established by the Office of Management and Budget (OMB), agencies generally reported increasing compliance in implementing key cybersecurity control activities. However, GAO and agency IGs (Inspector Generals) continue to report significant weaknesses in controls. This dichotomy exists in part because the OMB-defined metrics generally measure whether or not a control activity has been implemented, not how well it has been implemented. As a result, reported metrics may not provide a complete picture of the agency's cybersecurity posture. Providing information on the effectiveness of controls and processes could further enhance the usefulness of the data for management and oversight of agency information security programs.

In summary, Mr. Chair, DHS has not fully satisfied its cybersecurity responsibilities and needs to take further action to address shortcomings in several areas, including its efforts to coordinate with the private sector to ensure protection of our nation's cyber-critical infrastructures. NIST has developed a significant number of standards and guidelines for information security and continues to assist organizations in implementing security controls, and while NIST's role is to develop guidance, it remains the responsibility of federal agencies to effectively implement and sustain security over their systems. Developing and using metrics that measure how well agencies implement important controls can con-

tribute to increased focus on the effective implementation of federal information security.

Mr. Chair, this concludes my opening statement, and I would be happy to answer questions at the appropriate time.

[The prepared statement of Mr. Wilshusen follows:]

PREPARED STATEMENT OF GREGORY C. WILSHUSEN

Chairman Wu and Members of the Subcommittee:

Thank you for the opportunity to participate in today's hearing on computer-based (cyber) security activities at the Department of Homeland Security (DHS) and the National Institute of Standards and Technology (NIST). Cyber security is a critical consideration for any organization that depends on information systems and computer networks to carry out its mission or business. The need for a vigilant approach to cyber security has been demonstrated by the pervasive and sustained cyber attacks against the United States and others that continue to pose significant risks to computer systems and networks and the operations and critical infrastructures that they support.

In my testimony today, I will describe cyber security activities at DHS and NIST, including those activities related to establishing public/private partnerships with the owners of critical infrastructure. In addition, I will discuss the use of cyber security-related metrics in the Federal Government. In preparing for this testimony, we relied on our previous reports on federal information security and on DHS's efforts to fulfill its national cyber security responsibilities. We also relied on a draft report of our review of agencies' implementation of the *Federal Information Security Management Act* (FISMA).[1] These reports contain detailed overviews of the scope of our work and the methodology we used.

The work on which this testimony is based was performed in accordance with generally accepted government auditing standards. Those standards require that we plan and perform audits to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

As computer technology has advanced, federal agencies have become dependent on computerized information systems to carry out their operations and to process, maintain, and report essential information. Virtually all federal operations are supported by computer systems and electronic data, and agencies would find it difficult, if not impossible, to carry out their missions, deliver services to the public, and account for their resources without these cyber assets. Information security is thus especially important for federal agencies to ensure the confidentiality, integrity, and availability of their systems and data. Conversely, ineffective information security controls can result in significant risk to a broad array of government operations and assets, as the following examples illustrate:

- Computer resources could be used for unauthorized purposes or to launch attacks on other computer systems.
- Sensitive information, such as personally identifiable information, intellectual property, and proprietary business information could be inappropriately disclosed, browsed, or copied for purposes of identity theft, espionage, or other types of crime.
- Critical operations, such as those supporting critical infrastructure, national defense, and emergency services, could be disrupted.
- Data could be added, modified, or deleted for purposes of fraud, subterfuge, or disruption.

Government officials are increasingly concerned about attacks from individuals and groups with malicious intent, such as criminals, terrorists, and adversarial foreign nations. For example, in February 2009, the Director of National Intelligence

[1] FISMA was enacted as title III, *E-Government Act of 2002,* Pub. L. No. 107–347, 116 Stat. 2899, 2946 (Dec. 17, 2002). It permanently authorized and strengthened information security program, evaluation, and annual reporting requirements for federal agencies. The act also assigns specific responsibilities to agency heads and chief information officers, NIST, and the Office of Management and Budget (OMB).

testified that foreign nations and criminals have targeted government and private sector networks to gain a competitive advantage and potentially disrupt or destroy them, and that terrorist groups have expressed a desire to use cyber attacks as a means to target the United States.[2] The growing connectivity between information systems, the Internet, and other infrastructures creates opportunities for attackers to disrupt telecommunications, electrical power, and other critical infrastructures. As government, private sector, and personal activities continue to move to networked operations, digital systems add ever more capabilities, wireless systems become more ubiquitous, and the design, manufacture, and service of information technology have moved overseas, the threat will continue to grow.

DHS Is a Focal Point for National Cyber Security Efforts

Federal law and policy[3] establish DHS as the focal point for efforts to protect our nation's computer-reliant critical infrastructures[4]—a practice known as cyber critical infrastructure protection, or cyber CIP. In this capacity, the department has multiple cyber security-related roles and responsibilities. In 2005, we identified, and reported on, 13 key cyber security responsibilities.[5] They include, among others, (1) developing a comprehensive national plan for CIP, including cyber security; (2) developing partnerships and coordinating with other federal agencies, State and local governments, and the private sector; (3) developing and enhancing national cyber analysis and warning capabilities; (4) providing and coordinating incident response and recovery planning, including conducting incident response exercises; and (5) identifying, assessing, and supporting efforts to reduce cyber threats and vulnerabilities, including those associated with infrastructure control systems.[6] Within DHS, the National Protection and Programs Directorate has primary responsibility for assuring the security, resiliency, and reliability of the Nation's cyber and communications infrastructure.

DHS is also responsible for securing its own computer networks, systems, and information. FISMA requires the department to develop and implement an agency-wide information security program to provide security for the information and information systems that support the operations and assets of the agency. Within DHS, the Chief Information Officer is responsible for ensuring departmental compliance with federal information security requirements.

NIST Is Responsible for Establishing Federal Standards and Guidance for Information Security

FISMA tasks NIST—a component within the Department of Commerce—with responsibility for developing standards and guidelines, including minimum requirements, for (1) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of the agency and (2) providing adequate information security for all agency operations and assets, except for national security systems. The Act specifically required NIST to develop, for systems other than national security systems, (1) standards to be used by all agencies to categorize all their information and information systems based on the objectives of providing appropriate levels of information security, according to a range of risk levels; (2) guidelines recommending the types of information and information systems to be included in each category; and (3) minimum information security requirements for information and information systems in each category. NIST also is required to de-

---

[2] Statement of the Director of National Intelligence before the Senate Select Committee on Intelligence, *Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence* (Feb. 12, 2009).

[3] These include the *Homeland Security Act of 2002,* Homeland Security Presidential Directive-7, and the *National Strategy to Secure Cyberspace.*

[4] Critical infrastructures are systems and assets, whether physical or virtual, so vital to nations that their incapacity or destruction would have a debilitating impact on national security, national economic security, national public health or safety, or any combination of those matters. Federal policy established 18 critical infrastructure sectors: agriculture and food, banking and finance, chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, government facilities, information technology, national monuments and icons, nuclear reactors, materials and waste, postal and shipping, public health and health care, transportation systems, and water.

[5] GAO, *Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities,* GAO–05–434 (Washington, D.C.: May 26, 2005) and *Critical Infrastructure Protection: Challenges in Addressing Cybersecurity,* GAO–05–827T (Washington, D.C.: July 19, 2005).

[6] Control systems are computer-based systems that perform vital functions in many of our nation's critical infrastructures, including electric power generation, transmission, and distribution; oil and gas refining and pipelines; water treatment and distribution; chemical production and processing; railroads and mass transit; and manufacturing.

velop a definition of and guidelines for detection and handling of information security incidents as well as guidelines developed in conjunction with the Department of Defense and the National Security Agency for identifying an information system as a national security system. Within NIST, the Computer Security Division of the Information Technology Laboratory is responsible for developing information security-related standards and guidelines.

FISMA also requires NIST to take other actions that include:

- conducting research, as needed, to determine the nature and extent of information security vulnerabilities and techniques for providing cost-effective information security;
- developing and periodically revising performance indicators and measures for agency information security policies and practices;
- evaluating private sector information security policies and practices and commercially available information technologies, to assess potential application by agencies to strengthen information security; and
- assisting the private sector, in using and applying the results of its activities required by FISMA.

In addition, the *Cyber Security Research and Development Act*[7] required NIST to develop checklists to minimize the security risks for each hardware or software system that is, or likely to become, widely used within the Federal Government.

Metrics Established to Evaluate Information Security Programs

FISMA also requires the Office of Management and Budget (OMB) to develop policies, principles, standards, and guidelines on information security and to report annually to Congress on agency compliance with the requirements of the Act. OMB has provided instructions to federal agencies and their inspectors general for preparing annual FISMA reports. These instructions focus on metrics related to the performance of key control activities such as developing a complete inventory of major information systems, providing security training to personnel, testing and evaluating security controls, testing contingency plans, and certifying and accrediting systems. FISMA reporting provides valuable information on the status and progress of agency efforts to implement effective security management programs.

Recent Efforts to Improve National Cyber Security Strategy

Because the threats to federal information systems and critical infrastructure have persisted and grown, President Bush in January 2008 began to implement a series of initiatives—commonly referred to as the Comprehensive National Cybersecurity Initiative aimed primarily at improving DHS's and other federal agencies' efforts to protect against intrusion attempts and anticipate future threats.[8] Since then, President Obama (in February 2009) directed the National Security Council and Homeland Security Council to conduct a comprehensive review to assess the United States' cyber security-related policies and structures. The resulting report, *"Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure,"* recommended, among other things, appointing an official in the White House to coordinate the Nation's cyber security policies and activities, creating a new national cyber security strategy, and developing a framework for cyber research and development.[9] In addition, we testified in March 2009[10] that a panel of experts identified 12 key areas of the national cyber security strategy requiring improvement, such as developing a national strategy that clearly articulates strategic objectives, goals, and priorities; bolstering the public/private partnership; and placing a greater emphasis on cyber security research and development.

DHS Has Yet to Fully Satisfy Its Cyber Security Responsibilities

We have reported since 2005 that DHS has yet to comprehensively satisfy its key responsibilities for protecting computer-reliant critical infrastructures. Our reports included about 90 recommendations that we summarized into key areas, including

---

[7] *Cyber Security Research and Development Act*, Pub. L. No. 107–305, 116 Stat. 2367 (Nov. 27, 2002).

[8] The White House, National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (Washington, D.C.: Jan. 8, 2008).

[9] The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, D.C.: May 29, 2009).

[10] GAO, *National Cybersecurity Strategy: Key Improvements Are Needed To Strengthen the Nation's Posture*, GAO–09–432T (Washington, D.C.: March 10, 2009).

those listed in Table 1, that are essential for DHS to address in order to fully implement its responsibilities. DHS has since developed and implemented certain capabilities to satisfy aspects of its responsibilities, but the department still has not fully implemented our recommendations, and thus further action needs to be taken to address these areas.

Table 1: Key Cybersecurity Areas Reviewed by GAO

1. Bolstering cyber analysis and warning capabilities
2. Improving cybersecurity of infrastructure control systems
3. Strengthening DHS's ability to help recover from Internet disruptions
4. Reducing organizational inefficiencies
5. Completing actions identified during cyber exercises
6. Developing sector-specific plans that fully address all of the cyber-related criteria
7. Securing internal information systems

Source: GAO.

Bolstering Cyber Analysis and Warning Capabilities

In July 2008, we identified[11] that cyber analysis and warning capabilities included (1) monitoring network activity to detect anomalies, (2) analyzing information and investigating anomalies to determine whether they are threats, (3) warning appropriate officials with timely and actionable threat and mitigation information, and (4) responding to the threat. These four capabilities are comprised of 15 key attributes, including establishing a baseline understanding of the Nation's critical network assets and integrating analysis work into predictive analyses of broader implications or potential future attacks.

We concluded that while DHS's United States Computer Emergency Readiness Team (US–CERT) demonstrated aspects of each of the key attributes, it did not fully incorporate all of them. For example, as part of its monitoring, US–CERT obtained information from numerous external information sources; however, it had not established a baseline of the Nation's critical network assets and operations. In addition, while it investigated whether identified anomalies constituted actual cyber threats or attacks as part of its analysis, it did not integrate its work into predictive analyses of broader implications or potential future attacks, nor did it have the analytical or technical resources to analyze multiple, simultaneous cyber incidents. The organization also provided warnings by developing and distributing a wide array of attack and other notifications; however, these notifications were not consistently actionable or timely—i.e., providing the right information to the right persons or groups as early as possible to give them time to take appropriate action. Further, while the team responded to a limited number of affected entities in its efforts to contain and mitigate an attack, recover from damages, and remediate vulnerabilities, it did not possess the resources to handle multiple events across the Nation.

We also concluded that without fully implementing the key attributes, US–CERT did not have the full complement of cyber analysis and warning capabilities essential to effectively perform its national mission. As a result, we made 10 recommendations to the department to address shortfalls associated with the 15 attributes in order to fully establish a national cyber analysis and warning capability. DHS concurred and agreed to implement 9 of our 10 recommendations.

Improving Cyber Security of Infrastructure Control Systems

In a September 2007 report and October 2007 testimony, we reported[12] that DHS was sponsoring multiple control systems security initiatives, including an effort to improve control systems cyber security using vulnerability evaluation and response tools. However, DHS had not established a strategy to coordinate the various control

[11] GAO, *Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability,* GAO–08–588 (Washington, D.C.: July 31, 2008).

[12] GAO, *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain,* GAO–07–1036 (Washington, D.C.: Sept. 10, 2007) and *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain,* GAO–08–119T (Washington, D.C.: Oct. 17, 2007).

systems activities across federal agencies and the private sector, and it did not effectively share information on control system vulnerabilities with the public and private sectors. Accordingly, we recommended that DHS develop a strategy to guide efforts for securing control systems and establish a rapid and secure process for sharing sensitive control system vulnerability information. In response, DHS recently began developing a strategy and a process to share sensitive information.

Strengthening DHS's Ability to Help Recovery from Internet Disruption

We reported and later testified[13] in 2006 that the department had begun a variety of initiatives to fulfill its responsibility for developing an integrated public/private plan for Internet recovery in case of a major disruption. However, we determined that these efforts were not comprehensive or complete. As such, we recommended that DHS implement nine actions to improve the department's ability to facilitate public/private efforts to recover the Internet.

In October 2007, we testified[14] that the department had made progress in implementing our recommendations; however, seven of the nine had not been completed. For example, it revised key plans in coordination with private industry infrastructure stakeholders, coordinated various Internet recovery-related activities, and addressed key challenges to Internet recovery planning. However, it has not, among other things, finalized recovery plans and defined the interdependencies among DHS's various working groups and initiatives. In other words, it has not completed an integrated private/public plan for Internet recovery. As a result, we concluded that the Nation lacked direction from the department on how to respond in such a contingency. We also noted that these incomplete efforts indicated that DHS and the Nation were not fully prepared to respond to a major Internet disruption. To date, an integrated public/private plan for Internet recovery does not exist.

Reducing Organizational Inefficiencies

In June 2008, we reported[15] on the status of DHS's efforts to establish an integrated operations center that it agreed to adopt per recommendations from a DHS-commissioned expert task force. We determined that while DHS had taken the first step towards integrating two operations centers—the National Coordination Center Watch and US–CERT, it had yet to implement the remaining steps, complete a strategic plan, or develop specific tasks and milestones for completing the integration. We concluded that until the two centers were fully integrated, DHS was at risk of being unable to efficiently plan for and respond to disruptions to communications infrastructure and the data and applications that travel on this infrastructure, increasing the probability that communications will be unavailable or limited in times of need. As a result, we recommended that the department complete its strategic plan and define tasks and milestones for completing remaining integration steps so that we are better prepared to provide an integrated response to disruptions to the communications infrastructure. DHS concurred with our first recommendation and stated that it would address the second recommendation as part of finalizing its strategic plan.

Completing Corrective Actions Identified During a Cyber Exercise

In September 2008, we reported[16] on a major DHS-coordinated cyber attack exercise called Cyber Storm, which occurred in 2006 and included large-scale simulations of multiple concurrent attacks involving the Federal Government, states, foreign governments, and private industry. We determined that DHS had identified eight lessons learned from this exercise, such as the need to improve interagency coordination groups and the exercise program. We also concluded that while DHS had demonstrated progress in addressing the lessons learned, more needed to be done. Specifically, while the department completed 42 of the 66 activities identified to address the lessons learned, it identified 16 activities as ongoing and seven as

---

[13] GAO, *Internet Infrastructure: Challenges in Developing a Public/Private Recovery Plan*, GAO–06–863T (Washington, D.C.: July 28, 2006); and *Internet Infrastructure: DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan*, GAO–06–672 (Washington, D.C.: June 16, 2006).

[14] GAO, *Internet Infrastructure: Challenges in Developing a Public/Private Recovery Plan*, GAO–08–212T (Washington, D.C.: Oct. 23, 2007).

[15] GAO, *Critical Infrastructure Protection: Further Efforts Needed to Integrate Planning for and Response to Disruption on Converged Voice and Data Networks*, GAO–08–607 (Washington, D.C.: June 26, 2008).

[16] GAO, *Critical Infrastructure Protection: DHS Needs To Fully Address Lessons Learned from Its First Cyber Storm Exercise*, GAO–08–825 (Washington, D.C.: Sept. 9, 2008).

planned for the future.[17] In addition, DHS provided no timetable for the completion dates of the ongoing activities. We noted that until DHS scheduled and completed its remaining activities, it was at risk of conducting subsequent exercises that repeated the lessons learned during the first exercise. Consequently, we recommended that DHS schedule and complete the identified corrective activities so that its cyber exercises can help both public and private sector participants coordinate their responses to significant cyber incidents. DHS agreed with the recommendation. To date, DHS has continued to make progress in completing some identified activities but has yet to do so for others.

Developing Sector Specific Plans that Fully Address All of the Cyber-Related Criteria

In 2007, we reported and testified[18] on the cyber security aspects of CIP plans for 17 critical infrastructure sectors, referred to as sector-specific plans. Lead federal agencies, referred to as sector-specific agencies, are responsible for coordinating critical infrastructure protection efforts with the public and private stakeholders in their respective sectors. DHS guidance requires each of the sector-specific agencies to develop plans to address how the sectors' stakeholders would implement the national plan and how they would improve the security of their assets, systems, networks, and functions.

We determined that none of the plans fully addressed the 30 key cyber security-related criteria described in DHS guidance. Further, while several sectors' plans fully addressed many of the criteria, others were less comprehensive. In addition to the variations in the extent to which the plans covered aspects of cyber security, there was also variance among the plans in the extent to which certain criteria were addressed. Consequently, we recommended[19] that DHS request that the sector-specific agencies, fully address all cyber-related criteria by September 2008 so that stakeholders within the infrastructure sectors will effectively identify, prioritize, and protect the cyber aspects of their CIP efforts. We are currently reviewing the progress made in the sector specific plans.

We testified in March 2009[20] regarding the need to bolster public/private partnerships associated with cyber CIP. According to panel members, there are not adequate economic and other incentives (i.e., a value proposition) for greater investment and partnering with owners and operators of critical cyber assets and functions. Accordingly, panelists stated that the Federal Government should provide valued services (such as offering useful threat or analysis and warning information) or incentives (such as grants or tax reductions) to encourage action by and effective partnerships with the private sector. They also suggested that public and private sector entities use means such as cost-benefit analyses to ensure the efficient use of limited cyber security-related resources. We are also currently initiating a review of the status of the public/private partnerships in cyber CIP.

Securing Internal Information Systems

Besides weaknesses relating to external cyber security responsibilities, DHS had not secured its own information systems. In July 2007, we reported[21] that DHS systems supporting the US–VISIT program[22] were riddled with significant information security control weaknesses that place sensitive information—including personally identifiable information—at increased risk of unauthorized and possibly undetected disclosure and modification, misuse, and destruction, and place program operations at increased risk of disruption. Weaknesses existed in all control areas and computing device types reviewed. For example, DHS had not implemented controls to effectively prevent, limit, and detect access to computer networks, systems, and information. To illustrate, it had not (1) adequately identified and authenticated users in systems supporting US–VISIT, (2) sufficiently limited access to US–VISIT infor-

---

[17] At that time, DHS reported that one other activity had been completed, but the department was unable to provide evidence demonstrating its completion.

[18] GAO, *Critical Infrastructure Protection: Sector-Specific Plans' Coverage of Key Cyber Security Elements Varies*, GAO–08–64T (Washington D.C.: October 31, 2007) and *Critical Infrastructure Protection: Sector-Specific Plans' Coverage of Key Cyber Security Elements Varies*, GAO–08–113 (Washington D.C.: Oct. 31, 2007).

[19] GAO–08–113.

[20] GAO–09–432T.

[21] GAO, *Information Security: Homeland Security Needs to Immediately Address Significant Weaknesses in Systems Supporting the US–VISIT Program*, GAO–07–870 (Washington, D.C.: July 13, 2007).

[22] The US–VISIT program was established by DHS to record and track the entry and departure of foreign visitors who pass through U.S. ports of entry by air, land, or sea; to verify their identities; and to authenticate their travel documentation.

mation and information systems, and (3) ensured that controls adequately protected external and internal network boundaries. In addition, it had not always ensured that responsibilities for systems development and system production had been sufficiently segregated, and had not consistently maintained secure configurations on the application servers and workstations at a key data center and ports of entry. As a result, intruders, as well as government and contractor employees, could potentially bypass or disable computer access controls and undertake a wide variety of inappropriate or malicious acts. These acts could include tampering with data; browsing sensitive information; using computer resources for inappropriate purposes, such as launching attacks on other organizations; and disrupting or disabling computer-supported operations. According to the department, it has started remediation activities to strengthen security over these systems and implement our recommendations.

In January 2009, we briefed congressional staff on security weaknesses associated with the development of systems supporting the Transportation Security Administration's (TSA) Secure Flight program.[23] Specifically, TSA had not taken sufficient steps to ensure that operational safeguards and substantial security measures were fully implemented to minimize the risk that the systems will be vulnerable to abuse and unauthorized access from hackers and other intruders. For example, TSA had not completed testing and evaluating key security controls, performed disaster recovery tests, or corrected high- and moderate-risk vulnerabilities. Accordingly, we recommended that TSA take steps to complete security testing, mitigate known vulnerabilities, and update key security documentation prior to initial operations. TSA subsequently undertook a number of actions to complete these activities. In May 2009, we concluded that TSA had generally met its requirements related to systems information security and satisfied our recommendations.[24]

NIST Has Developed Important Federal Information Security Standards and Guidelines

NIST has taken steps to address its FISMA-mandated responsibilities by developing a suite of required security standards and guidelines as well as other publications that are intended to assist agencies in developing and implementing information security programs and effectively managing risks to agency operations and assets. In addition to developing specific standards and guidelines, NIST developed a set of activities to help agencies manage a risk-based approach for an effective information security program. These activities are known as the NIST Risk Management Framework. Several special publications support this framework and collectively provide guidance that agencies can apply to their information security programs for selecting the appropriate security controls for information systems—including the minimum controls necessary to protect individuals and the operations and assets of the organization.

NIST has developed and issued the following documents to meet its FISMA mandated responsibilities:

- Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems,* February 2004. This standard addresses NIST's requirement for developing standards for categorizing information and information systems. It requires agencies to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability. The security categories are based on the harm or potential impact to an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization.
- Special Publication 800-60 Volume I, revision 1, *Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories,* August 2008. This guide is to assist Federal Government agencies with categorizing information and information systems. It is intended to help agencies consist-

[23] This briefing contained information on our initial January 2009 assessment and recommendations. TSA, a component of DHS, developed an advanced passenger pre-screening program known as Secure Flight that will allow TSA to match airline passenger information against terrorist watch-list records.

[24] GAO, *Aviation Security: TSA Has Completed Key Activities Associated with Implementing Secure Flight, but Additional Actions Are Needed to Mitigate Risks,* GAO–09–292 (Washington, D.C.: May 13, 2009).

ently map security impact levels to types of (1) information (e.g., privacy, medical, proprietary, financial, investigation); and (2) information systems (e.g., mission critical, mission support, administrative). Furthermore, it is intended to facilitate application of appropriate levels of information security according to a range of levels of impact or consequences that might result from the unauthorized disclosure, modification, or use of the information or information system.

- Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems,* March 2006. This is the second of the mandatory security standards and specifies minimum security requirements for information and information systems supporting the executive agencies of the Federal Government and a risk-based process for selecting the security controls necessary to satisfy the minimum security requirements. Specifically, this standard specifies minimum security requirements for federal information and information systems in 17 security-related areas. Federal agencies are required to meet the minimum security requirements through the use of the security controls in accordance with NIST Special Publication 800–53.
- Special Publication 800–61, revision 1, *Computer Security Incident Handling Guide,* March 2008. This publication is intended to assist organizations in establishing computer security incident response capabilities and handling incidents efficiently and effectively. It provides guidelines for organizing a computer security incident response capability; handling incidents from initial preparation through post-incident lessons learned phase; and handling specific types of incidents, such as denial of service, malicious code, unauthorized access, and inappropriate usage.
- Special Publication 800–59, *Guideline for Identifying an Information System as a National Security System,* August 2003. The purpose of this guide is to assist agencies in determining which, if any, of their systems are national security systems as defined by FISMA and are to be governed by applicable requirements for such systems.
- Special Publication 800–55, *Performance Measurement Guide for Information Security,* July 2008. The purpose of this guide is to assist in the development, selection, and implementation of measures to be used at the information system and program levels. These measures indicate the effectiveness of security controls applied to information systems and supporting information security programs.
- Special Publication 800–30, *Risk Management Guide for Information Technology Systems,* July 2002. This guide provides a foundation for the development of an effective risk management program, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems. It also provides information on the selection of cost-effective security controls that can be used to mitigate risk for the better protection of mission-critical information and the IT systems that process, store, and carry this information.
- Special Publication 800–18, revision 1, *Guide for Developing Security Plans for Federal Information Systems,* February 2006. This guide provides basic information on how to prepare a system security plan and is designed to be adaptable in a variety of organizational structures and used as a reference by those having assigned responsibility for activities related to security planning.

NIST is also in the process of developing, updating, and revising a number of special publications related to information security, including the following:

- Special Publication 800–37, revision 1, *Guide for Security Authorization of Federal Information Systems,* August 2008. This publication is intended to, among other things, support the development of a common security authorization process for federal information systems. According to NIST, the new security authorization process changes the traditional focus from the stovepipe, organization-centric, static-based approaches and provides the capability to more effectively manage information system-related security risks in highly dynamic environments of complex and sophisticated cyber threats, ever increasing system vulnerabilities, and rapidly changing missions. The process is designed to be tightly integrated into enterprise architectures and ongoing system development life cycle processes, promote the concept of near real-time

risk management, and capitalize on current and previous investments in technology, including automated support tools.

- Special Publication 800–39, second public draft, *Managing Risk from Information Systems An Organizational Perspective*, April 2008. The purpose of this publication is to provide guidelines for managing risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation and use of information systems. According to NIST, the risk management concepts described in the publication are intentionally broad-based, with the specific details of assessing risk and employing appropriate risk mitigation strategies provided by supporting NIST security standards and guidelines.
- Special Publication 800–53, revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, June 2009. This publication has been updated from the previous versions to include a standardized set of management, operational, and technical controls intended to provide a common specification language for information security for federal information systems processing, storing, and transmitting both national security and non national security information.
- Draft IR–7502, *The Common Configuration Scoring System (CCSS): Metrics for Software Security Configuration Vulnerabilities.* This publication defines proposed measures for the severity of software security configuration issues and provides equations that can be used to combine the measures into severity scores for each configuration issue.

In addition, NIST has other ongoing and planned activities that are intended to enhance information security programs, processes, and controls. For example, it is supporting the development of a program for credentialing public and private sector organizations to provide security assessment services for federal agencies. To support implementation of the credentialing program and aid security assessments, NIST is participating or will participate in the following initiatives:

- **Training** includes development of training courses, NIST publication quick start guides, and frequently asked questions to establish a common understanding of the standards and guidelines supporting the NIST Risk Management Framework.
- **Product and Services Assurance Assessment** includes defining criteria and guidelines for evaluating products and services used in the implementation of controls outlined in NIST SP 800–53.
- **Support Tools** includes identifying or developing common protocols, programs, reference materials, checklists, and technical guides supporting implementation and assessment of SP 800–53-based security controls in information systems.
- **Mapping initiative** includes identifying common relationships and the mappings of FISMA standards, guidelines, and requirements with International Organization for Standardization (ISO) standards for information security management, quality management, and laboratory testing and accreditation.

These planned efforts include implementing a program for validating security tools.

Other Collaborative Activities Undertaken by NIST

NIST collaborated with a broad constituency—federal and non-federal—to develop documents to assist information security professionals. For example, NIST worked with the Office of the Director of National Intelligence, the Department of Defense, and the Committee on National Security Systems to develop a common process for authorizing federal information systems for operation. This resulted in a major revision to NIST Special Publication 800–37, currently issued as an initial public draft. NIST also collaborated with these organizations on Special Publication 800–53 and Special Publication 800–53A to provide guidelines for selecting and specifying security controls for Federal Government information systems and to help agencies develop plans and procedures for assessing the effectiveness of these controls. NIST also interacted with the DHS to incorporate guidance on safeguards and countermeasures for federal industrial control systems in Special Publication 800–53.

NIST is also working with public and private sector entities to establish specific mappings and relationships between the security standards and guidelines developed by NIST and the ISO and International Electrotechnical Commission Information Security Management System standard. For example, the latest draft of Special

Publication 800–53 introduces a three-part strategy for harmonizing the FISMA security standards and guidelines with international security standards including an updated mapping table for security controls.

NIST also undertook other information security activities, including:

- developing Federal Desktop Core Configuration checklists and
- continuing a program of outreach and awareness through organizations such as the Federal Computer Security Program Managers' Forum and the Federal Information Systems Security Educators' Association.

Through NIST's efforts, agencies have access to additional tools and guidance that can be applied to their information security programs.

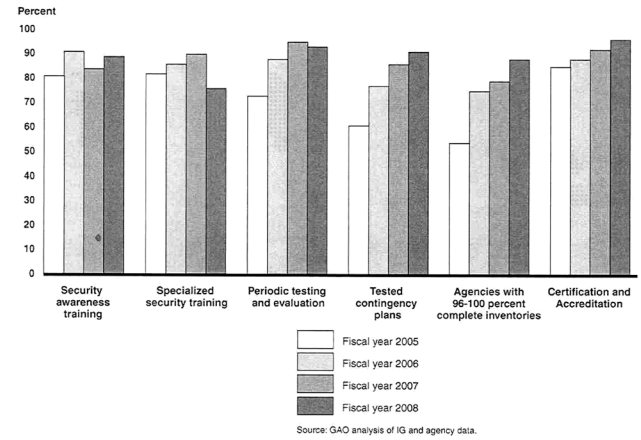
Opportunities for Improving Information Security Metrics

Despite federal agencies reporting increased compliance in implementing key information security control activities for fiscal year 2008, opportunities exist to improve the metrics used in annual reporting. The information security metrics developed by OMB focus on compliance with information security requirements and the implementation of key control activities. OMB requires federal agencies to report on key information security control activities as part of the FISMA-mandated annual report on federal information security. To facilitate the collection and reporting of information from federal agencies, OMB developed a suite of information security metrics, including the following:

- percentage of employees and contractors receiving security awareness training,
- percentage of employees with significant security responsibilities receiving specialized security training,
- percentage of systems tested and evaluated annually,
- percentage of systems with tested contingency plans,
- percentage of agencies with complete inventories of major systems, and
- percentage of systems certified and accredited.

In May 2009, we testified[25] that federal agencies generally reported increased compliance in implementing most of the key information security control activities for fiscal year 2008, as illustrated in Figure 1.

Figure 1: Selected Performance Metrics for Agency Systems



Source: GAO analysis of IG and agency data.

[25] GAO, *Information Security: Agencies Make Progress in Implementation of Requirements, but Significant Weaknesses Persist,* GAO–09–701T (Washington, D.C.: May 19, 2009).

However, reviews at 24 major federal agencies[26] continue to highlight deficiencies in their implementation of information security policies and procedures. For example, in their fiscal year 2008 performance and accountability reports, 20 of 24 major agencies noted that their information system controls over their financial systems and information were either a material weakness or a significant deficiency.[27] In addition, 23 of the 24 agencies did not have adequate controls in place to ensure that only authorized individuals could access or manipulate data on their systems and networks. We also reported that agencies did not consistently (1) identify and authenticate users to prevent unauthorized access; (2) enforce the principle of least privilege to ensure that authorized access was necessary and appropriate; (3) establish sufficient boundary protection mechanisms; (4) apply encryption to protect sensitive data on networks and portable devices; and (5) log, audit, and monitor security-relevant events. Furthermore, those agencies also had weaknesses in their agency-wide information security programs.

An underlying reason for the apparent dichotomy of increased compliance with security requirements and continued deficiencies in security controls is that the metrics defined by OMB and used for annual information security reporting do not generally measure the effectiveness of the controls and processes that are key to implementing an agency-wide security program. Results of our prior and ongoing work indicated that, for example, annual reporting did not always provide information on the quality or effectiveness of the processes agencies use to implement information security controls. Providing information on the effectiveness of controls and processes could further enhance the usefulness of the data for management and oversight of agency information security programs.

In summary, DHS has not fully satisfied aspects of its key cyber security responsibilities, one of which includes its efforts to protect our nation's cyber critical infrastructure and still needs to take further action to address the key areas identified in our recent reports, including enhancing partnerships with the private sector. In addition, although DHS has taken actions to remedy security weaknesses in its Secure Flight program, it still needs to address our remaining recommendations for strengthening controls for systems supporting the US–VISIT program. In taking these actions, DHS can improve its own information security as well as increase its credibility to external parties in providing leadership on cyber security. NIST has developed a significant number of standards and guidelines for information security and continues to assist organizations in implementing security controls over their systems and information. While NIST's role is to develop guidance, it remains the responsibility of federal agencies to effectively implement and sustain sufficient security over their systems. Developing and using metrics that measure how well agencies implement security controls can contribute to increased focus on the effective implementation of federal information security.

Chairman Wu, this concludes my statement. I would be happy to answer questions at the appropriate time.

Acknowledgements

Key contributors to this report include Michael Gilmore (Assistant Director), Charles Vrabel (Assistant Director), Bradley Becker, Larry Crosland, Lee McCracken, and Jayne Wilson.

---

[26] The 24 major departments and agencies are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, Social Security Administration, and U.S. Agency for International Development.

[27] A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected. A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or report financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the entity's financial statements that is more than inconsequential will not be prevented or detected. A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis.

BIOGRAPHY FOR GREGORY C. WILSHUSEN

Gregory Wilshusen is Director of Information Security Issues at GAO, where he leads information security-related studies and audits of the Federal Government. He has over 28 years of auditing, financial management, and information systems experience. Prior to joining GAO in 1997, Mr. Wilshusen held a variety of public and private sector positions. He was a senior systems analyst at the Department of Education. He also served as the Controller for the North Carolina Department of Environment, Health, and Natural Resources, and held senior auditing positions at Irving Burton Associates, Inc. and the U.S. Army Audit Agency. He's a certified public accountant, certified internal auditor, and certified information systems auditor. He holds a B.S. degree in business administration (accounting) from the University of Missouri and an M.S. in information management from George Washington University's School of Engineering and Applied Sciences.

Chair WU. Thank you very much, Mr. Wilshusen. And I think at this point I am going to recess the hearing for both prudential reasons. We have plenty of time to get to the Floor, but also I think this is an important set of topics, and I would hate for any of the Members of Congress or the staff to be watching the clock ticking down, rather than paying attention to these very, very important topics.

So at this point we will adjourn until after the last vote. I am sorry, we will recess until after the last vote in this series of votes.

[Recess.]

Chair WU. This hearing will come back to order. I thank everyone for their forbearance.

Mr. Bregman, please proceed.

STATEMENT OF MR. MARK BREGMAN, EXECUTIVE VICE PRESIDENT AND CHIEF TECHNOLOGY OFFICER, SYMANTEC CORPORATION

Mr. BREGMAN. Chair Wu, Ranking Member Smith, Members of the Committee, good afternoon, and thank you for the opportunity to testify today on cybersecurity efforts at NIST and DHS.

As a global information security leader, Symantec protects more people from on-line threats than anyone in the world by assuring the security, availability and integrity of their information. We are headquartered in California, and are the fourth largest software company with operations in 40 countries. We employ over 18,000 people, including several of which are located in the Chair's district in Beaverton, and I want to thank you for your support there.

Symantec releases an annual Internet Security Threat Report which is a comprehensive analysis of information security threat activity that analyzes network-based threats on consumers and business. We compile the data via our global intelligence network which consists of over 40,000 sensors monitoring computer activity in 180 countries. So in short, if there is a class of threat on the Internet, we're aware of it.

This year's report found that while vulnerabilities continue to increase dramatically, the scope and size and sophistication of cyber attacks is also growing dramatically. They are becoming much more targeted and more dangerous to our nation's critical infrastructure and our economic security.

The most common type of attack during this period targeting our government's critical infrastructure was denial of service attacks, accounting for about half of the top-ten threats in 2008. Denial of service attacks are a threat to the government and critical infra-

structure since the purpose of such attacks is to disrupt the availability of high-profile web sites and other network services and render them inaccessible to users and employees.

These kinds of attacks are often associated with political protests and were used to disrupt the Estonian government web sites in 2007 as well as the Georgian government web sites that were rendered inaccessible during the Georgia-Russia conflict in 2008. But denial of service attacks are just one type of cyber threat that affects government and critical infrastructure.

As the 60-day cyber review rightly points out, cybersecurity risks pose some of the most serious economic and national security challenges of the 21st century, and we applaud the President's commitment to take action on cybersecurity. We hope that the coordinator will be elevated within the White House to have the appropriate decision-making and budget authority that is necessary to set strategic direction for the Nation, to empower our government agencies and private sector to do their mission in a coordinated and balanced way, and take a more prominent role in international cyber policy.

Cybersecurity isn't a civilian or military problem or even a government problem. It is a universal problem. All networks, military, government, civilian and commercial are based on the same computers, same networking hardware technologies, same Internet protocols, many of the same software packages. We are all the target of the same attack tools and tactics. In addition, since most of the Nation's critical IT infrastructure is in commercial hands, hackers consistently go after both military and civilian targets.

We all have the same security challenges, so solutions must be shared. I want to underscore today that cybersecurity is a shared government and private-sector responsibility. We need transparent and accountable government processes, as well as cutting-edge government cybersecurity programs to improve security for everybody.

So with that in mind, let me turn to what DHS and NIST's respective roles and responsibilities are or could be in cybersecurity. We have seen a marked improvement in the Department of Homeland Security in their engagement with the private sector. Under the National Infrastructure Protection Plan construct, DHS is the lead department for engaging the IT sector, and Symantec and other private stakeholders, through the Sector Coordinating Councils, have provided input to DHS on a number of the Comprehensive National Cyber Initiative projects. We have been engaged with DHS and several other cyber policy initiatives, including resiliency, incentives, metrics, risk assessment, information sharing, and cyber exercises.

There are few areas in which we believe more can continue to be done by the department and private sector jointly, including establishing a front-line cyber defense, seeking ways to defend against threats to the supply chain, and taking cybersecurity to the next level through workforce education.

In cyberspace, we have a very rich base from the commercial sector. This is quite different from other historic government models for addressing front-line national defense where much of the solution comes from government or the defense industrial base. The U.S. Government could benefit greatly if the private cybersecurity

sector were brought in more consistently to assist in the development of cybersecurity solutions. One example was mentioned earlier where more input from the private sector could be helpful to DHS would be in project EINSTEIN.

Today, the private sector has not been formally asked to participate in DHS's global supply chain initiative, despite the fact that much of the supply chain the government cares about is in the hands of the private sector. If more information is not shared by the government on the threats or risks that government sees, then how can the private sector do more to protect against these threats and risks?

Symantec is a co-founder of SAFECODE, a non-profit organization created for companies to share software assurance and supply chain best practices. We strongly urge the Department of Homeland Security, Department of Defense (DOD), NIST, and other agencies to work closely with SAFECODE and its member companies to work collaboratively in addressing supply chain and software assurance.

DHS has also taken a lead role in education and awareness. For example, it is a sponsor and an active participant in the National Cyber Security Alliance and *staysafeonline.gov*. The purpose of NCSA is to educate consumers, K–12, higher education, and small business on how to protect themselves and their data in cyber infrastructure.

DHS is also working with NCSA and other stakeholders to develop a plan for the development and retention of trained cybersecurity professional workforce within the government, and we certainly support these.

DHS has a role to play in the area of cybersecurity R&D (research and development). We believe that much of the work completed by the S&T (Science and Technology) Directorate is important and that R&D determined to be not commercially viable should be funded by the government. I respectfully ask that the U.S. Government engage with the private sector more on the R&D collectively to collaborate on common problems.

Given this committee's jurisdiction, I would like to comment on NIST's mission on cybersecurity. It is very important through the promotion of national standards, in particular the work NIST does with federal agencies, industries and academia, to research, develop and deploy information security standards and technologies is critical. As these standards become more important, NIST's role and responsibility will continue to grow, and with that we believe NIST's funding level is not adequate and should be increased.

NIST has played a leading role in the development of FISMA guidelines and federal information processing standards, and as Congress looks to reform FISMA, we will look to NIST for appropriate guidance and standards.

Symantec has worked closely with NIST on Common Criteria for several years, and we fully support Common Criteria because it offers many advantages, including international certification framework for products. As the lead technical standards organization for the Federal Government, NIST has a critical role to play in revising the protection profiles and improving Common Criteria, and we ask that NIST become an active member of NIAP (National Infor-

mation Assurance Partnership) again and would like to see them play an even more active role in other international consensus standard bodies and organizations.

NIST has contributed to raising the quality of federal information security by promoting operational norms and by helping agencies to find model security processes. Experience shows that federal standards aligned with established commercial practices generally succeed, whereas unique government-only standards, such as the Government Open Systems Interconnection Profile, have achieved poor results.

Whether rigid or flexible, standards must be appropriate for the activities being regulated. They must be mindful of the market drivers. Credible federal mandates must strike a balance between ideal and practical standards, including setting reasonable expectations for compliance in the huge base of installed federal systems. NIST's guidelines strike a balance between general rules of thumb for all agencies and local knowledge and expertise of on-the-ground federal officials. However, fixed, inflexible process standards can't easily accommodate these situations.

So in summary, the constantly changing cyber threat landscape and its reliance on human activity, coupled with rapidly changing technology, makes it essential that security doctrine remains flexible.

I strongly recommend that NIST also engage with the private sector to include development of an independent supply chain verification process that will allow us to validate software integrity, focusing more on how technology is developed and less on where it is developed globally. The near-term action plan within the President's cyber review requires establishment of cybersecurity performance metrics, and this is another area that is ripe with opportunity, and we believe NIST should be a key driver of this activity, working with the private sector and other agencies.

In addition to cybersecurity metrics, NIST should consider collaborating more with the private sector and other areas such as cloud computing architecture and standards, SCAP (Security Content Automation Protocol) and other data taxonomy standards, health IT, and Smart Grid architecture with security standards built in from the beginning.

We also want to stress the importance of NIST working with private sector to ensure the agreed-upon standards, protocols, and requirements are rolled out with reasonable timelines and milestones to meet realistic commercial product development roadmaps.

In conclusion, we believe that both the Department of Homeland Security and NIST have done much to carry the cyber torch forward in many areas. However, there is much work still to be done and much more collaboration that needs to take place with the private sector. We stand committed to working with the Administration and Congress to improve cybersecurity, and I would like to thank you, Chair Wu, for allowing me the opportunity to testify before the distinguished Members of this committee.

[The prepared statement of Mr. Bregman follows:]

PREPARED STATEMENT OF MARK BREGMAN

Good afternoon, Chairman Wu, Ranking Member Smith, and Members of the Subcommittee on Technology and Innovation. Thank you for the opportunity to speak about cyber security activities at NIST and DHS.

I come before you today as Chief Technology Officer of Symantec Corporation, the global leader in providing information security solutions. We protect consumers and businesses by assuring the security, availability and integrity of their information. Headquartered in Cupertino, California, Symantec is the world's fourth largest software company with operations in more than 40 countries and over 18,000 employees.

In April, Symantec released our *Internet Security Threat Report* which is widely acknowledged to be the most comprehensive analysis of information security activity for today's economy. The *Report* includes an analysis of network based attacks including those on small businesses with a review of known threats, vulnerabilities, and security risks. Symantec has provided this report since 2002.

This year's report showed that the cyber attacks are growing in size, scope and sophistication. They are becoming more targeted and more dangerous to our critical infrastructure on which our economy depends. Vulnerabilities also continue to increase dramatically.

The most common type of attack this period targeting government and critical infrastructure organizations was denial-of-service attacks, accounting for 49 percent of the top 10 in 2008. Denial of Service (DoS) attacks are a threat to government and critical infrastructures since the purpose of such attacks is to disrupt the availability of high-profile web sites or other network services and make them inaccessible to users and employees. This could result in the disruption of internal and external communications, making it practically impossible for employees and users to access potentially critical information. Because these attacks often receive greater exposure than those that take a single user off-line, especially for high-profile government web sites, they could also result in damage to the organization's reputation. A successful DoS attack on a government network could also severely undermine confidence in government competence, and impair the defense and protection of government networks.

DoS attacks can often be associated with political protests, since they are intended to render a site inaccessible in the same way that a physical protest attempts to block access to a service or location. They can also be associated with conflict whereby one country may attempt to block Web traffic or take web sites off-line. As such, the high percentage of DoS attacks may be an attempt to express disagreement with targeted organization or countries. Examples of these types of attacks targeting governments were the DoS attacks that disrupted and took Estonian governmental web sites off-line in 2007 and the Georgia government web sites that were rendered inaccessible during the Georgia-Russia conflict in 2008.

SMTP, or simple mail transfer protocol, is designed to facilitate the delivery of e-mail messages across the Internet. E-mail servers using SMTP as a service are likely targeted by attackers because external access is required to deliver e-mail. In addition to illegally accessing networks, attackers who compromise e-mail servers may also be attempting to use the e-mail servers to send spam or harvest e-mail addresses for targeted phishing attacks. Because spam can often consume high quantities of unauthorized network bandwidth, these e-mails can disrupt or overwhelm e-mail services, which could result in DoS conditions. Successful SMTP attacks against government and critical infrastructure organizations could also allow attackers to spoof official government communications and obtain credentials in order to launch further attacks. These organizations heavily rely on e-mail as a communication method and as such, it is essential that e-mail traffic be secured. This is just one example of the type of threat affecting government and critical infrastructure sectors in cyberspace today.

As the President so eloquently articulated in May when he released the 60 day cyber review,

> "The globally-interconnected digital information and communications infrastructure known as "cyberspace" underpins almost every facet of modern society and provides critical support for the U.S. economy, civil infrastructure, public safety and national security." The report goes on to say "Cyber security risks pose some of the most serious economic and national security challenges of the 21st century."

We applaud the President's personal commitment to take the action that is so desperately needed around cyber security and look forward to working soon with the new cyber security coordinator, other agencies and stakeholders to develop the strat-

egy, policies, and operational plans necessary to improve cyber security. We hope that the coordinator will be elevated within the White House and have the appropriate policy, decision-making and budget review authorities necessary to set the strategic direction for the Nation, empower agencies and the private sector to do their mission in a coordinated and balanced way, and take a more prominent role in international cyber policy.

Cyber Security: A Shared Public and Private Sector Responsibility

Cyber security isn't a civilian or military problem, or even a government problem—it's a universal problem. All networks, military, government, civilian and commercial, use the same computers, the same networking hardware, the same Internet protocols and the same software packages. We all are the targets of the same attack tools and tactics. It's not even that government targets are somehow even more differentiated; these days, most of our nation's critical IT infrastructure is in commercial hands. Government-sponsored or civilian hackers go after both military and civilian targets.

GAO reports indicate that government problems include insufficient access controls, a lack of encryption where necessary, poor network management, failure to install patches, inadequate audit procedures, and incomplete or ineffective information security programs. These aren't top security issues; these are the same managerial problems that every corporate CIO wrestles with.

We all have the same information security challenges, so solutions must be shared. If the government has any innovative ideas to solve its cyber security problems, certainly a lot of us could benefit from those solutions. In addition, we need transparent and accountable government processes, using commercial security products. Finally, we also need government cyber security programs that improve security for everyone.

Now, I will keep the remainder of my comments focused on what DHS and NIST's respective roles and responsibilities are or should be in cyberspace.

DHS' Cyber Roles and Responsibilities

Let me start with the Department of Homeland Security or "DHS." Under the National Infrastructure Protection Plan construct, DHS is the lead department for engaging with the IT Sector. In addition to the 60-day roll-out, there has been a lot of talk regarding the "Comprehensive National Cyber Initiative" or "CNCI." Symantec and other private sector stakeholders, through the Sector Coordinating Councils, have been able to participate and provide input into DHS on a number of the Initiative's projects, including Project 12 regarding public-private partnerships, Project 4 on leap ahead technologies, and Project 10 on deterrence and the need for global norms of behavior in cyberspace. The private sector and DHS have been in engaged in a number of other projects and activities to address a myriad of cyber policy issues, including resiliency, incentives, metrics, risk assessments, information sharing, and cyber exercises just to name a few. We have seen a marked improvement over the last couple of years by the DHS and their engagement with the private sector.

There are a few areas we believe more can be done by the Department of Homeland Security and private sector jointly. As you heard from Dr. Fonash last week, there are three areas in which DHS has focused their priorities around CNCI: Establishing a front line of defense, seeking ways to defend against a full spectrum of threats through supply chain and intelligence, and taking cyber security to the next level through workforce education.

1) *Front Line of Defense:* In cyberspace we have a very rich, traditional base from the commercial sector very different from other historical government models for addressing national security issues where much of the solutions come from government or defense contractors. With that in mind, it could benefit the U.S. Government greatly if the private sector were brought in more consistently to assist in the development of cyber security solutions to address projects and other key cyber challenges. We would like to see more collaboration between the public and private sector on these programs so that the government can learn about what technologies may be more applicable now to address today or tomorrow's threats. One example of where more input from the private sector could be helpful is Project EINSTEIN. Project EINSTEIN was developed to detect network intrusions and create better situational awareness. However, since its inception a number of years ago, the threats and technologies used to prevent or mitigate against these threats have changed dramatically. No longer is delayed detection of threats and intrusions and delayed simply enough. The need for data prevention technologies and near or real-time sit-

uational awareness capabilities are imperative. We hope the public sector leverages the expertise and technology that the private

2) *Supply Chain:* In last week's hearing, there was a lot of discussion by the government witnesses on the importance of protecting our global supply chain. We heard about the work that the Department of Homeland Security and Department of Defense are undertaking to lead the CNCI Project on this topic. To date, the private sector has not been formally asked to participate in this activity despite the fact that much of the supply chain that government cares about is in the hands of the private sector. We as a company take actions on what we know and the risks we face. However, if more information is not shared by the government on the threats or risks they see, how can we do more to protect against the threats or risks that we have not been informed about? Additionally, we believe that much of the expertise and best practices for protecting supply chain reside within the private sector. Let me give you one example.

Symantec is a co-founder of SAFECODE, a non-profit organization created for companies to share software assurance and supply chain best practices. We strongly urge the Department of Homeland Security, Department of Defense, NIST and other agencies to work closely with SAFECODE and its member companies to work collaboratively in addressing supply chain and software assurance. This collaboration could focus on information sharing of supply chain threats and vulnerabilities and development of best practices and standards.

3) *Education and Awareness:* DHS has taken a lead role in this area. For example, DHS is a sponsor and active participant in the National Cyber Security Alliance (NCSA) and *staysafeonline.gov*. The purpose of NCSA, a 501c3, is to educate consumers, K–12, higher education, and small and medium sized businesses the steps they need to take in order to use the Internet safety and securely, protecting themselves, their data and the cyber infrastructure. The President's 60-day cyber review recognized the good work of the NCSA and highlights the need for formal K–12 education and curriculum to address cyber safety, cyber security and cyber ethics (C3) within schools. NCSA and DHS will be working with other key stakeholders to develop this C3 framework. In addition to a K–12 curriculum framework, NCSA has established a volunteer program (C–SAVE) for computer security professionals to teach cyber security in schools and is working to conduct a small and medium-sized business study to identify current cyber practices, gaps, resource needs, and ways to effectively communicate with this important audience. There are many more activities underway which can be found at *www.staysafeonline.gov*.

4) *Workforce and Training:* In addition to education and awareness responsibilities, DHS is working with several agencies, NCSA and other stakeholders to develop a plan for the development and retention of a trained cyber security professional workforce that can meet the increasing demand and gaps within the government. DHS is also developing a program to retrain the current workforce in the public and private sector to ensure they have the most up-to-date skills and capabilities to address today's technology and cyber security demands. We fully support these activities and believe this appropriate work for DHS to engage in with other interagency partners.

5) *Exercises and National Incident Response Planning:* The 60-day review's near-term action plan calls for "a cyber security incident response plan to enhance public-private partnerships with an eye toward streamlining, aligning, and providing resources to optimize contribution and engagement." We believe that DHS is well positioned to help lead these efforts and ask that the private sector be included early on in the development process.

6) *R&D:* DHS has a role to play in the area of cyber security R&D through the Science and Technology Directorate. The S&T Directorate maps their R&D projects based on the needs of their primary internal customer, the Cyber Security and Communications Directorate. We believe that much of the work completed by the S&T Directorate is very important and believe that increased funding is necessary in order for the S&T Directorate to meet their customers' needs. We also believe that a more formal process of identifying priorities and coordinating with internal customers is necessary. We also believe that DHS writ large, in their capacity as the Government Specific Agency for interacting with the IT and Communications Sectors, must have a formal process of engaging with the private sector on the CNCI R&D Project. It is not surprising that the private sector spends more than the U.S. Government on R&D. It is also not surprising that both the public and private sector have limited resources with which to spend on R&D.

Imagine if we could work together to identify what the collective problems and priorities are for government and industry, determine which of those priorities are commercially viable and therefore should not be funded by government, and identify the gaps and/or redundancies that exist. Those projects which may be redundant can be de-conflicted and re-allocated. Those priorities that are gaps and not determined to be commercially viable could then be funded by government. This process would allow us all to maximize our collective resources to the fullest extent possible and ensure that we are working from a coordinated roadmap and set of priorities. We respectfully ask that the U.S. Government engage with the private sector to the extent possible in this area. Some initial challenges or problem areas for R&D consideration could include: Attribution, Situational Awareness, Early Warning, and ID management.

NIST's Roles and Responsibilities

In addition to DHS' role, NIST's mission in cyber security is very important. Beginning with its founding in 1901 as the National Bureau of Standards, NIST has played a key role in U.S. commerce through promotion of various national standards. In particular, the work NIST does with federal agencies, industry and academia to research, develop and deploy information security standards and technology is critical. As cyber security standards and metrics become increasingly important, NIST's role and responsibility will continue to grow. With that, we believe NIST's funding level is not adequate and should increase so they can meet the community's growing needs and requirements.

FISMA: Since its inception, NIST has played a leading role in the development of FISMA guidelines and Federal Information Processing Standards (FIPS). As Congress looks to reform FISMA, we will look to NIST for appropriate guidance and standards.

Common Criteria/NIAP and other international standards activities: Symantec has been involved with Common Criteria evaluations for several years. In fact, our Symantec Enterprise Firewall was the first product to be certified against the U.S. Government's application firewall protection profile. We currently have several products currently certified. Symantec supports the Common Criteria because it offers many advantages, including an international certification framework for products. Based on the results of evaluations against the Basic and Medium Robustness Protection Profiles and comments from vendors and government customers, NIAP, the U.S. Government implementation arm for Common Criteria, has determined that the current U.S. Protection Profile Robustness model needs to be revised. The original implementation did not create the necessary test plans and documentation needed to achieve consistent results across different products evaluated in different labs. As a result, NSA is creating a Standard Protection Profile, which will replace any corresponding U.S. Government Protection Profile. NSA plans to work with industry, government stakeholders, and the Common Criteria community to create these Protection Profiles. As the lead technical standards organization for the Federal Government, we believe that NIST has a critical role to play in revising the protection profiles and improving Common Criteria. We ask that NIST become an active member of NIAP again and would like to see them play an even more active role in other international consensus standards bodies and organizations.

Flexible NIST Federal Security Standards: NIST has contributed to raising the quality of federal information security by promoting operational norms and by helping agencies to find model security processes. Experience shows that federal standards aligned with established commercial practices generally succeed. However, unique government-only standards, such as the Government Open Systems Interconnection Profile (GOSIP), have achieved poor results.

Whether flexible or rigid, standards must be appropriate for the activities being regulated, and they must be mindful of market drivers and required precision. The precision and specificity in standards vary considerably according to their goals and purposes. For example, some technical standards, such as communications protocols, must be very precise and rigid because of a need for inter-operation among many vendors' products.

Thus, credible federal mandates must strike a balance between ideal and practical standards, including setting realistic expectations for compliance in the huge base of installed federal systems. Additionally, we must remember that compliance will be put in jeopardy if the standards are perceived to be unreasonable or not viable.

First, standards require reliable metrics to enable tracking of compliance. Second, they must be introduced at a specific point in the product life cycle when customers seek standard products and manufacturers are no longer competing on features.

Third, there must be a compelling market benefit supporting use of a standard. Finally, standards must be appropriate for the application being standardized.

NIST's guidelines strike a balance between general rules of thumb for all agencies and the local knowledge and expertise of on-the-ground federal officials. However, fixed, inflexible process standards cannot easily accommodate all of these situations. In summary, the constant changing cyber threat landscape and its high reliance on human activity coupled with the rapid changes in technology make it essential that security doctrine remains flexible.

Metrics: The near-term action plan within the President's cyber review requires the establishment of cyber security performance metrics. This is an area ripe with opportunity and we believe NIST should be a key driver of this activity working with the private sector and other agencies.

In addition to cyber security metrics, there are some areas we believe NIST should consider collaborating more with the private sector on, including: Cloud Computing architecture and standards, SCAP and other data taxonomy standards, Supply Chain best practices, Health IT, and Smart Grid architecture with security standards built in. We also want to stress the importance of NIST and OMB working with the private sector to ensure that agreed upon standards, protocols and requirements are rolled out with the reasonable timelines and milestones to meet realistic commercial product development roadmaps.

In conclusion, we believe both the Department of Homeland Security and NIST have done much to carry the cyber torch forward in several areas. However, there is much more work to be done and much more collaboration that needs to take place with the private sector. We stand committed to working with the Administration and Congress to improve cyber security.

Thank you again, Chairman Wu, for allowing me the opportunity to testify before the distinguished Members of the House Science Subcommittee on Technology and Innovation regarding cyber security responsibilities for DHS and NIST. I am happy to answer any questions that any Members of the Committee may have.

BIOGRAPHY FOR MARK BREGMAN

Mark Bregman is Executive Vice President and Chief Technology Officer at Symantec, responsible for the Symantec Research Labs, Symantec Security Response and shared technologies, emerging technologies, architecture and standards, localization and secure coding, and developing the technology strategy for the company. Bregman guides Symantec's investments in advanced research and is responsible for the company's development centers in India and China.

Additionally, Bregman leads the field technical enablement team, which works closely with the technical sales team to ensure they are prepared to assist customers in managing the impact of changing and emerging technical requirements.

Bregman joined Symantec through the company's merger with Veritas Software, where he served as chief technology officer, responsible for cross-product integration, advanced product development, merger and acquisition strategy, and the company's engineering development centers in India and China.

Prior to joining Veritas, Bregman was CEO of Airmedia, a wireless Internet firm.

Previously, Bregman spent 16 years at IBM where he led the RS/6000 and Pervasive Computing divisions and held senior management positions in IBM Research and IBM Japan. He was also technical assistant to IBM CEO Lou Gerstner.

Bregman holds a Bachelor's degree in physics from Harvard College and a Master's degree and doctorate in physics from Columbia University. He is a member of the Visiting Committee to the Harvard University Libraries, a member of the American Physical Society, and a senior member of IEEE. He also serves on the Board of Directors of ShoreTel and the Bay Area Science and Innovation Consortium.

Chair WU. Thank you very much, Mr. Bregman. Mr. Charney, please proceed.

STATEMENT OF MR. SCOTT CHARNEY, CORPORATE VICE PRESIDENT, TRUSTWORTHY COMPUTING, MICROSOFT CORPORATION

Mr. CHARNEY. Thank you, Chair Wu. Thank you, Member Smith, Members of the Subcommittee. Thank you for the opportunity to appear today at this important hearing on cybersecurity.

My name is Scott Charney. I am the Corporate Vice President for Trustworthy Computing at Microsoft. In cyberspace today, we are locked in an escalating and sometimes hidden conflict. Cyber threats have grown in sophistication, expanding from opportunistic viruses and worms that were once disruptive and sometimes damaging to include very targeted, stealthy and persistent attacks. In the information age, any individual can engage in activities formerly limited to nation states, and any nation, regardless of traditional measures of power and sophistication, can gain economic and military advantage through cyber programs. The lack of identity for hardware, software and people on the Internet also makes it difficult to determine the source of an attack. Understanding the sources and the motivations of attacks is essential to ensuring the appropriateness of response. Absent strong attribution abilities which balance security and privacy, international and national strategies to deter cyber attacks will not succeed. Attribution can and must be a top priority to improve cyberspace security moving forward.

The challenge for the government today is that it must balance dual and often interrelated roles to manage cyber threats effectively. The government is responsible for protecting public safety and national security, and it is also responsible for managing a large IT infrastructure. I support the near-term action plan in the recently released White House 60-day review and specifically the action to prepare an updated national strategy to secure the information and communications infrastructure.

Just as we need an updated national strategy to ensure the Nation's cybersecurity, the government must also implement an effective model for managing its own cybersecurity. Such a model would include a centrally managed horizontal security function to provide a foundation of government-wide policy standards and oversight. And because each federal agency has its own mission, customers, partners, and threats, there must also be vertical security functions resident in each agency to ensure that agency-specific missions are accomplished and agency-specific risks are managed appropriately.

Let us turn to the more specific roles for DHS and NIST. The hybrid model I just outlined could be applied more effectively to the federal enterprise. In this implementation, DHS and NIST would provide the horizontal, centrally managed cybersecurity functions, and individual agencies would have vertical functions to manage their unique risks. Simply stated, the Department of Homeland Security should set security control policy articulating minimum cybersecurity baselines, goals, and outcomes. DHS should also develop processes to exchange and foster implementation of best practices so that agencies can more quickly achieve higher levels of security when necessary. NIST should create government-wide standards to help agencies meet the security control policy set by DHS. To realize the value created by analyzing data horizontally, DHS and NIST must have the right data, they must analyze that data, and the data must drive action. This will require enhanced cybersecurity monitoring, audit, and analytics to gain valuable insights on the real-time health of the federal enterprise and enable agile actions to mitigate and respond to incidents.

Agencies should continue to have the responsibility and accountability for creating documented information security programs, assessing their risks, implementing effective management controls, and responding to agency incidents. This is the vertical function in the hybrid model.

In conclusion, as long as threats evolve, so must our efforts to protect against them. Technology alone will not create the trust necessary to security cyberspace. Technological innovation must be aligned with social, political, economic, and IT forces to enable change. Microsoft helps drive and shape these forces with partners in the ecosystem to create a safe and more trusted Internet. The United States must similarly drive forward with a clear vision and holistic information-age strategies to combat threats to national and economic security and to public safety.

Thank you again, Chair Wu, for providing me the opportunity to testify before the distinguished Members of the Subcommittee on Technology and Innovation, and I am happy to answer any questions you may have.

[The prepared statement of Mr. Charney follows:]

PREPARED STATEMENT OF SCOTT CHARNEY

Chairman Wu, Ranking Member Smith, and Members of the Subcommittee, thank you for the opportunity to appear today at this important hearing on cyber security and for entering my written testimony into the record of this committee. My name is Scott Charney, and I am the Corporate Vice President for Trustworthy Computing at Microsoft. I also served as one of four Co-Chairs of the Center for Strategic and International Studies (CSIS) Commission on Cybersecurity for the 44th Presidency. Prior to joining Microsoft, I was Chief of the Computer Crime and Intellectual Property Section in the Criminal Division of the United States (U.S.) Department of Justice. I was involved in nearly every major hacker prosecution in the U.S. from 1991 to 1999; worked on legislative initiatives, such as the *National Information Infrastructure Protection Act* that was enacted in 1996; and chaired the G8 Subgroup on High Tech Crime from its inception in 1996 until I left government service in 1999.

Today I will share a brief assessment of cyberspace security and discuss:

1) Establishing Information Age security strategies for government;
2) Advancing federal civilian enterprise security; and
3) Clarifying roles and enhancing capabilities for the Department of Homeland Security (DHS) and the National Institute of Standards and Technology (NIST).

Cyberspace Security: Understanding the Evolving Threats

We are locked in an escalating and sometimes hidden conflict in cyberspace. The battle of bits and bytes has very real consequences for America, other nations, the private sector, and all other Internet users. Cyber attack joins terrorism and weapons of mass destruction as one of the new, asymmetric threats that puts the U.S. and other governments at risk. Cyber security has improved, but these improvements have not kept pace with the increasing availability and value of data, nor the number or sophistication of cyber attacks. In the Information Age, governments, industries, and consumers around the world rely on globally connected networks and cyber systems, and create and store volumes of sensitive data electronically. Such data, particularly when not well secured, presents an attractive target for those seeking competitive or strategic advantage, or financial gain.

The resulting cybercrime economy is complex, sophisticated, and growing. It has numerous participants, some willing (malware developers) and some unwilling (victims of cyber attacks); some clearly good (security researchers that disclose vulnerabilities responsibly) and some clearly bad (vulnerability traffickers). Over the past decade, attacks that bad actors carry out have also grown in sophistication, expanding from opportunistic viruses and worms that were disruptive and sometimes damaging to very targeted, stealthy, and persistent attacks. In today's evolving cybercrime economy, any individual can engage in activities formerly limited to na-

tion-states, and any nation, regardless of traditional measures of sophistication, can gain economic and military advantage through cyber programs.

When self-replicating computer worms entered the public consciousness several years ago, it was in the form of malware, such as Win32/MSBlast, Win32/Sasser, and Win32/Slammer, that exploited vulnerabilities to spread rapidly and caused system disruption or failure. These threats were highly visible and garnered significant attention. Exploit-based worms, while still a concern, have receded from prominence as Microsoft and other software vendors have reduced the vulnerabilities these worms relied on to spread, and users deployed security technologies meant to thwart these attacks. With the traditional vectors of mass propagation reduced significantly, today's prominent worms rely much more on social engineering techniques to gain access to information technology (IT) environments, like enterprise networks and consumer machines. A gap in the application and oversight of enterprise-wide and consumer security controls, as well as insufficient monitoring and analysis of the real-time health of networks, can create significant risk both nationally and globally.

Today Microsoft tracks more than 30,000 types of malware families and some of these families have millions of variants. There are infections by these variants in machines around the world, but linking an infected machine with the cyber attacker who infected it is very difficult. The lack of identity for hardware, software, data, and people on the Internet makes it difficult to determine the source of attacks, yet knowing the source is essential to ensuring the appropriateness of response. Attribution of cyber attacks is one of the most fundamental challenges facing the international community. Absent strong attribution abilities, international and national strategies to deter cyber attacks will not succeed.

Microsoft has long recognized the growing need to improve software security to counter cyber threats. In 2002, Microsoft changed the way it built software by implementing the Security Development Lifecycle (SDL). The SDL provides customers with high quality, well-engineered and rigorously tested software that helps withstand malicious attacks by requiring threat models to be built at design time and requiring that specific security milestones be met at each stage of the development process. Every Internet-facing or enterprise-class product from Microsoft is required to go through the SDL, resulting in measurable improvements in the security and privacy of Microsoft's software. We also continue to work with partners in the computing ecosystem to help better protect our mutual customers and all Internet users. For example, we are members of the Software Assurance Forum for Excellence in Code (SAFECode)[1] which promotes the advancement of demonstrably effective software assurance methods. These efforts are essential in reducing the attack surface of products. Technology alone, however, will not create the trust necessary to realize the full potential of the Internet. Technological innovation must be aligned with social, political, economic and IT forces to enable change. Working with partners in the ecosystem, Microsoft is advancing End-to-End Trust,[2] driving and shaping these forces to create a safer, more trusted Internet.

What can government do to counter this underground cybercrime economy? First, understanding the nature of cyber threats is critical. Breaking down the complexity of the cyber threat is necessary to inform the useful allocation of resources for defense and to guide more effective risk management. Our defenses must consider the diversity of players, motivations, and methods in the cybercrime economy, and must either raise the costs for adversaries to carry out attacks or decrease the value of successful attacks. Lowering the return on investment for cyber attacks can deter some bad actors or lessen the consequences of attacks that do occur.

Establishing Information Age Security Strategies for Government

Government must balance dual, and often interrelated, roles to effectively manage emerging cyber threats. First, as a public policy entity, the government is responsible for protecting public safety, as well as economic and national security. In this capacity, the United States must develop a national cyberspace strategy to address the full spectrum of significant risks presented by the Information Age. But the Federal Government is also a large and widely distributed enterprise, with countless globally distributed ?customers? (e.g., citizens who want to connect with their government), partners, operations, networks, and resources. Although distinct, the policy and enterprise roles are not entirely separate, as each affects and informs the other.

---

[1] *www.safecode.org;* members include EMC, Juniper, Microsoft Nokia, SAP, and Symantec.
[2] *www.microsoft.com/endtoendtrust*

Architecting a Comprehensive and Coordinated National Strategy

The recently released White House *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* outlined key policy challenges the Nation faces as a result of the dynamic cyber threat landscape.[3] The White House review recognized that:

> *The Federal Government is not organized to address this growing problem effectively now or in the future. Responsibilities for cyber security are distributed across a wide array of federal departments and agencies, many with overlapping authorities, and none with sufficient decision authority to direct actions that deal with often conflicting issues in a consistent way. The government needs to integrate competing interests to derive a holistic vision and plan to address the cyber security-related issues confronting the United States. The Nation needs to develop the policies, processes, people, and technology required to mitigate cyber security-related risks.*

I support the near-term action plan in the review, which includes activities to appoint a lead policy official in the White House, staff a National Security Council Directorate, and prepare an updated national strategy to secure information and communications infrastructure.

This is a significant undertaking that will require continued White House and Congressional leadership. National security strategies create a framework to employ all elements of national power—economic, diplomatic, law enforcement, military, and intelligence. A comprehensive cyberspace security strategy must include these elements and articulate how they will be employed to ensure national security, economic security, and public safety, and to assure delivery of critical services to the American public. In the Industrial Age, power was generally based on physical might; in the Information Age, power is derived from information, knowledge, and communications.

Constructing An Information Age Security Model

Just as we need a new national strategy to ensure the Nation's cyber security, the government must also carefully determine an effective model for managing government-wide cyber security. In this regard, one can view the Federal Government as a large collection of businesses with different missions, partners, customers, data, assets, and risks. There are some responsibilities and practices (e.g., developing information security plans, implementing the Federal Desktop Core Configuration (FDCC)) that should be done by each and every federal agency. The number and diversity of component organizations, functions, and systems, however, means that a fully centralized model for managing security will not work. Each agency has a unique security paradigm with differing threats, so each agency needs to manage its own risk.

If some security controls should be applied uniformly across the government, but other security controls need to be carefully tailored to address an agency's mission and risks, it becomes clear that the government needs to establish a hybrid model for information security that improves security across the federal enterprise and fosters agility to counter ever-changing threats. A hybrid model could create a holistic security framework for managing and reducing the attack surface of the federal enterprise. Such a model would include:

- A centrally managed *horizontal security function* to provide a foundation of government-wide policy, standards, and oversight; as well as
- *Vertical security functions* resident in individual agencies to manage their risks.

This combination of horizontal and vertical functions ensures that minimum security goals and standards are set, yet provides agencies the flexibility to manage risks appropriately for their unique operating environments.

Advancing Federal Civilian Enterprise Security

For more than 25 years, the Federal Government has been struggling to evolve its policy, organizational, and operational information security management frameworks. Over two decades, legislation has been passed that has incrementally established and enhanced authority, organization, and accountability. The three most important elements of the foundation include: the *Paperwork Reduction Act of 1980*,[4] which centralized government-wide responsibilities into the Office of Management

[3] *http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf*
[4] P.L. 96–511, December 11, 1980.

and Budget (OMB); the *Clinger-Cohen Act*,[5] which established dedicated Chief Information Officers for the major departments and agencies across the government; and the *Federal Information Security Management Act* (FISMA),[6] which created the first comprehensive information security framework for the Federal Government. Additionally, OMB mandated implementation of the FDCC by February 2008. The FDCC mandate requires Federal agencies to standardize desktop configurations to meet FDCC requirements and is intended to improve security, reduce costs, and decrease application-compatibility issues. This was an attempt to create government-wide policy and standards, but it lacked the oversight and supporting capabilities to be implemented effectively.

Understanding what exists and conducting periodic tests of controls does not create the strategic and operational information security commensurate with the sophisticated Information Age threats that now confront agencies. Congress should consider how to implement an effective model for managing the security of the federal enterprise, build enhanced cyber security capabilities within the government, and fund agencies appropriately to fulfill their vertical and, in some cases, horizontal responsibilities. There are two basic options I see: coordinated incremental change or comprehensive reform. Incremental change may be more appealing to agencies and the under-resourced individuals responsible for cyber security, but slow change may be inadequate and ineffective to counter evolving threats. Comprehensive reform, however, will substantially challenge the status quo. Such reform would require a sustained commitment of the Executive and Legislative branches to construct an innovative and agile federal enterprise for the Information Age.

Defining Clear Roles for DHS and NIST

The hybrid model I outlined above could be applied more effectively to the federal enterprise to improve security and increase agility. In this implementation, DHS and NIST would provide the horizontal function, and individual agencies would have vertical functions:

- *Horizontal Functions:*
  - *Department of Homeland Security:* DHS should set security control policy, articulating cyber security goals and outcomes. Put another way, DHS should develop "minimum baselines for security" and work with the standards community where appropriate. DHS should also develop processes to exchange and foster implementation of best practices that exceed minimum standards so that agencies can more quickly achieve higher levels of security when necessary to address their own unique agency risks.
  - *National Institute of Standards and Technology:* NIST should create government-wide standards to help agencies meet the security control policy set by DHS. NIST's Special Publication (SP) 800–53, *Recommended Security Controls for Federal Information Systems*[7] is an example of standards created by NIST that apply government-wide. NIST should, like DHS, also help agencies exceed any government-wide minimum standards.
- *Vertical Function in Individual Agencies:* Agencies should continue to have responsibility for—and accountability for—assessing their risks and implementing effective management controls. This includes activities to configure and patch systems, build effective incident response capabilities, identify and detect unauthorized access, test security controls regularly, audit for compliance, and implement security changes based upon testing, auditing, and environment changes. Agencies' risk management should be a continuous cycle of related activities performed as part of a documented information security program.

Clarifying Roles and Enhancing Capabilities for DHS and NIST

To fulfill the horizontal function described above, DHS and NIST need to have clear roles and enhanced capabilities. I will briefly describe some of the successes

[5] P.L. 104–106, February 10, 1996. The law, initially entitled the *Information Technology Management Reform Act* (ITMRA), as subsequently renamed the *Clinger-Cohen Act* in P.L. 104–208, September 30, 1996.

[6] P.L. 107–347, December 17, 2002.

[7] Federal Information Processing Standards (FIPS), including "*Standards for Security Categorization of Federal Information and Information Systems*" and "*Minimum Security Requirements for Federal Information and Information Systems*" also provide guidance.

of and challenges to each of these organizations, and then focus my remarks on how to enhance their capabilities and funding so they may successfully provide the horizontal security function for the federal enterprise.

DHS

DHS is in a state of transition, with changes in vision and leadership underway, so an assessment of its efforts must separate the past from the future.

DHS has partnered well with industry in the IT and Communications Sectors for infrastructure protection and that partnership is producing results. The partnership has advanced both strategic risk management and operational information sharing. For example, industry and government will be releasing shortly the IT Sector Risk Assessment called for in the National Infrastructure Protection Plan. The Risk Assessment outlines several mitigations (e.g., robust coordinated response and out-of-band data delivery) that public and private sector owners and operators can implement to better manage sector-wide risk. DHS is also improving how it facilitates distribution of actionable information (via Critical Infrastructure Information Notices and Federal Information Notices), which enables more timely implementation of security updates and helps to reduce malware infections such as the Conficker worm. This partnership is essential because cyber security is a shared challenge that involves government as well as the owners, operators, and vendors that make cyberspace possible. To date, this partnership does not yet fully extend into the cyber security research and development (R&D) portfolio managed by the DHS Science and Technology Directorate. This gap must be addressed to provide greater awareness of and, where possible, coordination across public and private sector R&D activities.

But DHS has struggled without an actual strategic plan for cyber security. As a result, its efforts have not always focused on the right areas and were not optimized for effectiveness. The lack of a cohesive vision was exacerbated by constant changes in leadership, lack of personnel, and inadequate funding for its mission. The Comprehensive National Cybersecurity Initiative (CNCI) was an important catalyst to drive improvements in DHS. It outlined specific initiatives in key areas, provided greater funding, and enabled more rapid increases in staff. The CNCI, however, still did not provide the coordinated vision that is needed. Moving forward, DHS should develop a strategic vision and look to build on its strengths in partnership, information sharing, and growing security capabilities to function in the horizontal role I outlined above.

NIST

NIST has also contributed significantly to advancements in cyber security, and must continue to do so in the future. The Information Technology Laboratory is an important voice in the cyber security conversation, and its Computer Security Division is doing valuable work, such as creating NIST's cyber guidance and hosting the Information Security Automation Program to automate technical security operations. The Computer Security Division, unfortunately, is not sufficiently resourced to address the growth in its responsibilities and workload.

This growth is proportionate with the continuing pace of technological innovation. For example, NIST is advancing two important initiatives for newer technologies and services that will each have considerable cyber security implications: Securing the SmartGrid and Cloud Computing. In particular, NIST's cloud computing work is focused on the effective and secure use of cloud computing in the government and private sector. As NIST continues to explore cloud computing and cloud security, I would suggest it focus on three areas:

- Utilize a risk-based information security program that assesses and prioritizes security and operational threats;
- Promote regular maintenance and update of security controls that mitigate risk; and
- Support international standards frameworks and certifications that ensure controls are designed appropriately and are operating effectively.

The Computer Security Division should continue to focus on standards, and its resources should be increased to meet those expanding responsibilities. NIST's cyber security efforts will also continue to grow and benefit from increasing the partnership with the private sector, and more specifically, the IT and Communications Sectors. With greater resources, NIST will make a more dramatic impact on the cyber security of the computing ecosystem.

Enhanced Capabilities

DHS and NIST both must build on their successes, overcome challenges, and expand their capabilities to support government-wide policy, standards, and oversight of cyber security. I will outline five core capabilities that I believe should exist as part of a government-wide horizontal function for the federal enterprise. These capabilities must be operationalized in the agencies to meet basic security requirements; however, my discussion below focuses on the government-wide horizontal function provided by NIST and DHS and the enhanced value created by analyzing data across the government infrastructure. NIST should provide the standards to enable these capabilities, and DHS should provide the operational aspect of each.

The growing connectivity of systems, number of devices, and value of information that exists in the federal enterprise means that it is critically important to improve the trustworthiness of connections and transactions to reduce risk. The five capabilities outlined below will provide value in the near-term, but that value will only increase as the federal enterprise develops better ways to ensure that hardware, software and data can be trusted and that those connecting to its networks are who they claim to be and can only do what they are authorized to do. Improving identity and authentication of these elements in the federal enterprise will empower better trust decisions and increase accountability.

Security Monitoring: Watching the real-time health of the networks involves more than traditional network monitoring. In addition to security data from intrusion detection systems, the government could also use information provided by IT assets, such as routers, hosts, and proxy servers, to evaluate its operational and security status. By taking advantage of the general purpose sensors that are built into every well-managed infrastructure, government can gain greater insight on the real-time health of the networks and take action to mitigate risks and respond to incidents.

Audit: Meaningful audit data can improve agencies' cyber security posture because audit drives behavior, and it provides accountability. The audit capabilities I am referring to are more than comprehensive yearly reporting; they include continuous audit, with spot checks and periodic evaluations, as well as quarterly and annual reporting. Quarterly or annual reporting provides a snapshot of overall security posture and trends, while the spot and periodic evaluations can be used to assess the adequacy of controls and compliance to defined requirements.

Advanced Analytics: The large amounts of monitoring and audit data must ultimately be turned into insights that can be used to inform more effective cyber security responses. That response may be operational as discussed below, or it may be more strategic and involve changes in policies, controls, and oversight. It may also be a combination of both, with operational incidents informing longer-term decisions. Either way, for this to happen, government must have the right data, must analyze that data in the context of the federal enterprise, and that data must drive action. Fusing together disparate data from a variety of organizations and systems to create a common operational picture is challenging; building the analytic capabilities (e.g., correlation) to derive valuable insights is even harder. The monitoring and audit capabilities I mentioned earlier would create a baseline of data about the real-time health and overall trends in security across the Federal Government. DHS can combine this with threat information from the Intelligence Community and advanced technical analyses to create an operational awareness of the attack surface of the Federal Government in ways simply not possible in the private sector. This is the power of innovative government analytics—insights gained from this fusion not only inform horizontal response, but also transition back to the vertical functions resident in the departments and agencies to manage steady State risks. It can even aid the private sector if the government is willing to share the analysis.

Agile Response: Building Information Age security in the federal enterprise will make it a better partner with the private sector for improving operational security. Over the past 10 years, there have been several attempts to improve operational coordination between and among key government and private sector stakeholders, but these have met with limited success. I strongly support creating a more effective model for operational collaboration to move us from the less effective government-led partnerships of the past to a more dynamic and collaborative approach involving cyber security leaders from government, industry, and academia. A collaboration framework for public private partnerships should include focused efforts to:

- Exchange threat and technical data (at the unclassified level as much as possible) to enable meaningful action, with rules and mechanisms that permit both sides to protect sensitive data. This approach is a shift from past practices that viewed information sharing as an objective as opposed to a tool;
- Create global situational awareness to understand the state of the computing ecosystem and events that may affect it;
- Analyze risks (threats, vulnerabilities, and consequences) and develop mitigation strategies; and
- When necessary and consistent with their respective roles, respond to threats.

Innovative Security Controls: The technologies used in enterprises today often grow faster than security organizations can make sense of them. Since computing technologies will continue to advance at a rapid pace, organizations creating security policy, standards, and technologies must consider how transformative changes in technology (e.g., wireless, RFID, peer-to-peer networks) create different risks and require different controls to maintain or improve security.

Moving Forward

One of the greatest challenges facing government is measuring its progress in improving cyber security. Are things better, worse, or the same? What is "success"? I strongly advocate for tracking progress, but must also caution against thinking of cyber security in terms of success and failure. Recognizing that cyberspace threats are not going to disappear and that attackers will be persistent and adaptive, it is not about risk elimination but risk management. As long as threats evolve, so must our efforts to protect against them. The U.S. must build holistic Information Age strategies to combat these threats in a coordinated manner. Reducing the attack surface of the federal enterprise and mitigating broad classes of threat will require fundamental changes. According to OMB, federal agencies spent approximately $6.2 billion (approximately 9.2 percent of the total IT portfolio) securing the government's total IT investment of approximately $68 billion for the fiscal year 2008.[8] But these resources and the current capabilities they fund do not provide sufficient defense. Absent agile government-wide security policies, standards, and oversight capabilities, the federal enterprise will present an unacceptably easy target. There is mounting proof that we must build an Information Age security model that creates a horizontal (cross-government) set of security requirements and builds, on top of that horizontal layer, agency specific protections to ensure that the government (generally) and each agency can fulfill its mission and protect the security of its information network.

BIOGRAPHY FOR SCOTT CHARNEY

Scott Charney serves as Corporate Vice President of Microsoft's Trustworthy Computing (TwC) Group within the Core Operating System Division. The group's mission is to drive Trustworthy Computing principles and processes within Microsoft and throughout the IT ecosystem. This includes working with business groups throughout the company to ensure their products and services uphold Microsoft's security and privacy policies, controls and best practices. The TwC group also collaborates with the rest of the computer industry and the government to increase public awareness, education and other safeguards.

In addition, Charney oversees Microsoft's efforts to address critical infrastructure protection, Engineering Excellence, network security, and industry outreach about privacy and security.

Charney possesses a wealth of computer privacy and security experience in both the government and the private sector. Before joining Microsoft in 2002, he was a principal for the professional services organization PricewaterhouseCoopers (PwC), where he led the firm's Cybercrime Prevention and Response Practice. He provided computer security services to Fortune 500 companies and smaller enterprises. These services included designing and building computer security systems, testing existing systems and conducting cybercrime investigations.

Before PwC, Charney served as Chief of the Computer Crime and Intellectual Property Section (CCIPS) in the Criminal Division of the U.S. Department of Justice. As the leading federal prosecutor for computer crimes, he helped prosecute

[8] Fiscal year 2008 FISMA Report to Congress.

nearly every major hacker case in the United States from 1991 to 1999. He co-authored the original *Federal Guidelines for Searching and Seizing Computers*, the federal *Computer Fraud and Abuse Act*, federal computer crime sentencing guidelines and the Criminal Division's policy on appropriate computer use and workplace monitoring. He also chaired the Group of Eight nations (G8) Subgroup on High-Tech Crime, served as Vice Chair and head of the U.S. delegation to an ad hoc group of experts on global cryptography policy for the Organization for Economic Cooperation and Development (OECD). In addition, he was a member of the U.S. delegation to OECD's Group of Experts on Security, Privacy and Intellectual Property Rights in the Global Information Infrastructure.

Charney also served as an assistant district attorney in Bronx County, N.Y., where he later was named Deputy Chief of the Investigations Bureau. In addition to supervising 23 prosecutors, he developed a computer-tracking system that was later used throughout the city for tracking criminal cases.

Charney has received numerous professional awards, including the prestigious John Marshall Award for Outstanding Legal Achievement in 1995 and the Attorney General's Award for Distinguished Service in 1998. He was nominated to the Information System Security Association's Hall of Fame in 2000. That same year, the Washington Chapter of the Armed Forces Communications and Electronics Association presented him with its award for excellence in critical electronic infrastructure protection. Among his other affiliations, he served on the American Bar Association Task Force on Electronic Surveillance, the American Health Lawyers Association Task Force on Security and Electronic Signature Regulations, the Software Engineering Institute Advisory Board at Carnegie-Mellon University, and the Privacy Working Group of the Clinton Administration's Information Infrastructure Task Force.

He holds a law degree with honors from Syracuse University in Syracuse, N.Y., and Bachelor's degrees in history and English from the State University of New York in Binghamton.

Chair WU. Thank you very much, Mr. Charney. Mr. Harper, please proceed.

STATEMENT OF MR. JIM HARPER, DIRECTOR OF INFORMATION POLICY STUDIES, THE CATO INSTITUTE

Mr. HARPER. Thank you. Thank you very much, Chair Wu. Thank you Ranking Member Smith for having me here to testify on cybersecurity activities at DHS and NIST today.

I welcome your oversight and your focus on results rather than output, such as dollars spent. This is very important work but not very easy.

As I tried to illustrate in my written submission, talking about cybersecurity is like talking about securing all the things we prize. Cybersecurity is many different problems, and it would be a mistake to believe that a discreet number of activities or a discreet set of government policies could solve all of them. I am concerned in the cybersecurity area there is a common practice of threat exaggeration and that that could buffalo this Congress to adopt policies that are not balanced and that ultimately waste resources, frustrate innovation, and threaten privacy and civil liberties.

Yesterday I came across an article in the Boston Review called Cyberscare on this very topic, and if it would please you, I would be happy to submit it for the record.

I was pleased, by the way, also to see that my co-panelists and colleagues didn't engage in threat exaggeration here and spoke about cybersecurity seriously without hyping threats.

I would like to feature one cybersecurity policy that I think has been lost in some of the cyber terrorism, cyber warfare cacophony, and that is the policy of keeping critical infrastructure off the public Internet. This policy is a proven success, but some policy-makers

I believe have ignored it, thinking that all resources should be on the public Internet or managed over the public Internet. So I encourage you and your colleagues to keep in mind the policy of keeping the true critical infrastructure off the 'net. That takes care of the lion's share of many security problems.

As I said, cybersecurity society-wide is many, many different problems, and I think your goal in Congress should not be to solve cybersecurity but to determine the systems, the social and legal systems, that will best discover and propagate good security technology and practices. You might think of a hierarchy of legal mechanisms that Congress could consider for advancing that goal starting with contracts, considering also tort liability and arriving last at prescriptive regulation.

Because the government is a large consumer of technology, it is well-positioned to positively affect the cybersecurity ecology, and NIST's standards are integral to that process. As a representative and worker at the Cato Institute, I would like to see the Federal Government a smaller purchaser of things, but while it is a large market actor, its buying decisions can help the market for secure technology products advance.

One way, obviously, is by setting high security standards in its purchasing. A second is to consider pushing technology providers to accept the risk of loss when their products are not sufficiently secure.

There is a market failure in technology when insecure technology harms networks or harms other users. I wouldn't leap to regulating in these cases, though, especially because none of us know efficiently and effectively how to solve these problems. Nobody knows what a regulation would say. For getting buyers and sellers of technology to internalize risks, I think liability should be the preferred mechanism. Liability is an open-ended process of discovery. As courts discover the legal doctrines that will help them prevent cyber harms, buyers and sellers of technology will have to discover the technologies and practices that prevent cyber harms.

Concerns for me arise when the government steps out of its role as a market participant and becomes a market dominator, a regulator, a partner or investor with private-sector entities. Standards are difficult things as you, and my co-panelists know well. When done right, they are extraordinarily valuable, and that can't be overstated. But when done wrong, they can distort markets or threaten privacy and civil liberties. I briefly note in my written testimony a potential concern with a standard, FIPS 201, and one of the witnesses in your earlier hearings mentioned that FIPS 201, an identity standard for federal employees and contractors, was becoming a national rather than a government standard. I work extensively on national ID issues, and I am concerned with the idea of a single standard for identification throughout the country.

I am suspicious of various public-private partnerships in the cybersecurity area and elsewhere. They can be valuable, and threat information sharing is valuable, but they can also suppress competition, they can foster security monoculture, immunize responsible parties from liability, and as I mentioned before, threaten privacy and civil liberties.

I will conclude my remarks there, and thank you again for having us here. You are looking at important issues in a careful way, and I appreciate that. Thank you again.

[The prepared statement of Mr. Harper follows:]

PREPARED STATEMENT OF JIM HARPER

Executive Summary

Cyber security is a bigger, more multi-faceted problem than the government can solve, and it certainly cannot solve the whole range of cyber security problems quickly.

With a few exceptions, cyber security is less urgent than many commentators allege. There is no argument, of course, that cyber security is not important.

The policy of keeping true critical infrastructure off the public Internet has been lost in the "cyber security" cacophony. It is a simple security practice that will take care of many threats against truly essential assets.

The goal of policy-makers should be not to solve cyber security, but to determine the systems that will best discover and propagate good security technology and practices.

As a market participant, the Federal Government is well positioned to effect the cyber security ecology positively, with NIST standards integral to that process. The Federal Government may also advance cyber security by shifting risk to sellers of technology by contract.

For the market failure that is on exhibit when insecure technology harms networks or other users, liability is preferable to regulation for discovering who should bear responsibility.

When the Federal Government abandons its role of market participant and becomes a market dominator, regulator, "partner," or investor with private sector entities, a number of risks arise, including threats to privacy and civil liberties, weakened competition and innovation, and waste of taxpayer dollars.

Introduction

Chairman Wu, Ranking Member Smith, and Members of the Subcommittee, thank you for inviting me to address you in this hearing on the cyber security activities of the National Institute of Standards and Technology and the Department of Homeland Security. The hearings you have conducted so far are a valuable contribution to the national discussion, as I hope my participation in this hearing will be valuable as well.

My name is Jim Harper and I am Director of Information Policy Studies at the Cato Institute. In that role, I study and write about the difficult problems of adapting law and policy to the challenges of the information age. I also maintain an online federal spending resource called *WashingtonWatch.com*. Cato is a market liberal, or libertarian, think-tank, and I pay special attention to preserving and restoring our nation's founding, constitutional traditions of individual liberty, limited government, free markets, peace, and the rule of law.

I serve as an advisor to the Department of Homeland Security on its Data Integrity and Privacy Advisory Committee, and my primary focus in general is on privacy and civil liberties. I am not a technologist or a cyber security expert, but a lawyer familiar with technology and security issues. As a former committee counsel in both the House and Senate, I also blend an understanding of lawmaking and regulatory processes with technology and security. I hope this background and my perspective enhance your consideration of the many challenging issues falling under the name "cyber security."

In my testimony, I will spend a good deal of time on fundamental problems in cyber security and the national cyber security discussion so far. I will then apply this thinking to some of the policies NIST, DHS, and other agencies are working on.

The Use and Misuse of "Cyberspace" and "Cyber Security"

One of the profound challenges you face in setting "cyber security" policy is the framing of the issue. "Cyberspace" is insecure, we all believe, and by making it integral to our lives, we are importing insecurity, as individuals and as a nation.

In some senses this is true, and "securing cyberspace" is a helpful way of thinking about the problem. But it also promotes over-generalization, suggesting that a bounded set of behaviors called "cyber security" can resolve things.

A new world or "space" is indeed coming into existence through the development of communications networks, protocols, software, sensors, commerce, and content. In many ways, this world is distinct and different from the physical space that we occupy. In "cyberspace," we now do many of the things we used to do only in physical space: we shop, debate, read the news, work, gossip, manage our financial affairs, and so on. Businesses and government agencies, of course, conduct their operations in the new "cyberspace" as well.

It is even helpful to extend this analogy and imagine "cyberspace" as organized like the physical world. Think of personal computers as people's homes. Their attachments to the network analogize to driveways, which connect to roads and then highways. (Perhaps phones and hand-held devices are data-bearing cars and motorcycles.) E-mails, financial files, and pictures are the personal possessions that could be stolen out of houses and private vehicles, leading to privacy loss.

Corporate and government networks are cyberspace's office buildings. Business data, personnel files, and intellectual property are the goods that sometimes get left on the loading dock, personnel files and business places that are left on the desk in an executive's office overnight, and so on. They can be stolen from the "office buildings" in data breaches.

How do you secure these places and things from theft, both casual and organized? How do you prevent fires, maintain water and electric service, ensure delivery of food, and prevent outbreaks of disease? How do you defend against military invasion or weapons of mass destruction in this all-new "space"?

These problems are harder to solve in some senses, and not as hard to solve in others. Consider, for example, that the "houses" and "office buildings" of cyberspace can be reconstituted in minutes or hours if software and data have been properly backed up. Lost possessions can be "regained" just as quickly—though copies of them may permanently be found elsewhere. "Cyberspace" has many resiliencies that real space lacks.

On the other hand, "diseases" (new exploits) multiply much more quickly and broadly than in the real world. "Cyber-public-health" measures like mandated vaccinations (the required use of security protocols) are important, though they may be unreliable. On a global public medium like the Internet, they would have to be mandated by an authority or authorities with global jurisdiction and authority over every computing device, which is unlikely and probably undesirable.

The analogy between cyberspace and real space shows that "cyber security" is not a small universe of problems, but thousands of different problems that will be handled in thousands of different ways by millions of people over the coming decades. Securing cyberspace means tackling thousands of technology problems, business problems, economics problems, and law enforcement problems.

In my opinion, if it takes decades to come up with solutions, that is fine. The security of things in "real" space has developed in an iterative process over hundreds and, in some cases, thousands of years. Even "simple" security devices like doors, locks, and windows involve fascinating and intricate security, utility, and convenience trade-offs that are hard even for experts to summarize.

Many would argue, of course, that we do not have decades to figure out cyber security. But I believe that, with few exceptions, most of these assertions are mistaken. Your ability to craft sound cyber security policies for the government is threatened by the breathlessness of public discussion that is common in this field.

Calm Down, Slow Down

Overuse of urgent rhetoric is a challenge to setting balanced cyber security policy. Threat exaggeration has become boilerplate in the cyber security area, it seems, and while cyber security is important, overstatement of the problems will promote imbalanced responses that are likely to sacrifice our wealth, progress, and privacy.

For example, comparisons between "cyberattack" and conventional military attack are overwrought. As one example (which I select only because it is timely), the Center for a New American Security is hosting a cyber security event this week, and the language of the invitation says: "[A] cyberattack on the United States' telecommunications, electrical grid, or banking system could pose as serious a threat to U.S. security as an attack carried out by conventional forces." [1]

As a statement of theoretical extremes, it is true: The inconvenience and modest harms posed by a successful crack of our communications or data infrastructure could be more serious than an invasion by an ill-equipped, small army. But as a serious assertion about real threats, an attack by conventional forces (however un-

[1] Center for a New American Security, "Developing a National Cybersecurity Strategy" web page (visited June 23, 2009) *http://www.cnas.org/node/2818*

likely) would be entirely more serious than any realistic cyberattack. We would stand to lose national territory, which cannot be reconstituted by rebooting, repairing software, and reloading backed-up files.

The Center for Strategic and International Studies' influential report, *Securing Cyberspace for the 44th Presidency*, said similarly that cyber security "is a strategic issue on par with weapons of mass destruction and global jihad."[2] Many weapons of mass destruction are less destructive than people assume, and the threat of global jihad appears to be waning, but threats to our communications networks, computing facilities, and data stores pale in comparison to true WMD like nuclear weapons. Controlling the risk of nuclear attack remains well above cyber security in any sound ranking of strategic national priorities.

It is a common form of threat exaggeration to cite the raw number of attacks on sensitive networks, like the Department of Defense's. It suffers hundreds of millions of attacks per year. But happily most of these "attacks" are repetitious use of the same attack. They are mounted by "script kiddies"—unsophisticated know-nothings who get copies of others' attacks and run them on the chance that they will find an open door.

The defense against this is to continually foreclose attacks and genres of attack as they develop, the way the human body develops antibodies to germs and viruses. Securing against these attacks is important work, and it is not always easy, but it is an ongoing, stable practice in network management and a field of ongoing study in computer science. The attacks may continue to come in the millions, but this is less concerning when immunities and fail-safes are in place and continuously being updated.

In his generally balanced speech on cyber security, President Obama cited a threat he termed "weapons of mass disruption."[3] Again, analogy to the devastation that might be done by nuclear weapons is misleading. Inconvenience and disruption are bad things, they can be costly, and in the extreme case deadly—again, cyber security is important—but securing against the use of real weapons on the U.S. and its people is a more important government role.

In a similar vein, a commentator on the *National Journal*'s national security experts blog recently said, "Cyberterrorism is here to stay and will grow bigger."[4] Cyberterrorism is not here, and thus it is not in a position to stay.

Provocative statements of this type lack a key piece of foundation: They do not rest on a sound strategic model whereby opponents of the United States and U.S. power would use the capabilities they actually have to gain strategic advantage.

Take cyberterrorism. With communications networks, computing infrastructure, and data stores under regular attack from a variety of quarters—and regularly strengthening to meet them—it is highly unlikely that terrorists can pull off a cyber security event disruptive enough to instill widespread fear of further disruption. Fear is a necessary element for terrorism to work its will, of course. The impotence of computer problems to instill fear renders "cyberterrorism" an unlikely threat. This is not to deny the importance of preventing the failure of infrastructure, of course.

Cyberattacks by foreign powers have a similarly implausible strategic logic. The advantage gained by a disabling attack on private and civilian government infrastructure would be largely economic, with perhaps some psychological effects. Such attacks would not plausibly "soften up" the United States for invasion. But committing such attacks would risk harsh responses if the perpetrators were found, and conventional intelligence methods are undoubtedly keenly tuned to doing so. Ultimately, a foreign government's cyberattack on the United States would have to be a death-blow, as it would risk eliciting ruinous responses. This makes it very unlikely that a cyberattack on civilian infrastructure would be a tool of true war.

Attacking military communications infrastructure and data does have a rational strategic logic, of course. And the testimony your committee received from Dr. Leheny of the Defense Advanced Research Project Agency at your June 16 hearing illustrates some of what the Defense Department is doing to anticipate and prevent attacks on this true critical infrastructure.

The more plausible strategic use of attacks on communications and data infrastructure is not "cyberterrorism" or "cyberattack," but what might be called

---

[2] CSIS Commission on Cybersecurity for the 44th Presidency, "Securing Cyberspace for the 44th Presidency," p. 15 (2008) *http://www.csis.org/media/csis/pubs/081208_securing cyberspace_44.pdf* [hereinafter "CSIS Report"].

[3] "Remarks by the President on Securing Our Nation's Cyber Infrastructure," (May 29, 2009) *http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/*.

[4] *http://security.nationaljournal.com/2009/06/how-can-cyberspace-be-protecte.php*

"cybersapping": Infiltrating networks to gain business intelligence, intellectual property, money, personal and financial data, and perhaps strategic government information. These infiltrations can slowly degrade the advantages that the U.S. economy and government have over others. They are important to address diligently and promptly. But they are not a reason to panic and overreact.

A final example of cyber security boilerplate that deserves mention is the alleged weakness of military information systems. The story that confidential files about the Joint Strike Fighter were compromised earlier this year has become a standard dire warning about our national vulnerability. But many are conveniently forgetting the other half of the story, even though it is available right there in some of the earliest reporting. According to a contemporaneous story on *CNN.com*:

> [O]fficials insisted that none of the information accessed was highly sensitive data. The plane uses stealth and other highly sensitive electronic equipment, but it does not appear that information on those systems was compromised, because it is stored on computers that are not connected to the Internet, according to the defense officials.[5]

The compromise of some data about the Joint Strike Fighter is regrettable, but this is also a story of cyber security success. The key security policy of keeping the most sensitive data away from the public Internet successfully protected that data. The Department of Defense deserves credit for instituting and maintaining that policy.

Cyber security is important, but exaggerating threats and failures as a matter of routine will lead to poor policy-making. Do not let the urgency of many statements about cyber security "buffalo" you into precipitous, careless, and intrusive policies.

Exhortation about some cyber security policies seem to be pushing others off the table, like the policy so successful at protecting the most important information about the Joint Strike Fighter. The simple, elegant policy of keeping truly critical infrastructure off the public Internet is not receiving enough discussion.

Critical Infrastructure: Off the Internet

At the confirmation hearing of Commerce Secretary Gary Locke earlier this year, Senator Jay Rockefeller stated his view of the cyber security problem in no uncertain terms. Of cyberattack, he said:

> It's an act which can shut this country down—shut down its electricity system, its banking system, shut down really anything we have to offer. It is an awesome problem . . .. It is a fearsome, awesome problem.[6]

What is fearsome is the embedded premise that everything important to our country would be put on the Internet rather than controlled over separate, dedicated networks. This is not true, as the example of the Joint Strike Fighter example illustrates. And it turns out that many important functions in government and society are indeed handled by dedicated communications networks.

Cato Institute adjunct fellow Timothy B. Lee, a Ph.D. student in computer science at Princeton University and an affiliate of the Center for Information Technology Policy, commented on the Estonian cyberattacks last year:

> [S]ome mission-critical activities, including voting and banking, are carried out via the Internet in some places. But to the extent that that's true, the lesson of the Estonian attacks isn't that the Internet is "critical infrastructure" on par with electricity and water, but that it's stupid to build "critical infrastructure" on top of the public Internet. There's a reason that banks maintain dedicated infrastructure for financial transactions, that the power grid has a dedicated communications infrastructure, and that computer security experts are all but unanimous that Internet voting is a bad idea.[7]

Tim has also noted that the Estonia attacks did not reach parliament, ministries, banks, and media—just their web sites. Access to some businesses and government agencies went down, but their core functions were not compromised.

Yet this policy—of keeping critical functions away from the Internet—has received almost no discussion in the recent major reports on cyber security. The White

---

[5] Mike Mount, "Hackers Stole Data on Pentagon's Newest Fighter Jet," *CNN.com* (Apr. 21, 2009) *http://www.cnn.com/2009/US/04/21/pentagon.hacked/index.html*

[6] See "Jay Rockefeller: Internet Should Have Never Existed," YouTube (posted Mar. 20, 2009) *http://www.youtube.com/watch?v=Ct9xzXUQLuY*

[7] Tim Lee, "The Internet Isn't 'Critical Infrastructure,'" TechDirt (May 27, 2008) *http://www.techdirt.com/articles/20080522/1905471205.shtml*

House's *Cyberspace Policy Review* did not highlight this approach,[8] and the President's speech presenting the review did not either. The CSIS report also did not emphasize this simple, straightforward method for securing truly critical functions.

Where security is truly at a premium, the lion's share of securing infrastructure against cyberattack can be achieved by the simple policy of fully decoupling it from the Internet.

"Criticality" has become a popular line to draw in discussions of cyber security, of course, and the meaning of the term is in no way settled. A 2003 Congressional Research Service report explored the dimensions of the concept at the time.[9] My study of "criticality" is cursory, but the CSIS report's suggestion is sensible, if loosely drawn:

> [C]ritical means that, if the function or service is disrupted, there is immediate and serious damage to key national functions such as U.S. military capabilities or economic performance. It does not mean slow erosion or annoying disruptions.[10]

In my mind, criticality should probably turn on whether compromise of the resource would immediately and proximately endanger life and health. Immediacy is an important limitation because resources that can be promptly repaired to prevent harm should be made resilient that way rather than treated as critical infrastructure.

Proximity to harm is also important to prevent "criticality" grade-inflation. The loss of electric power for even an hour will kill people on respirators in hospitals, for example, but the proximate solution to such foreseeable risks is to have backup power systems at hospitals-not to make the entire electricity grid critical infrastructure on that basis.

If it is to be a focal point for cyber security policies, the notion of "critical infrastructure" must be sharply circumscribed. Given the special treatment accorded critical infrastructure by government, private entities will all clamor for that status, and the government will be stuck protecting thousands of things that are kind of important, rather than the networks and data that are immediately needed for protecting life and health.

Keeping the small universe of truly critical infrastructure entirely separate from the public Internet, and encouraging private operators of critical infrastructure to do so, is a policy that has not received enough discussion so far. It deserves a great deal more.

But this is one among dozens of policy choices to deal with thousands of problems. The many complex challenges lumped together as "cyber security" cannot be solved by any one expert, group of experts, legislature, regulatory body, or commission. It has too many moving parts.

Rather than trying to address cyber security in toto, I recommend addressing the problem at a level once-removed: By asking what systems we should use to address cyber security. There are a variety of social mechanisms, each with merits and demerits.

Cyber Security Through Contract

In my testimony so far, I have argued against over-generalization and over-heated rhetoric around cyber security. Cyber security is many different problems, only some of which are urgent.

None of this is to deny that cyber security is a serious and important challenge. I applaud the work of the Defense Department to secure its critical information, and find very interesting DARPA's innovative work to develop networks over which our military branches can conduct their very important functions. These are two examples among many government-wide efforts to secure true critical infrastructure.

But what about the rest of the country's communications and data infrastructure? Is the entire Nation's cyberstuff a "strategic national asset," as the President sug-

---

[8] "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure," The White House (undated) *http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf*; "Remarks by the President on Securing Our Nation's Cyber Infrastructure," (May 29, 2009) *http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/*

[9] John Moteff et al., Resources, Science, and Industry Division, Congressional Research Service, "Critical Infrastructures: What Makes an Infrastructure Critical?" CRS Order Code RL31556 (updated Jan. 29, 2003) *http://www.fas.org/irp/crs/RL31556.pdf*

[10] CSIS Report, p. 44.

gested in his speech on cyber security?[11] Should it all come under a military or quasi-military command-and-control operation?

The CSIS study called for a "comprehensive national security strategy for cyberspace" and stated accordingly and unflinchingly that the government should "regulate cyberspace."[12] The report also laid our cyber security woes at the feet of the market: "We have deferred to market forces in the hope that they would produce enough security to mitigate national security threats. It is not surprising that . . . industrial organization and over-reliance on the market has not produced success."[13]

Competition and markets should not be passed over in favor of regulation. Indeed, the argument for regulation begs the central question: What do we want from our technical infrastructures so that we have appropriate security? What would a cyber security regulation *say*? Nobody yet knows.

To illustrate, FISMA the *Federal Information Security Management Act*, has not taken care of cyber security for the Federal Government. Federal chief information security officers and others rightly criticize the government's self-regulation for its focus on compliance reporting and paperwork at the expense of addressing known problems.[14]

If the Federal Government knew how to do cyber security well, FISMA would be a to-do list that more or less secured the federal enterprise. We would not have the cyber security problem all agree we have. But the practices that lead to successful cyber security have not yet been discovered. Regulations to implement these undiscovered practices would not help.

Success in cyber security is not easy to define. Professor Ed Felten from Princeton University's Center for Information Technology Policy points out that the ideal is not perfect security, but optimal security—the efficient point where investments in security avoid equal or greater losses.[15] Communications and computing devices are meant to process, display, and transmit information that they often acquire from other resources. To make them useful, we must embrace the risk of opening them up to other computers, software, and data. Some level of insecurity is what makes the Internet, computing, and "cyberspace" so useful and valuable.

Again, the question is what processes we can use to discover optimal or near-optimal cyber security products and behaviors, then propagate them throughout the society.

Criticisms of the market are not misplaced, though they may be mis-focused. The market for communications and computing technologies is very immature. Many products are rushed to market without adequate security testing. Many are delivered with insecure settings enabled by default. My impression also is that most are sold without any warranty of fitness for the purposes users will put them to, leaving all risk of failure with buyers who are poorly positioned to make sound security judgments. There are several ways to address these problems.

As this committee is aware, the Federal Government is one of the largest purchasers—if not the largest purchaser—of information technology in the world. This is not the preferred state of affairs from my perspective, but there is no reason to deny that its purchasing decisions can affect the improvement of products available on the market.

Thanks to entities like the National Institute of Standards and Technology, the Federal Government is also one of the most sophisticated purchasers of technology. As other witnesses and advocates have articulated better than I can, the government can drive maturation in the market for technology products by setting standards and defaults for the products and services it buys.

The Federal Government can also insist on shifting the risk of loss from the buyer to the seller. Contracts with technology sellers can include guarantees that their products are fit for the purposes to which they will be put—including, of course, secure operation.

Federal buyers should expect to pay more if they demand fitness and security guarantees, of course, but more secure products have more value. Sellers will have

---

[11] "Remarks by the President on Securing Our Nation's Cyber Infrastructure," (May 29, 2009) *http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/*

[12] CSIS Report, pp. 1–2.

[13] CSIS Report, p. 12.

[14] See, e.g., Government Futures, "The 2009 State of Cybersecurity from the Federal CISO's Perspective—An (ISC)2 Report" (April 2009) http://media.haymarketmedia.com/Documents/7/FederalCISOSurveyReport—1638.pdf.

[15] Nestor Abreu, "Conversation: Debugging our Cyber-Security Policy" (podcast at minute 12:00) (Feb. 27, 2009) *http://citp.princeton.edu/blog/2009/02/27/conversation-debugging-our-cyber-security-policy/*

to do more thorough development and more rigorous security testing. Because they currently bear little or no risk of loss, technology sellers will probably howl at the prospect of bearing risk, but ready to step in will be technology sellers willing to produce better, more secure, and more reliable products for the premium that gets them.

As a large market participant, the Federal Government can have a good influence on the security ecology without resorting to intrusive regulation. Whether it creates a "gold standard" for security in technologies purchased in the private sector, or whether it moves the market toward contract-based liability for technology sellers, the Federal Government can help the technology market mature.

Cyber Security Through Tort Liability

There is more to criticism of the market for cyber security than "lack of maturity," however. There is also an arguable market failure in the area of technology products and services, caused by a lack of maturity in the law. I was pleased that the executive summary of the White House *Cyberspace Policy Review* cited a short paper I wrote arguing that updated tort law would be superior to regulation for curing the market.[16]

A market failure exists when the market price of a good does not include the costs or benefits of externalities (harmful or beneficial side effects that occur in the production, distribution, or consumption of a good). Producers or consumers may have little incentive to alter activities that contribute to air pollution, for example, when the costs of pollution do not affect their costs. Likewise, users of computers that are insecure may harm the network or other users, such as when malware infects a computer and uses it to launch spam or distributed denial-of-service attacks.

When there is no contractual relations between the parties, getting network operators, data owners, and computer users to internalize risks can be done one of two ways: Regulation—you mandate certain behaviors—or liability—you make them pay for harms they cause others. Regulation and liability each have strengths and weaknesses, but I believe a liability regime is ultimately superior.

One of the main problems with regulation—especially in a dynamic field like technology—is that it requires a small number of people to figure out how things are going to work for an unknown and indefinite future. Those kinds of smarts do not exist.

So regulators often punt: When the *Financial Services Modernization Act* tasked the Federal Trade Commission with figuring out how to secure financial information, it did not do that. Instead, the "Safeguards Rule"[17] (similarly to FISMA) simply requires financial institutions to have a security plan. If something goes wrong, the FTC will go back in and either find the plan lacking or find that it was violated.

Another weakness of regulation is that it tends to be too broad. In an area where risks exist, regulation will ban entire swaths of behavior rather than selecting among the good and bad. In 1998, for example, Congress passed the *Children's Online Privacy Protection Act,* and the FTC set up an impossible-to-navigate regime for parental approval of the web sites their children could use.[18] Today, no child has been harmed by a site that complies with COPPA because they are so rare. The market for serving children entertaining and educational content is a shadow of what it could be.

Regulators and regulatory agencies are also subject to "capture." Industries have historically co-opted the agencies intended to control them and turned those agencies toward insulating incumbents from competition.[19]

And regulation often displaces individual justice. The *Fair Credit Reporting Act* preempted state law causes of action against credit bureaus that, thus, cannot be held liable for defamation when their reports wrongfully cause someone to be denied credit. "Privacy" regulations under the *Health Insurance Portability and Accountability Act* gave enforcement powers to an obscure office in the Department of Health and Human Services. While a compliance kabuki dance goes on overhead,

---

[16] Much of Jim Harper, "Government-Run Cyber Security? No, Thanks," Cato Institute TechKnowledge #123 (March 13, 2009) *http://www.cato.org/tech/tk/090313-tk.html,* is incorporated into this testimony.

[17] See Federal Trade Commission, "Protecting Customers' Personal Information: The Safeguards Rule" web page (visited June 23, 2009) *http://www.ftc.gov/bcp/edu/microsites/idtheft/business/safeguards.html*

[18] See Federal Trade Commission, "You, Your Privacy Policy, and COPPA: How to Comply with the Children's Online Privacy Protection Act" web page (visited June 23, 2009) *http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus51.pdf*

[19] See Timothy B. Lee, "The Durable Internet: Preserving Network Neutrality without Regulation," Cato Policy Analysis #626 (Nov. 12, 2008) *http://www.cato.org/pub_display.php?pub_id=9775*

people who have suffered privacy violations are diverted to seeking redress by the grace of a federal agency.

Tort liability is based on the idea that someone who does harm, or allows harm to occur, should be responsible to the injured party. The role of law and government is to prevent individuals from harming one another. When a person drives a car, builds a building, runs a hotel, or installs a light switch, he or she owes it to anyone who might be injured to keep them safe. A rule of this type could apply to owners and operators of networks and databases, and possibly even to software writers and computer owners.

A liability regime is better at discovering and solving problems than regulation. Owners faced with paying for harms they cause will use the latest knowledge and their intimacy with their businesses to protect the public. Like regulation, a liability regime will not catch a new threat the first time it appears, but as soon as a threat is known, all actors must improve their practices to meet it. Unlike regulations, which can take decades to update, liability updates automatically.

Liability also leaves more room for innovation. Anything that causes harm is forbidden, but anything that does not cause harm is allowed. Entrepreneurs who are free to experiment will discover consumer-beneficial products and services that improve health, welfare, life, and longevity.

Liability rules are not always crystal clear, of course, but when cases of harm are alleged in tort law, the parties meet in a courtroom before a judge, and the judge neutrally adjudicates what harm was done and who is responsible. When an agency enforces its own regulation, it is not neutral: Agencies work to "send messages," to protect their powers and budgets, and to foster future careers for their staffs.

Especially in the high-tech world of today, it is hard to prove causation. The forensic skill to determine who was responsible for an information-age harm is still too rare. But regulation is equally subject to evasion. And liability acts not through lawsuits won, but by creating a protective incentive structure.

One risk unique to liability is that advocates will push to do more with it than compensate actual harms. Some would treat the creation of risk as a "harm," arguing, for example, that companies should pay someone or do something about potential identity fraud just because a data breach created the risk of it. They often should, but blanket regulations like that actually promote too much information security, lowering consumer welfare as people are protected against things that do not actually harm them.

It is also true that the tort liability system has been abused in some cases. Plaintiffs' bars have sought to turn litigation into another regulatory mechanism—or a cash cow. State common law reforms to meet these challenges are in order; dismissing the common law out of hand is not.

There are dozens of complexities to how the tort law would operate in the cyber security area, of course. The common law is a system of discovery that crafts doctrines to meet emerging challenges. I cannot predict each challenge common law courts would encounter and how they would address them, but the growth of common law doctrines to prevent harm is an important alternative to the heavy hand of regulation.

As complex and changing as cyber security is, the Federal Government has no capability to institute a protective program for the entire country. While it secures its own networks, the Federal Government should observe the growth of state common law duties that require network operators, data owners, and computer users to secure their own infrastructure and assets. (They in turn will divide up responsibility efficiently by contract.) This is the best route to discovering and patching security flaws in all the implements of our information economy and society.

Between the two, contract and tort liability can provide a seamless web of cyber security incentives, spreading risks to the parties most capable of controlling them and bearing their costs. Regulation pushes responsibility to protect where it is politically palatable, not where it is economically most efficient or best done. Regulation often shields the private sector from liability, foisting risk onto the public—one of the concerns I will turn to next.

Standards, Public-Private Partnerships, and the Risks Thereof

As a market participant, the Federal Government can play an important role in promoting secure products and practices. When it leaves the role of market participant and becomes a market dominator, a regulator, a "partner," or investor with private sector entities, a number of risks arise, including threats to privacy and civil liberties, weakened competition and innovation, and waste of taxpayer dollars. I will address selected examples of NIST and DHS activity in that light.

As a standard-setting organization for the Federal Government, NIST is a valuable resource—not just for the government but for the cybersecurity ecology. But

standards are tricky business. What may be appropriate in one context may not be in another.

An area of keen interest to me as an advocate for privacy and civil liberties is the avoidance of a national ID system in the United States. My book, *Identity Crisis: How Identification is Overused and Misunderstood*, sought to reveal the demerits in having a U.S. national ID. The *REAL ID Act of 2005*, which attempted to create a national ID system in the United States, has foundered for a variety of reasons. Unfortunately, a bill recently introduced in the Senate would seek to revive this national ID program.[20]

Accurate identification or "identity security" is important in some contexts, but less so in others. Anonymity and obscurity are important protections for Americans' privacy and freedom to speak and act as they wish. Ultimately, I believe a diverse and competitive identity and credentialing system will deliver all the benefits that digital identity systems can provide, without the surveillance.

So I was concerned to see one bullet point in the testimony of Cita Furlani from NIST at your recent joint hearing. She characterized NIST's identity and credentialing management standard for federal employees and contractors (FIPS 201) as "becoming the de facto national standard."[21]

It is unclear exactly what this means, of course, and I do not view FIPS 201 as the foremost threatened national ID standard at this time. But the needs in identity and credentialing outside the Federal Government are quite different from those within the government. The same market dominance that makes the Federal Government such a potential boon to cyber security could make it an equal bane to privacy and civil liberties should FIPS 201 be adopted widely by State governments for their employees, by states for their drivers' licenses and IDs, and in private-sector employment and access control. The same is probably true of other standards in other ways.

Cyber security standard-setting for Federal Government purchasing and use should present few problems. It can often be beneficial when it drives forward the cyber security marketplace. But pressing standards onto the private sector where they are not a good fit—in delicate areas such as personal information handling—creates concerns.

Professor Schneider from Cornell said it well in your first hearing of this series:

> [T]he Internet is as much a social construct as a technological one, and we need to understand what effects proposed technological changes could have; forgoing social values like anonymity and privacy (in some sense, analogous to freedom of speech and assembly) in order to make the Internet more trustworthy might significantly limit the Internet's utility to some, and thus not be seen as progress.[22]

A different array of concerns arises from nominal "public-private partnerships." The concept is much ballyhooed among governments and corporations because it suggests happiness and cooperation. But I am not enthusiastic about a joining of hands between the government and the corporate sector.

Public-private partnerships take many forms, of course. The least objectionable are information-sharing arrangements like the Department of Homeland Security's US–CERT, or United States Computer Emergency Readiness Team. But consumers, the society, and our economy do not get the best from corporations when they cooperate, much less when they cooperate with government. Markets squeeze the most out of the business sector when competitors are nakedly pitted against each other and forced to compete on every dimension of their products and services, including cyber security.

Programs like US–CERT run the risk of diminishing competition and innovation in cyber security. Vulnerability warning is not a public good; it can be provided privately by companies competing against each other to do the best job for their clients.

---

[20] S. 1261, The PASS ID Act (111th Cong., 1st Sess.) *http://www.washingtonwatch.com/bills/show/111_SN_1261.html*

[21] Testimony of Ms. Cita Furlani, Director, Information Technology Laboratory, National Institute of Standards and Technology (NIST), to a hearing entitled "*Agency Response to Cyberspace Policy Review*," Subcommittee on Technology & Innovation, Committee on Science and Technology, United States House of Representatives, p. 4 (June 16, 2009) *http://democrats.science.house.gov/Media/file/Commdocs/hearings/2009/Tech/16jun/Furlani_Testimony.pdf*

[22] Testimony of Dr. Fred B. Schneider, Samuel B. Eckert Professor of Computer Science, Cornell University, to a hearing entitled "*Cyber Security R&D*," Subcommittee on Technology & Innovation, Committee on Science and Technology, United States House of Representatives, p. 4 (June 10, 2009) *http://democrats.science.house.gov/Media/file/Commdocs/hearings/2009/Research/10jun/Scheider_Testimony.pdf*

"Free" taxpayer-funded vulnerability warning will tend to squeeze private providers out of the market.

This risks lowering overall consumer welfare, especially if it leads to cyber security monoculture. "Monoculture" is the idea that uniformity among security systems is a weakness. In a security monoculture, one flaw could be exploited in many domains at once, bringing them all down and creating problems that would not have materialized in a diverse security environment.

With US–CERT this is only a risk. Public-private partnerships of other stripes raise more powerful concerns.

Earlier in my testimony, I wrote about how liability can promote cyber security. It is equally the case that the absence of liability can degrade security. If public-private partnerships confuse lines of responsibility for security, the results can be very bad indeed.

Consider how responsibility for passenger air transportation was mixed before the 9/11 attacks. Airlines nominally provided security, but they had to obey the dictates of the Federal Aviation Administration. Were something bad to happen, both entities were in a position to deny responsibility.

Flying a plane into a building had been written about in a 1994 novel—and kamikaze attacks were, of course, a tactic of the Japanese in World War II—but on 9/11 hijacking protocols had not been seriously revamped since the 1970s, when absconding to Cuba was the chief goal of most airline takeovers.

After 9/11, neither airlines nor the Federal Aviation Administration shouldered responsibility. The airlines moved swiftly to capitalize on emotion and patriotism, getting Congress to shield them from liability, give them an infusion of taxpayer dollars, and take over their security obligations. This "public-private partnership" in security was a disaster from start to finish, and remains so. The party ultimately bearing the loss—and still at risk today—was the American taxpayer and traveler.

This illustration is not to suggest that cyber security failures threaten attacks equivalent to 9/11. It is simply to suggest that the better role of the government is to stand apart from industry and to arbitrate liability when a company has failed to meet its contractual or tort-based obligations.

Public-private partnerships may also be conduits for transferring taxpayer funds to corporations, or to universities who do research for corporations. While reviewing the testimonies presented to you in earlier hearings, I was impressed by the nearly uniform requests for taxpayer money.

Much of the money requested would go to research that industry needs to do a good job. In other words, it is research they would fund themselves in the absence of a subsidy. Using a small amount of money taken from each taxpayer, Congress can give money to corporations and claim a role in the production of security, even though the corporations would have put their own money to that use themselves. This is another form of "partnership" where the American taxpayer loses.

When the Federal Government abandons the role of market participant and neutral arbiter, difficulties arise. Though NIST standards are useful for the Federal Government—and many of them can apply well in the private sector—they may not be appropriately forced on the private sector when the government is market-dominant. Government-corporate collaboration raises many risks: security monoculture; mixed responsibility and weakened security; and simple waste of taxpayer dollars.

Cyber security is special, but not so special that principles about the limited role of government should go by the wayside. We will get the best security and the best deal for taxpayers and the public if the government remains within its proper sphere.

Conclusion

Cyber security is a huge topic, and I have ranged widely across it in my imperfect testimony. I hope it is more clear that "cyber security" is a bigger, more multi-faceted problem than the government can solve, and government certainly cannot solve the whole range of cyber security problems quickly.

Happily, with a few exceptions, cyber security is also less urgent than many commentators allege. "Cyberattack" or "cyberterrorism" might be replaced by "cybersapping" of the country's assets and technology as the threat we should promptly and diligently address. There is no argument, of course, that cyber security is not important.

I am concerned that the policy of keeping true critical infrastructure off the public Internet has been lost in the cyber security cacophony. It is a simple, elegant practice that will take care of many threats against truly essential assets.

The government will not fix the Nation's cyber security. Your goal as policy-makers should be one level removed: to determine the system that will best discover and propagate good cyber security practices.

As a market participant, the Federal Government is well positioned to effect the cyber security ecology positively, with NIST standards integral to that process. The Federal Government may also advance cyber security by shifting risk to sellers of technology by contract.

For the market failure that is on exhibit when insecure technology harms networks or other users, liability is a preferable mechanism to regulation for discovering who should bear the responsibility to protect.

When the Federal Government abandons its role of market participant and becomes a market dominator, regulator, "partner," or investor with private sector entities, a number of risks arise, including threats to privacy and civil liberties, weakened competition and innovation, and waste of taxpayer dollars.

I appreciate the chance to share these ideas with you, and I hope that they will aid the Committee's deliberations.

BOSTON REVIEW
JULY/AUGUST 2009

Cyber-Scare

The exaggerated fears over digital warfare

Evgeny Morozov

The age of cyber-warfare has arrived. That, at any rate, is the message we are now hearing from a broad range of journalists, policy analysts, and government officials. Introducing a comprehensive White House report on cyber-security released at the end of May, President Obama called cyber-security "one of the most serious economic and national security challenges we face as a nation." His words echo a flurry of gloomy think-tank reports. The Defense Science Board, a federal advisory group, recently warned that "cyber-warfare is here to stay," and that it will "encompass not only military attacks but also civilian commercial systems." And "Securing Cyberspace for the 44th President," prepared by the Center for Strategic and International Studies, suggests that cyber-security is as great a concern as "weapons of mass destruction or global jihad."

Unfortunately, these reports are usually richer in vivid metaphor—with fears of "digital Pearl Harbors" and "cyber-Katrinas"—than in factual foundation.

Consider a frequently quoted CIA claim about using the Internet to cause widespread power outages. It derives from a public presentation by a senior CIA cyber-security analyst in early 2008. Here is what he said:

We have information, from multiple regions outside the United States, of cyber-intrusions into utilities, followed by extortion demands. We suspect, but cannot confirm, that some of these attackers had the benefit of inside knowledge. We have information that cyber-attacks have been used to disrupt power equipment in several regions outside the United States. In at least one case, the disruption caused a power outage affecting multiple cities. We do not know who executed these attacks or why, but all involved intrusions through the Internet.

So "there is information" that cyber-attacks "have been used." When? Why? By whom? And have the attacks caused any power outages? The CIA may have some classified information, but very little that is unclassified suggests that such cyber-intrusions have occurred.

Or consider an April 2009 *Wall Street Journal* article entitled "Electricity Grid in U.S. Penetrated By Spies." The article quotes no attributable sources for its starkest claims about cyber-spying, names no utility companies as victims of intrusions, and mentions

just one real cyber-attack, which occurred in Australia in 2000 and was conducted by a disgruntled employee rather than an external hacker.

It is alarming that so many people have accepted the White House's assertions about cyber-security as a key national security problem without demanding further evidence. Have we learned nothing from the WMD debacle? The administration's claims could lead to policies with serious, long-term, troubling consequences for network openness and personal privacy.

Cyber-security fears have had, it should be said, one unambiguous effect: they have fueled a growing cyber-security market, which, according to some projections, will¬†grow twice as fast as the rest of the IT industry. Boeing, Raytheon, and Lockheed Martin, among others, have formed new business units to tap increased spending to protect U.S. government computers from cyber-attacks. Moreover, many former government officials have made smooth transitions from national cyber-security policy to the lucrative worlds of consulting and punditry. Speaking at a recent conference in Washington, D.C., Amit Yoran—a former cyber-security czar in the Bush administration and currently the C.E.O. of NetWitness, a cyber-security start-up—has called hacking a national security threat, adding that "cyber-9/11 has happened over the last ten years, but it's happened slowly, so we don't see it." One way for the government to protect itself from this cyber-9/11 may be to purchase NetWitness's numerous software applications, aimed at addressing both "state and non-state sponsored cyber threats."

From a national security perspective, cyber-attacks matter in two ways. First, because the back-end infrastructure underlying our economy (national and global) is now digitized, it is subject to new risks. Fifty years ago it would have been hard—perhaps impossible, short of nuclear attack—to destroy a significant chunk of the U.S. economy in a matter of seconds; today all it takes is figuring out a way to briefly disable the computer systems that run Visa, MasterCard, and American Express. Fortunately, such massive disruption is unlikely to happen anytime soon. Of course there is already plenty of petty cyber-crime, some of it involving stolen credit card numbers. Much of it, however, is due to low cyber-security awareness by end-users (you and me), rather than banks or credit card companies.

Second, a great deal of internal government communication flows across computer networks, and hostile and not-so-hostile parties are understandably interested in what is being said. Moreover, data that are just sitting on one's computer are fair game, too, as long as the computer has a network connection or a USB port. Despite the "cyber" prefix, however, the basic risks are strikingly similar to those of the analog age. Espionage has been around for centuries, and there is very little we can do to protect ourselves beyond using stronger encryption techniques and exercising more caution in our choices of passwords and Wi-Fi connections.

To be sure, there is a war-related caveat here: if the military relies on its own email system or other internal electronic communications, it is essential to preserve this capability in wartime. Once more, however, the concern is not entirely novel; when radio

was the primary means of communication, radio-jamming was also a serious military concern; worries about radio go back as far as the Russo-Japanese War of 1904-1905.

Before accepting the demands of government agencies for new and increased powers, we should look more closely at well-defined dangers.

The ultimate doomsday scenario—think *Live Free or Die Hard*—could involve a simultaneous attack on economic e-infrastructure and e-communications: imagine al Qaeda disabling banks, destroying financial data, disrupting networks, and driving the American economy back to the nineteenth century. This certainly sounds scary—almost as scary as raptors in Central Park or a giant asteroid heading toward the White House. The latter two are not, however, being presented as "national security risks" yet.

There are certainly genuine security concerns associated with the Internet. But before accepting the demands of government agencies for new and increased powers to fight threats in cyberspace and prepare for cyber-warfare, we should look more closely at well-defined dangers and ask just where existing technological means and legal norms fall short. Because the technologies are changing so quickly, we cannot expect definitive answers. But cyber-skeptics—who argue that cyber-warfare is still more of an urban legend than a credible hazard—appear to be onto something important.

One kind of cyber-security problem grows out of resource scarcity. A network has only so much bandwidth; a server can serve only so much data at one time. So if you want to disable (or simply slow down) the computer backbone of a national economy, for example, you need to figure out how to reach its upper limit.

It would be relatively easy to protect against this problem if you could cut your computer or network off from the rest of the world. But as the majority of governmental and commercial services have moved online, we expect them to be offered anywhere; Americans still want to access their online banking accounts at Chase even if they are travelling in Africa or Asia. What this means in practice is that institutions typically cannot shut off access to their online services based on nationality of the user or the origin of the computer (and in the case of news or entertainment sites, they do not want to: greater access means more advertising income).

Together, these limitations create an opportunity for attackers. Since no one, not even the U.S. government, has infinite computer resources, any network is potentially at risk.

Taking advantage of this resource scarcity could be an effective way of causing trouble for sites one does not like. The simplest—and also the least effective—way of doing this is to visit the URL and hit the "reload" button on your browser as often (and for as long) as you can. Congratulations: you have just participated in the most basic kind of "denial-of-service" (DoS) attack, which aims to deny or delay the delivery of online services to legitimate users. These days, however, it would be very hard to find a site that would suffer any noticeable damage from such a nuisance; what is missing from your cyber-guerilla campaign is scale.

Now multiply your efforts by a million—distribute your attacks among millions of other computers—and this could be enough to cause headaches to the administrators of many Web sites. These types of attacks are known as "distributed denial-of-service" or DDoS attacks. Administrators may be able to increase their traffic and bandwidth estimates and allocate more resources. Otherwise they have to live with this harassment, which may disable their Web site for long periods.

DDoS attacks work, then, by making heavier-than-normal demands on the underlying infrastructure, and they usually cause inconvenience rather than serious harm. Not sure how to do it yourself? No problem: you can buy a DDoS attack on the black market. Try eBay.

In fact, your own computer may well be participating in a DDoS attack right now. You may, for example, have inadvertently downloaded a trojan—a hard-to-detect, tiny piece of software—that has allowed someone else to take control of your machine, without obvious effect on your computer's speed or operations. Some computer experts put the upper limit of infected computers as high as a quarter of all computers connected to the Internet.

Because a single computer is inconsequential, the infected computers form "botnets"—nets of robots—that can receive directions from a command-and-control center—usually just another computer on the network with the power to give commands. What makes the latest generation of botnets hard to defeat is that every infected computer can assume the role of the command-and-control center: old-fashioned methods of decapitation do not work against such dispersed command-and-control. Moreover, botnets are strategic: when network administrators try to block the attacks, botnets can shift to unprotected prey. Commercial cyber-security firms are trying to keep up with the changing threats; thus far, however, the botnets are staying at least one step ahead.

DDoS threats have been far more commercial than political. The driving force has been cyber-gangs (many of them based in the former Soviet Union and Southeast Asia) which are in the extortion business. They find a profitable Internet business that cannot afford downtime and threaten to take down its Web site(s) with DDoS attacks. The online gambling industry—by some estimates, a $15-billion-a-year business—is a particularly appealing target because it is illegal in the United States: it cannot seek protection and take advantage of robust U.S. communications infrastructure. Thus, administrators of popular gambling sites commonly receive threats of DDoS attacks and demands for $40,000-$60,000 to "protect" the sites from attacks during peak betting periods (say, before big sporting events such as the Super Bowl). Many legitimate businesses fall victim to cyber-extortion, too. Since it is better to dole out a little cash to stop future attacks than to deal with the PR fallout—and possible drop in stock prices—that usually follows cyber-attacks, cyber-crime is underreported and underprosecuted.

The risks to online freedom of expression may be considerable: saying anything controversial may trigger cyber-attacks that your adversaries can purchase easily.

Another commercial opportunity for cyber-gangs is the creation of a large army of for-hire botnets, with extremely powerful attack capabilities. It is currently quite straightforward to rent the destructive services of a botnet ($1000/day is a going rate). The point was made forcefully by a controversial recent experiment: a group of BBC reporters purchased the services of a botnet 22,000 infected-computers strong from a vendor of cyber-crime services and used it to attack the site of a cyber-security company.

The commercial availability of DDoS-attack capability has generated excitement about political applications. The risks to online freedom of expression may be considerable: saying anything controversial may trigger a wave of cyber-attacks that your adversaries can purchase easily. These attacks are financially burdensome and politically disabling for the victim. Getting your server back online is usually the least of your problems. Your Web hosting company may kick you off its servers because the cost of dealing with the damage caused by cyber-attacks usually outweighs the monetary gains of hosting controversial groups, from political bloggers to LGBT groups to exiled media from countries such as Burma (just to mention some recent victims of DDoS attacks). Protection from DDoS is available, but usually too expensive for nonprofits.

An alternative to expensive DDoS protection is a kind of distributed defense network. Imagine an idealized world in which every computer has the latest anti-virus update and where users do not open suspicious attachments or visit dubious Web sites. Cyber-gangs would then be left to their own devices—to attacking with computers they own—and the security issues would be considerably diminished. This perfect world is impossible to achieve, but the right policies could get us pretty close. One option is to go "macro"—to ensure that all critical national infrastructure is prioritized and protected, with extremely flexible resource allocation for the key assets (part of the job of a cyber-czar). This, however, would do little to curb the DDoS market. Indeed, it might embolden the attackers to ratchet up their capabilities. An alternative is to go "micro"—ensure that people who are responsible for the creation of this market in DDoS attacks in the first place (i.e., you and me) are knowledgeable (or at least literate) in cyber-security matters and do not surf with their antivirus protection turned off. This latter solution could eliminate the problem at root: if all computers were secure and computer users careful, botnets would significantly shrink in size. This, however, is a big "if," and most skepticism over whether the federal government is well-placed to educate about these threats is justified.

The security threats from DDoS attacks pale in comparison with the *potential* consequences of another kind of online insecurity, one more likely to be associated with terrorists than criminals and potentially more consequential politically: data breaches or network security compromises (I say "potential" because very few analysts with access to intelligence information agree to speak on the record). After all, with DDoS, attackers simply slow down *everyone's* access to data that are, in most cases, already public (some data are occasionally destroyed). With data breaches, in contrast, attackers can gain access to private and classified data, and with network security compromises, they might also obtain full control of high-value services like civil-aviation communication systems or nuclear reactors.

Data breaches and network security compromises also create far more exciting popular narratives: the media frenzy that followed the detection of China-based GhostNet—a large cyber-spying operation that spanned more than 1250 computers in 103 countries, many of them belonging to governments, militaries, and international organizations—is illustrative. Much like botnets, cyber-spying operations such as GhostNet rely on inadvertently downloaded trojans to obtain full control over the infected computer. In GhostNet's case, hackers even gained the ability to turn on computers' camera and audio-recording functions for the purposes of remote surveillance, though we have no evidence that attackers used this function.

In fact, what may be most remarkable about GhostNet is what did *not* happen. No computers belonging to the U.S. or U.K. governments—both deeply concerned about cyber-security—were affected; one NATO computer was affected, but had no classified information on it. It might be unnerving that the computers in the foreign ministries of Brunei, Barbados, and Bhutan were compromised, but the cyber-security standards and procedures of those countries probably are not at the global cutting edge. With some assistance on upgrades, they could be made much more secure.

In part, then, the solution to cyber-insecurity is simple: if you have a lot of classified information on a computer and do not want to become part of another GhostNet-like operation, do not connect it to the Internet. This is by far the safest way to preserve the integrity of your data. Of course, it may be impossible to keep your computer disconnected from *all* networks. And by connecting to virtually any network—no matter how secure—you relinquish sole control over your computer. In most cases, however, this is a tolerable risk: on average, you are better off connected, and you can guard certain portions of a network, while leaving others exposed. This is Network Security 101, and high-value networks are built by very smart IT experts. Moreover, most really sensitive networks are designed in ways that prevent third-party visitors—even if they manage somehow to penetrate the system—from doing much damage. For example, hackers who invade the email system of a nuclear reactor will not be able to blow up nuclear facilities with a mouse click. Data and security breaches vary in degree, but such subtlety is usually lost on decision-makers and journalists alike.

Hype aside, what we do know is that there are countless attacks on the government computers in virtually every major Western country, many of them for the purpose of espionage and intelligence gathering; data have been lost, compromised, and altered. The United States may have been affected the most: the State Department estimates that it has lost "terabytes" of data to cyber-attacks, while Pentagon press releases suggest that it is under virtually constant cyber-siege. Dangerous as they are, these are still disturbing incidents of data loss rather than seriously breached data or compromised networks. Breakthroughs in encryption techniques have also made data more secure than ever. As for the data loss, the best strategy is to follow some obvious rules: be careful, and avoid trafficking data in open spaces. (Don't put important data anywhere on the Internet, and don't leave laptops with classified information in hotel rooms.)

Gloomy scenarios and speculations about cyber-Armaggedon draw attention, even if they are relatively short on facts.

Although there is a continuous spectrum of attacks, running from classified memos to nuclear buttons, we have seen no evidence that access to the latter is very likely or even possible. Vigilance is vital, but exaggeration and blind acceptance of speculative assertions are not.

So why is there so much concern about "cyber-terrorism"? Answering a question with a question: who frames the debate? Much of the data are gathered by ultra-secretive government agencies—which need to justify their own existence—and cyber-security companies—which derive commercial benefits from popular anxiety. Journalists do not help. Gloomy scenarios and speculations about cyber-Armaggedon draw attention, even if they are relatively short on facts.

Politicians, too, deserve some blame, as they are usually quick to draw parallels between cyber-terrorism and conventional terrorism—often for geopolitical convenience—while glossing over the vast differences that make military metaphors inappropriate. In particular, cyber-terrorism is anonymous, decentralized, and even more detached than ordinary terrorism from physical locations. Cyber-terrorists do not need to hide in caves or failed states; "cyber-squads" typically reside in multiple geographic locations, which tend to be urban and well-connected to the global communications grid. Some might still argue that state sponsorship (or mere toleration) of cyber-terrorism could be treated as *casus belli*, but we are yet to see a significant instance of cyber-terrorists colluding with governments. All of this makes talk of large-scale retaliation impractical, if not irresponsible, but also understandable if one is trying to attract attention.

Much of the cyber-security problem, then, seems to be exaggerated: the economy is not about to be brought down, data and networks can be secured, and terrorists do not have the upper hand. But what about genuine cyber-warfare? The cyber-attacks on Estonia in April-May 2007 (triggered by squabbling between Tallinn and Moscow over the relocation of a Soviet-era monument) and the cyber-dimension of the August 2008 war between Russia and Georgia have reignited older debates about how cyber-attacks could be used by and against governments.

The Estonian case is notable for the duration of the attacks—the country was under "DDoS-terror" for almost a month, with much of its crucial national infrastructure (including online banking) temporarily unavailable. The local media and some Estonian politicians were quick to blame the attacks on Russia, but no conclusive evidence emerged to prove this. The Georgian case—widely discussed as the first major instance of cyber-attacks (primarily DDoS) accompanying conventional warfare—has barely lived up to its hype. Many Georgian government Web sites were, in fact, targets of severe DDoS attacks. So was at least one bank. Yet, the broader strategic importance of such attacks within the Russian military operation is not clear at all, nor did Russia acknowledge responsibility for the attacks.

Although the attacks on Estonia and Georgia are often grouped together—perhaps because of the tentative Russian involvement in both—they are also very different. One important difference is in the degree of technological sophistication of the two countries. Attacking the Internet in Estonia, which made Internet access a basic human right in 2000, is like attacking the banks in Lichtenstein: the country's economy, politics, and even some emergency services are pegged to it so tightly that being offline is a national calamity.

Georgia, on the other hand, is a technological laggard. When Georgia's major government Web sites became inaccessible during the war, the Foreign Ministry was slow in finding a temporary home on a blog. The lapse may have gone largely unnoticed: 2006 Internet statistics gathered by the United Nations show that Georgia had about seven Internet users per one hundred population compared to 55 in Estonia and 70 in the United States. The Georgian case also highlights the danger of drawing too many strategic lessons from cyber-attacks. After all, one common result of the loss of Internet access is power outages, common during wartime regardless of cyber-attacks.

Moreover, both Georgia and Estonia are in a sense "cyber-locked," with limited points of connection (even in Estonia) to the external Internet. This limited connectivity and the two country's dependence on physical infrastructure heighten their vulnerability. Less cyber-locked nations do not face the same risk. As Scott Pinzon, former Information Security Analyst with WatchGuard Technologies, told me, "If Georgia or Estonia were enmeshed into the Internet as thoroughly as, say, the State of California, the cyber-attacks against them would have been reduced to the level of nuisance." The smartest way to guard against future attacks may, then, be to build robust infrastructure—laying extra cables, creating more Internet exchange points (where Internet service providers share data), providing incentives for new Internet service providers, and attracting more players to sell connectivity in places that now have limited infrastructure. The United States has actually done quite a bit of this already, so the Estonian experience may have little to teach Americans. While it might benefit Estonia and some other countries to invest heavily in upgrades, the United States may be able to forego dramatic and costly changes in favor of regular maintenance and incremental improvements.

Quite apart from the technological issues of cyber-warfare, there is the question of what even constitutes cyber-war. How do existing legal categories apply in this new setting?

Using the metrics of conventional conflicts to assess these attacks is not easy. How severe must the damage be in order for the cyber-attacks to qualify as armed attacks?

For largely geopolitical reasons, Estonia initially called the cyber-attacks a cyber-war, a move that now seems ill-considered (on a recent trip to Estonia, I noticed that Estonian officials had replaced the term "cyber-war" with the more neutral "cyber-attacks"). The militarization of cyberspace that inevitably comes with any talk of war is disturbing, for there is no evidence yet to link the current generation of cyber-attacks to warfare, at least not in the legal sense of the term. However, the attacks on Estonia and Georgia did each pose an intriguing legal question, and neither has yet been answered definitively. First, do

cyber-attacks constitute a "use of armed force" as understood by international law (the Estonian case)? Second, what kind of cyber-attacks are allowed under the laws of war once the conflict has already begun (the Georgian case)?

The first question is the trickiest. Commenting on the attacks, the Estonian defense minister said "such sabotage cannot be treated as hooliganism, but has to be treated as an attack against the state." But did the cyber-attacks constitute the beginning of an armed conflict, as understood by the Geneva Conventions or Article 51 of the United Nations Charter? If the cyber-attacks constituted an armed attack, Estonia's NATO allies should have followed Article 5 of the North Atlantic Treaty, which treats an attack against one member state as an attack against all and calls for collective defense. NATO only sent a team of experts to assess the damage. Using the metrics of conventional conflicts to assess the severity of these attacks is not easy. How intense and severe must the damage be in order for the cyber-attacks to qualify as armed attacks? Does damage in cyberspace qualify, even in the absence of offline damage? Is inconvenience to Internet users enough? What about the duration of the attacks?

However such questions are answered, the aggrieved party would still have to prove that a cyber-attack was state-sponsored, and it is unclear how one makes this argument in a legally convincing fashion. Are states only responsible for actions they directly control? Are they also responsible for all cyber-activity in their territory? And how far does that responsibility extend? At least one computer with an IP address belonging to the Russian government was identified as part of a botnet used in the Estonian attacks, but it is hard to build a case for Russian government responsibility on that IP address alone, since there were thousands of other participating computers.

If state involvement cannot be proven beyond doubt, cyber-attacks should be treated as crimes and dealt with under national and, in some cases, international criminal law. But there are difficulties on this front as well. For example, unlike Estonia and many countries, Russia has never signed the Council of Europe Convention on Cybercrime, which is the first international treaty seeking to harmonize national laws and facilitate cross-border cooperation among states on issues of cyber-crime. This makes it impossible to hold Russia to the standards envisioned in the Convention, and international law also provides few mechanisms for punishment.

The second question—what kinds of attacks would be allowed under the law of armed conflict?—presents another theoretical challenge, though for now at least, existing legal standards may suffice to address the issues.

Common sense dictates that the severity and targets of such attacks should be guided by international law, particularly the Geneva Conventions and associated protocols. Broadly speaking, current norms state that the conduct of war must meet three fundamental standards: belligerents must *distinguish* military from civilian objects when selecting targets; *balance* military necessity with humanitarian concern (the choice of weapons is not unlimited and must be made with the avoidance of unnecessary suffering in mind); and shun the use of force that is *disproportionate*, in the sense that it shows insufficient

attention to the unnecessary suffering that might result. These principles have proved very hard, but not impossible, to interpret in conventional conflict; applying them to cyberspace is not an insurmountable challenge.

The careful application of these three principles to the conduct of war could explain why militaries might shy away from cyber-attacks. First, it is hard to predict the consequences of such attacks; cyber-attacks typically lack surgical precision and are notorious for side effects—a virus planted in a military network could easily spread to civilian computers, causing much unanticipated collateral damage.

Second, precisely targeted cyber-attacks could be a more humane way of conducting warfare. Instead of bombing a military train depot, with collateral civilian deaths, one can temporarily disable it by hacking into its dispatch system. However, the rules of war also stipulate that once a belligerent has used a more humane weapon, it ought to use that weapon in similar situations—and who would voluntarily abandon tanks in favor of computers only?

Third, most cyber-attacks are hard to justify in strategic terms and therefore would open associated personnel to prosecution for war crimes. For example, if there is little to be gained from attacking a poorly maintained Web site of the Georgian parliament, Russia could not justify an attack on it in military terms. If it went ahead with such an attack, its commanders woul risk prosecution for a disproportionate use of force.

The Internet does create one complexity worth considering in the context of applying existing laws of war: civilians on both sides can now participate in hostilities remotely. At the height of the war with Georgia, Russian blogs were full of detailed instructions on how to enlist in the cyber-war effort. Currently, humans are of little value in this process: a conventional botnet attack is more damaging. Yet, it is possible that human-powered botnets—or "meatbots"—could soon play a more serious role. Would participants then be liable for war crimes for their actions as civilians, who, unlike combatants, do not enjoy immunity under the law of war for their participation in hostilities? Would such civilian actions fall under the category of "direct participation in hostilities," outlined in Commentary to Additional Protocol I to the Geneva Conventions ("Direct participation in hostilities implies a direct causal relationship between the activity engaged in and the harm done to the enemy at the time and the place where the activity takes place")? We may need a special clarification of this concept for cyberspace, but other metrics—the damage caused, the targets chosen, and so forth—could still apply.

There is a line between causing inconvenience and causing human suffering, and cyber-attacks have not crossed it yet.

The legal options are also complicated in the case of classical rather than meatbot-powered DDoS attacks because there are often at least five parties to it: attackers, computer users whose machines are enlisted by the attackers, target Internet sites, software vendors responsible for the exploited security vulnerabilities, and various Internet service providers who deliver the attack traffic. These parties have different

degrees of responsibility, and some of them are liable for negligence, itself a murky legal area.

Putting these complexities aside and focusing just on states, it is important to bear in mind that the cyber-attacks on Estonia and especially Georgia did little damage, particularly when compared to the physical destruction caused by angry mobs in the former and troops in the latter. One argument about the Georgian case is that cyber-attacks played a strategic role by thwarting Georgia's ability to communicate with the rest of the world and present its case to the international community. This argument both overestimates the Georgian government's reliance on the Internet and underestimates how much international PR—particularly during wartime—is done by lobbyists and publicity firms based in Washington, Brussels, and London. There is, probably, an argument to be made about the vast psychological effects of cyber-attacks—particularly those that disrupt ordinary economic life. But there is a line between causing inconvenience and causing human suffering, and cyber-attacks have not crossed it yet.

The usefulness of cyber-attacks as a military tool is also contested. Some experts are justifiably skeptical about the arrival of a new age of cyber-war. Marcus J. Ranum, Chief Security Officer of Tenable Network Security, argues that it is pointless for superpowers to develop cyber-war capabilities to attack non-superpowers, as they can crush them in more conventional ways. As for non-superpowers, their use of cyber-capabilities would almost certainly result in what Ranum calls "the Blind Mike Tyson" effect: the superpower would retaliate with offline weaponry ("blind me, I nuke you"). If Ranum is right, we should forget about the prospect of all-out cyber-war until we have technologically advanced superpowers that are hostile to each other. Focusing on cyber-crime, cyber-terrorism, and cyber-espionage may help us address the more pertinent threats in a more rational manner.

In the meantime, those truly concerned about the future of the Internet, global security, and e-Katrinas would be advised to watch a recent *South Park* episode, in which the Internet suddenly disappears and hordes of obsessed families head to the Internet Refugee Camp in California, where they are allowed to browse their favorite Web sites for 40 seconds a day, while the military fights the no-longer-blinking giant Internet router. Finally, a nine-year-old boy plugs the router back in, and its magic green light returns. This would make a sensible strategy for many governments, which are all-too eager to adopt militaristic postures instead of focusing on making their own Internet infrastructures more robust.

BIOGRAPHY FOR JIM HARPER

As Director of Information Policy Studies at the Cato Institute, Jim Harper focuses on the difficult challenges of adapting law and policy to the unique problems of the information age. Harper is a member of the Department of Homeland Security's Data Privacy and Integrity Advisory Committee. His work has been cited by *USA Today*, the Associated Press, and Reuters. He has appeared on Fox News Channel, CBS, and MSNBC, and other media. His scholarly articles have appeared in the *Administrative Law Review*, the *Minnesota Law Review*, and the *Hastings Constitutional Law Quarterly*. Recently, Harper wrote the book *Identity Crisis: How Identification Is Overused and Misunderstood*. Harper is the Editor of *Privacilla.org*, a web-based think tank devoted exclusively to privacy, and he maintains online federal spending resource *WashingtonWatch.com*. He holds a J.D. from UC Hastings College of Law.

DISCUSSION

Chair WU. Thank you very much, Mr. Harper. And at this point, we will open for our first round of questions, and the Chair recognizes himself.

You each referred at least in part to cybersecurity performance metrics, and apparently we have not been as good at developing them as we should. What have been some of the impediments and how can we be better off if we are better at developing them?

Mr. WILSHUSEN. Well, I guess I will start. One of the things about the metrics that have been developed by OMB for FISMA reporting purposes is that the metrics themselves probably served a useful purpose when they were first developed, and this was several years ago. The ones they had developed were primarily implementation-related metrics that addressed whether or not a control has been activated and implemented.

When they were first developed several years ago, many of the federal agencies were not performing some very basic security controls. And so over the intervening years as agencies increasingly performed these control activities, it is natural to start taking a look at these metrics and see, do they need to evolve as well? Is there a need to continue to report whether or not agencies are implementing specific controls when they are all up in the 90-plus percentile of performing these controls over their systems?

So now it is important to look at, well, how well are these agencies implementing these controls and looking at different types of measures. We have an engagement that is ongoing right now, looking at how leading organizations develop and use metrics to gauge and monitor their information security activities and will be issuing a report later this summer about that particular topic. But one thing that we have noted previously is that it is probably time to start measuring how well agencies are actually implementing controls and the effectiveness of the control activities, rather than just mere implementation of those specific control activities.

Chair WU. Several of you referred to having a unified standard or set of standards for the Federal Government, that is, we currently have a division between defense applications and civilian governmental applications, and I just wanted to confirm that is a consensus view of the panel, that the division between DOD and NSA (National Security Agency) on the one hand, and DHS and NIST on the other, is maybe one rooted in jurisdiction but not rooted in utility or the sense of the field.

Mr. CHARNEY. Yeah, I would agree with that. As the Co-Chair of the CSIS (Center for Strategic and International Studies) Commission on Cyber Security, one of the things we noted, there were historical reasons in the past why there was a clear delineation between the national security world and the civilian world. But to some extent, in cyber networks, a lot of these things tend to merge together. And when you are trying to devise the best security practices, you want to take all of your great capabilities and knowledge and bring that together and have holistic programs in cybersecurity. So bringing them together is helpful.

Chair WU. And I would like to walk that over a little bit further. Getting to the civilian non-governmental sector, my understanding is that there are different cybersecurity standards for different fields, whether you are dealing with health care, banking, and these have developed over time. Would there be a utility in developing consensus standards for cybersecurity for the civilian non-governmental sector, and Mr. Harper may not like this, or will that field de facto borrow what governmental standards exist or is it not possible to better develop cybersecurity standards for that field at this point in time?

Mr. CHARNEY. No, I actually think it is possible. One of the things that we have done at Microsoft is we looked at the different regulations that impose certain security requirements on information systems. So you have things like Graham Leach Bliley for financial data, you have PCI, which is the credit card standard for securing credit card data, you have HIPAA (*Health Insurance Portability and Accountability Act*) for health care data. It turns out most of these regulations actually promote the same concepts in terms of the framework, which is reasonable security controls based on traditional risk management principles.

So what we did is we looked at all those laws and then we mapped the controls that are necessary to an international standard. ISO standard 27001 by the International Standards Organization is a standard for controls around IT systems. And we have actually gotten ISO certification for one of our largest properties and networks.

So I think the short answer is there is a lot of similarity in these regimes. Having a unified standard that people can map to is a good and healthy thing, and the other nice thing, of course, is the threats of all of those standards can always be modified to address new environments.

Chair WU. Well, I see nodding heads there. I just want to ask one quick follow-up on this topic before I yield to Mr. Smith. Would NIST and NIST's existing activities in the field be a logical place to begin working on consensus private-sector standards? Anyone on the panel?

Mr. BREGMAN. I think so, but I think it has to be done in collaboration with the private sector, and I think it is a logical place to bring together the various constituencies to coalesce the standards into an overarching set of security guidelines and standards.

Chair WU. Mr. Wilshusen, Mr. Charney, Mr. Harper, any comments on that?

Mr. WILSHUSEN. I would also agree, and NIST does have a mechanism in place where it coordinates and collaborates with the

International Standards Organizations, or ISO rather, and it would be a logical place to start.

Mr. HARPER. I will voice the concern that I think you anticipated from me. Federal-developed standards should be available to the private sector and perhaps produced in collaboration with the private sector. There is a touch of concern, though, that the Federal Government, as a large market actor, would drive standards into the marketplace that don't meet the needs on the other side of the security equation which include privacy and anonymity and that kind of thing.

So standards are important, they are good, but it is not a given that all federal-developed standards should be imported into the marketplace. They have to go through a different series of tests for private adoption, I think.

Chair WU. Yeah, what we are working on here is the divide between the public sector and the private sector, and NIST traditionally has played a light leadership role in assisting the private sector to develop consensus, bottom-up developed standards from players in particular arenas. At least that is what I was asking about, and I take that to be the answers of the other panelists. Mr. Charney.

Mr. CHARNEY. Yes, if I could just say I think you are right. It is one thing for NIST to develop standards for the government's own use, but to be clear, NIST also participates in international standards organizations with members of industry. So if you are looking at standards that would apply more broadly than the government, there are four that already exist to do that. The government and industry participates in that, so the mechanism is there to work it through that process.

Chair WU. Thank you very much. Mr. Smith, you are recognized for five minutes.

Mr. SMITH. Thank you, Mr. Chair. Mr. Harper suggested in his testimony that the critical infrastructure vulnerabilities should be addressed by physically separating such infrastructure from the public Internet as similar to the DOD network. What is your response to that, Mr. Charney and Mr. Bregman and Mr. Wilshusen?

Mr. BREGMAN. I think it is impractical in many cases because it is one thing in the realm of DOD or the intelligence community to operate in a separate environment, but in many cases, other parts of government have to interact with citizenry, they have to interact with private sector in the course of their normal operations. And the challenge in cybersecurity is, as soon as I connect my perhaps well-defended, well-defined network to someone else, I have opened myself up to vulnerabilities that may be present in the other components that I don't control. And so there is a real risk in isolating government function in the attempt to achieve this security through isolation and becoming much less effective.

So I think the real challenge is finding ways to develop security and secure the cyber infrastructure, even in a world in which it isn't an isolated, totally controlled environment for the government.

Mr. CHARNEY. I would echo those points, and if you think about some of the evolving models, like a Smart Grid, for example, where people's homes can communicate intelligent power consumption information to the power grid so that they can draw power at appro-

priate times or feed power back into the grid, I don't know how you do that by creating a power infrastructure that is isolated from all the citizens that need to connect to it. I think the trend of these private critical infrastructures are basically becoming Internet enabled because of the huge business imperative, efficiency cost-drivers and other things that are really critical to the success of these new technologies.

Mr. WILSHUSEN. And it is our experience, too, in the reviews that we have done at the Tennessee Valley Authority when we looked at the control systems and the security over the control systems that the trend is to go to more IP-based type of systems to run these control systems. Now, while that is—it really helps and serves additional benefits to the company to enable such control protocols, but it also raises the risk because of the risk associated with running those IP-based systems can now extend to control systems. So agencies need to make sure that they assess those risks and take the appropriate steps to secure against and mitigate those risks. But certainly due to the benefits, the trend seems to be going more toward an IP-based type of network and structure.

Mr. SMITH. Mr. Harper.

Mr. HARPER. I would anticipate these criticisms of what I had said, and they are not wrong, they are not unfair. And the way I thought about it was that criticality should be a very, very tightly circumscribed adjective, and I have dealt with it a little bit in my written testimony, though I wouldn't call myself an expert. Criticality should be when there is an immediate and proximate danger to life and health from the loss of an asset. That is under basically a definition that I have worked on. There is a lot of history behind it that didn't go into my testimony which is why there is a lot of stuff out there that is referred to as critical infrastructure that I would not.

But if again, something would immediately injure life and health proximately, so the example of an electrical grid going down, it could kill people in a hospital, for example, to lose electric power for an hour, people who are on a heart-lung device, that kind of thing. Well, it is not proximate because what you do for a likely risk like that is you put electrical infrastructure at the hospital that would take care of things when the broader infrastructure went down.

So again, these are fair comments. I think the critical infrastructure should be very tightly defined to a small universe of assets.

Mr. SMITH. Okay. Thank you. And another one, we heard that liability is preferable to regulation as a tool for internalizing any market failures that exist in terms of private-sector cybersecurity. I was wondering, Mr. Bregman and Mr. Charney, how do Symantec and Microsoft feel about this, if you could elaborate?

Mr. CHARNEY. So we have repeatedly said that you have to think about different ways to motivate the markets to do the right thing, and there are many ways to do that, everything from incentives to regulation and liability. The biggest challenge in the software industry I believe is that software is extremely complex and it is not entirely clear what the reasonable practice would be in developing security today and how you could apply them uniformly in the spectrum of people who make software. So it is not just about large

companies. I mean, one of the great things about the Internet is it creates this incredible innovative environment where people in their garage can develop software and distribute it around the globe. And this has led to a lot of great, innovative technologies. And I don't know how they survive under a regime that is laden with a lot of up-front costs.

Having said that, I think there are better ways to get there. One of the things that we have been active proponents of is reforming Common Criteria, which is the method by which the government evaluates products for security and that then affects purchasing acquisitions in the government. And I think if the government wants to drive better security practices, one of the ways to do that is to use Common Criteria reform and acquisition regulations to achieve that result. I think that drives a much more effective and efficient process. It also allows, you know, still a very innovative and low barrier to entry environment.

Mr. BREGMAN. I would echo Mr. Charney's remarks, but I would add two other things. I think not only is software very complex, but any software that is delivered by a supplier becomes part of an even more complex integrated solution, and in most cases where we have seen vulnerability at the system level, it is traceable to configuration that is outside the core of any given product, but it is the interaction in the customer's environment or in the user's environment which opens up the vulnerabilities. That is something that is very hard to legislate liability around without putting tremendous constraints on what people are willing to supply.

And related to that I think, and I was also echoing Mr. Charney's remarks, liability as a way to control this will stifle a lot of the innovation which is what we need in order to get ahead of the threat. And so I would be fearful that if liability were to be the tool primarily used to improve security, we would actually see the opposite effect. There would be retrenchment on the part of suppliers and fear to try innovative, new solutions.

Mr. SMITH. So maybe I hear you saying you would not advocate liability in addition to regulation?

Mr. BREGMAN. That is correct.

Mr. SMITH. Mr. Wilshusen, can you elaborate on your findings on the impact of such things?

Mr. WILSHUSEN. Yes, in a couple areas. One, regarding the use of Common Criteria, we did a review several years ago looking at the National Information Assurance Program, or NIAP, which is a program in which NIST and NSA at that time established and certified laboratories to examine the security controls that were designed into these products. One of the problems that we identified as a challenge to overcome was just the length of time that it took these laboratories to go through and evaluate the security of these products. In many of these cases, some of the vendors indicated that by the time they went through the process, the technology and the applications were already obsolete. There were newer versions out there. So to implement that, we are going to need to have some sort of measure and mechanism that will allow a speedy and a quicker response time to evaluate such products.

There is also another mechanism that government can use, in addition to providing incentives, through its procurement policy.

The government procures $60, $70 billion worth of IT products and services a year. It can use that leverage and specify the requirements that it needs, or security requirements for the products that it requires which can help maybe move markets into an area where they implement security or design security into their products more readily.

Mr. SMITH. Thank you. Thank you, Mr. Chair.

Chair WU. Thank you, Mr. Smith. We have had several different cybersecurity czars, and at least a couple of them have departed or resigned. Can the panel comment on whether there is integral problems in the way that we have tried to structure a cybersecurity program at the federal level?

Mr. WILSHUSEN. I will tread lightly here, but I think one of the issues that may be resolved as we go forward with the new official, the cybersecurity official in the White House, one of the concerns is going to be what authorities and what control he or she will have over budgets and strategy and what will be his or her levers of power to effect change? And I don't know if decisions about that exist, but that would be just one of the challenges I will say in trying to make sure that conditions are established to where the official can be productive in that role.

Chair WU. Well, Mr. Wilshusen, you are from the GAO, and you are supposed to give it to us unvarnished. What I am hearing between the lines is that this is a difficult field with a lot of responsibility and perhaps not enough line authority in budget to accomplish the mission or the multiple missions.

Mr. WILSHUSEN. And it will depend upon what their role and responsibilities are, I would agree.

Chair WU. Mr. Bregman, do you have anything to add to this?

Mr. BREGMAN. I would agree with that. I think appropriate decision-making and budget authority is going to be necessary because a key part of the role is helping coordinate the strategic direction across the various parts of government and also, coordinating better on an international front. One of the challenges is this is not a problem that occurs just within our own borders. It is borderless. And so better coordination globally is going to be an important part of this as well.

Chair WU. Thank you. Several of you referred to the importance of public-private partnerships and coordinating with the private sector. What in our structure today is not creating the kinds of public-private partnerships that we need and what kind of incentives should we try to build in?

Mr. CHARNEY. Since the early '90s, we have been talking about this public-private partnership, and it was really a reflection of the fact that the private sector designs, deploys, and maintains about 90 percent of the critical infrastructure.

And so government is in an interesting situation here, unlike things like nuclear weapons where they had both responsibility and control, here they have responsibility for public safety and national security but they don't control the assets to be protected or maintained.

And so the idea of a partnership is the right idea. I think it got off on the wrong foot. In large part, early efforts at partnership were focused on information sharing, and there was a lot of discus-

sion that industry and government should share information about threats and vulnerabilities.

The problem is information sharing is not an objective, it is a tool. You share information so you can do something. Sharing information just for the sake of sharing information doesn't make any operational change that makes security better. So the first problem is the wrong focus, focus on sharing instead of action.

The second thing is that the government has been concerned for understandable reasons about not playing and picking favorites in the marketplace. So it often took the view that it has to share with everyone or no one. And of course, when you share with everyone, when you share a lot of information about vulnerabilities, threats and risks too broadly, you actually make the problem worse, and if you share with no one, then there is nothing.

And so I think in addition to focusing on what information to share, that is, how is this information actionable, the next question is who is it actionable by and we have to share it with the organizations, people, companies, whatever, who can do something with the information specifically and not worry so much about sharing with everyone or no one because that is not a productive model.

Chair WU. Mr. Charney, is one of your criticisms of the current advisory committees and coordinating committees that they are mechanisms for sharing information and that that becomes an end-goal rather than a tool for accomplishing mission objectives?

Mr. CHARNEY. That is correct, although there has been effort in recent times to refocus on more operational security issues and share actionable information, but there was a long history of having the wrong focus.

Chair WU. Thank you. I might have a couple more questions, but at this time I am going to yield to my colleague, Mr. Smith, for five minutes.

Mr. SMITH. If Mr. Charney or others would still like to maybe elaborate on what exactly the partnership would look like, I mean, I think you started down that track. But obviously it can be difficult to define. I know that sometimes partnerships are overstated here on the hill, but if you could elaborate?

Mr. CHARNEY. I would be delighted to. In addition to the misfocus, I don't think the partnership ever had the right philosophical underpinning. Here is the way I see the problem. Markets actually do deliver some level of security. Customers demand it and markets deliver it. Governments need a level of security for public safety and national security that often exceeds what the market will provide. Markets are not designed to do national security. You cannot make a market case for the Cold War. In those situations, the government steps in and does things. It seems to me that the proper basis of a partnership is to figure out how much security you are going to get from the market through its natural proclivities and a little more because companies do have a sense of corporate responsibility. They do care about public safety and national security, so they do a little more than the markets would require. Then you have to figure out what the government thinks it really needs, and the key is filling the gap between what the market will provide and what the government sees as necessary. And then there are a lot of ways to fill that gap. Acquisition regulations are

an example to drive the market in a particular direction, regulation, standardization. There are many ways to fill a gap, tax incentives.

So the real key, and I think the basis of the partnership, is to focus on meeting the requirements that span between where markets are and what government wants and figure out the right way to incentivize the right behaviors so the products take you where you want to go.

Mr. SMITH. Any one else?

Mr. HARPER. I will briefly comment on it some more. I think the question of public-private partnerships—I agree in large part with what Mr. Charney said, that partnerships formed up to share information as if that was the goal. The problem is goal-setting and then asking what achieves that goal, and I think it has been the idea, well, let us have a public-private partnership.

In an area I have a relative amount of experience, Homeland Security issues. Everyone said data sharing, you know, connect the dots, and nobody knows exactly what that means. It is a more difficult problem.

I would prefer to see the government play the role of partner that you see in security of houses and buildings in a given city. The primary responsibility is on the holder of private infrastructure to secure the house with locks on the windows and doors, and when something really goes wrong and there is criminal behavior afoot, the police are called or if the police have information about what is afoot, they contact the community. That is a public-private partnership that I think is a success, but putting together programs to try to describe that don't really work. What works is when the government stays in its law enforcement and national security role for the most part, and the private sector for the most part takes the role of securing its own infrastructure. That doesn't mean they can't work together, but I don't think the focus has to be on them working together to improve security It works with them separately.

Mr. SMITH. Thank you. Mr. Bregman, relevant to EINSTEIN and the program there and the software, obviously it was developed a number of years ago and the focus was on threats and intrusions, and perhaps that is not enough of a focus now. Would you concur with that?

Mr. BREGMAN. I think we see a very, very rapidly evolving threat landscape, and EINSTEIN was developed with somewhat looking at the then-current threat landscape. And so given the long lead time and deployment lead time, it is not taking advantage of the best practice, best technologies that are currently available in the private sector. And I think that is an area where, again, private sector working together with government could do a much better job of looking forward, anticipating things, and being closer to the leading edge of protection as opposed to looking backward at what the previous threats were and then going through a rather cumbersome development process to deploy something which is inadequate when it is deployed.

Mr. SMITH. Okay. Thank you.

Chair WU. Several of you have referred to the importance of setting goals rather than processes. And also I think there has been

reference to having a more crisp strategy for cybersecurity. What are the components that we need to put together to develop a strategy or a means of accomplishing a clear set of goals?

Mr. CHARNEY. It seems to me there are two separate issues, and it comes back to a comment in my testimony about the government as a policy arm and the government as a large IT enterprise. So part of the goal of developing a comprehensive strategy is recognizing that the way cyberspace works today, there are some very interesting challenges about how you secure it and also respond to incidents.

I will give you a somewhat classic example. There have been widespread reports in the media about attacks on U.S. Defense Department systems. There are a lot of interesting questions about what constitutes cyber warfare. When can you shoot back? What does it mean to do collateral damage on the Internet? These are hard policy questions, and it is even an interesting question of whether or not you want to respond in a cyber way or impose a trade sanction. You know, because cyberspace of course ties all our economies together, just like it ties all our systems together. And so the government has to think very holistically about diplomatic efforts, intelligence efforts, military efforts, economic efforts, and law enforcement efforts and integrate them into a strategy and set norms because right now around the world we now have norms on certain behaviors, like proliferation of weapons of mass destruction or proliferation of nuclear material. We don't even have norms on what constitutes appropriate cyber conduct around the world. And as a result of that, countries internationally haven't developed the processes, procedures and strategies to deal with these issues because the Internet is sovereign agnostic, even though sovereignty is very much well and alive.

And so in the policy space, this is one of the reasons why the commission recommended the advisor has to be at the White House and could not sit in any one agency because thinking about this problem comprehensively means that the government has to think about all the tools in its arsenal and how to implement as one government. On the IT infrastructure protection side, that is when you get into very specific controls where you want security controls in place, and I would echo the comments made earlier about the need to actually test the efficacy of those controls, make sure they are doing what you think they are doing, and making sure they are always current. And as I said, there are international standards now as well as regulations that require controls be put in place. So to some extent, the more I think about some of these issues, we are reaching the point, at least in the network enterprise, where the philosophy is right, and we are getting to the point of we need to execute well and we need to focus on execution. And that requires being rigorous about putting your policies in place, testing your controls, having audits done whether they are internal, self-certifications, or external to make sure you are achieving your desired levels of security.

Chair WU. Well, I think we have surfaced a lot of concerns about the lack of—the dearth of rules of the road for the Internet, but Mr. Charney, your reference to accords about WMD (Weapons of Mass Destruction) and so on brings to mind that we have been able to

work, at least try to work, on rules for warfare for 4,000 years at least, and the early versions of the Internet are at most 30 years old, and cyberspace probably is more like in the teens than anything else.

So in essence, we are here all together at the inception, and some of the decision we make will have reverberations down the road.

Let me ask you a question about research. There is a set of challenges about identifying research priorities at DHS and commentary that this process should include private industry to a larger extent. Can you give us your best analysis of the research that is currently being done at either NIST or DHS?

Mr. BREGMAN. I think when we think about research in the cybersecurity space, there are several different objectives. There obviously is the primary objective of the research itself and the outcome of that research and with the goal that one would think of ultimately impacting technologies and products which could be delivered and implemented. And so that is an area where linking the research activities with the industrial base is important because to exploit them, there is going to have to be some commercialization that takes place.

The other dimension of research is that setting the research agenda is a very good way to stimulate along side investment, both by private sector and sort of intellectual capital investment within the academic world. And I think one of the things we need to improve our cybersecurity posture is a larger cadre of expertise at all levels, people who can be the next generation leading researchers but also practitioners in government and in private sector and carefully aligning the research agenda with the interests of DHS, NIST, and the private sector, and using that to create interest within the academic community will draw more students, some more people into that area and that field and create a much larger community of expertise.

Chair WU. Mr. Wilshusen, or anyone else, anything to add to the research agenda or research strategy?

Mr. WILSHUSEN. We haven't looked at—in fact, we just received a request to look at research and development in cybersecurity. That was a couple of weeks ago, and we are just starting a review of that within the Federal Government. But about four years ago we did a review over cybersecurity research and development and looking at the NITRD and the group that was responsible for coming up with a plan for conducting cybersecurity within the Federal Government, and we found that while there were some overall goals and objectives that were identified, there really wasn't a clear, concise plan on how to conduct and how to perform and fund which particular projects. And so making sure that there is a clear consideration of what the goals are and coming up with a plan to fund those projects I think will be important.

Mr. HARPER. Mr. Chair, if I may?

Chair WU. Yes, Mr. Harper.

Mr. HARPER. It often falls to me to be the skunk at the garden party, and I enjoy it. Research that benefits——

Chair WU. Animals of all stripes are of value.

Mr. HARPER. Research that benefits industry really is subsidy. And I want research done. I think everybody does, but research

that is funded by industry goes then into the price of products and is paid for then by the users of the security technologies, rather than taxpayers, many of which don't use the Internet and live perfectly good lives without it.

Chair WU. Mr. Charney.

Mr. CHARNEY. Yes, I actually don't disagree, and earlier I said the philosophy of the partnership should be that the government doesn't do what the market is already delivering but do something else. That is true in research, too. So industry does a lot of research, and we do research that we can monetize and commercialize. And there is other very hard research that we can't do because there is no economic model that permits it. Remember, the Internet was a government research effort which has revolutionized the world. It came out of DARPA (Defense Advanced Research Projects Agency).

So I think it is really important that the government as part of its strategy do two things, one, invest in the research that actually advances the overall strategy that we have talked about to create a more secure environment, but also do the things that industry won't do. And to be clear, Mr. Bregman's point about commercialization is not the same as financing industry research. The Internet, which was invented by the government, was then commercialized by the private sector because the government made it available. That is not exactly funding industry research. It is saying invest in things that will find a place in the commercial market so it gets widespread adoption so that everyone benefits from the research. But do research that won't otherwise happen and is consistent with your cybersecurity strategy.

Chair WU. Well, perhaps as an artifact of the Committee that I sit on, or it is a natural draw, but my bias is toward the direction that we underfund research rather than over purchase research. Compared to other, immediately pressing needs, there is the tendency to address those pressing needs, rather than something which is long-term.

Something else which we underfund publicly is education. The market would probably not fund education properly, and along those lines I think several of you mentioned the role that education, consumer education, user education, could play in improving cybersecurity at relatively low cost. Can you identify some things that we could be doing either as a society or as a government to use that education tool more effectively to enhance cybersecurity?

Mr. BREGMAN. Well, Mr. Chair, you mentioned the fact that the cyber world that we are living in today is only maybe dozens of years old, and it is changing at a pace which is much more rapid than the generational shift. And I think there is a very important role in educating our citizens on how to behave and what are the norms and what are the risks and what are the processes to use to protect oneself in the cyber world. And I think that it requires government to take the role particularly of coordinating that delivery of that education because if it delivered in a very fragmented way, it is just confusing to the populous.

Some of the programs that are in place today, NCSA and others, I think are good starting points for government collaborating with

private sectors to bring that education to the mass market citizenry.

Mr. WILSHUSEN. And there are several federal programs which allow, for example, Scholarship for Service in which the Federal Government offers scholarships and repays student loans for graduates who have studied in cybersecurity and then decide to work for the Federal Government. So there are various different programs available now, like an education assistance program, that can help bring those individuals with information security degrees into the federal workplace.

Chair WU. Thank you all very much. You have traveled a long way, and this is a large, bedeviling set of topics. We have only had the opportunity to ask a few questions and not engage across the breadth and depth of this topic. If there are things that you would like to comment on or tell us at this point, I would like to open this to all the witnesses. You can just go from left to right or right to left so that those things that you might wake up tonight or tomorrow and say, gee, I wish I had said that. This is your chance of laying it out in the record.

Mr. WILSHUSEN. One thing I would just like to add related to the research and development question that came up earlier is that the results of the research and development activities should be made available, and particularly those funded by the Federal Government. There is a requirement under the *E-Government Act* that federally funded research, particularly in the cybersecurity, maintain the results in repositories. What we found several years ago is that the results of many of the efforts were not being considered and placed into these repositories, thereby making them unavailable for other researchers who might have benefited from the knowledge gained from those research efforts.

Chair WU. Thank you.

Mr. BREGMAN. Well, I would like to start by thanking the Committee for taking on this task. I think as the Chair mentioned, it is a very complex problem and one that is changing very rapidly, and it is very important that this committee and other parts of the government focus on it.

I think there has been increased focus, and we see improvement in the work we do with DHS and with NIST and with other parts of government. We need to continue that and accelerate that momentum if we are going to be able to really protect our nation in the face of this increasing cyber threat. Thank you.

Chair WU. Thank you.

Mr. CHARNEY. Thank you. I do want to comment one further point about education, in particular. We have spent a lot of time educating consumers about some of the basic steps they can take to protect themselves on the network, and I think this is important to do and we will all continue to do it.

The challenge it seems to me is in part that IT technology is very opaque to end-users. My mother is 79 and found e-mail, bless her heart, and when I talk to her about security issues, she really does not want to become a security IT professional. She remembers the day of the telephone where it just worked and if something went wrong, the telephone company took care of it. And I think to some extent we have to think about models that provide consumers a

higher level of protection with less work. And I don't think we are going to get there unless we start thinking about some very hard problems, some of which I outlined in my testimony about things like attribution. How does my mother know where her mail really came from or who really wrote the software that is being asked to be installed on her system? And how do we think of the role of Internet service providers who are the choke points to the Internet and might be able to look at machines and clean infected machines? There are a lot of difficult, challenging things we have to do. There are some very interesting models. If you think about WHO, the World Health Organization, and the way we deal with pandemics. You know, they are called viruses and worms for a reason in the computer world because they propagate in many of the same ways. And we have to start thinking about other models that have worked and how we bring new protections to the Internet because the ability to create malicious malware and propagate it worldwide at machine speed, virtually at the speed of light, is going to continue unabated. Human beings are not going to be able to react fast enough to respond to machine-based attacks.

And so one of the areas for intense research and development and one of the things we have to think about is how we are going to protect people in this environment where things move that quickly and things change so rapidly.

Chair WU. Thank you very much, Mr. Charney. Mr. Harper.

Mr. HARPER. Just briefly before I close, I thought I would come back to the question of liability, which Mr. Smith asked some of the other witnesses, and they made the case, a fair case, that software is very complex and so finding liability for negligent failure to secure a technology product would be hard to do. It also could frustrate innovation, and I think that is also true. Those things are true of regulation as well, and so maybe if there is consensus on the panel it might be that government contracting is the best way using well-developed NIST standards as the best way to advance the market for technology products, and then liability and regulation should be distant second and third places.

I think that the Federal Government has a role as a market actor in promoting standards, though it is not a given that government-created standards should be adopted in the private marketplace. Its best role, for the most part, is as an outside referee and policeman, rather than as a partner or participant in a public-private partnership. And for fun, I will note the fact that just before the hearing started, I tweeted the fact that I would be speaking in a hearing, and people could tune in and see this hearing. Hopefully they did. But one of the responses was a friend who pointed me to a web site where people's self-important tweets are collected. And so I think I will be ratcheting back on my use of twitter. Thanks for having us this afternoon.

Chair WU. Thank you all very much. There are many, many insights which were very interesting, sometimes surprising, and always very thoughtful. I think that is one of the benefits of being able to hear from people who are able to think deeply and consider topics. Thank you all very, very much for coming before the Committee this afternoon.

The record will remain open for two weeks for additional statements from the Members and for answers to any follow-up questions that the Committee may ask the witnesses. The witnesses are now excused, and the hearing is adjourned. Thank you very much.

[Whereupon, at 5:00 p.m., the Subcommittee was adjourned.]

○