ADDRESSING THE NATION'S CYBERSECURITY CHALLENGES: REDUCING VULNERABILITIES REQUIRES STRATEGIC INVESTMENT AND IMMEDIATE ACTION

HEARING

BEFORE THE

SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY AND SCIENCE AND TECHNOLOGY

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

APRIL 25, 2007

Serial No. 110–30

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html

U.S. GOVERNMENT PRINTING OFFICE
43–566 PDF 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 HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

LORETTA SANCHEZ, California,
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
JANE HARMAN, California
PETER A. DEFAZIO, Oregon
NITA M. LOWEY, New York
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
JAMES R. LANGEVIN, Rhode Island
HENRY CUELLAR, Texas
CHRISTOPHER P. CARNEY, Pennsylvania
YVETTE D. CLARKE, New York
AL GREEN, Texas
ED PERLMUTTER, Colorado
VACANCY

PETER T. KING, New York
LAMAR SMITH, Texas
CHRISTOPHER SHAYS, Connecticut
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
BOBBY JINDAL, Louisiana
DAVID G. REICHERT, Washington
MICHAEL T. MCCAUL, Texas
CHARLES W. DENT, Pennsylvania
GINNY BROWN-WAITE, Florida
MARSHA BLACKBURN, Tennessee
GUS M. BILIRAKIS, Florida
DAVID DAVIS, Tennessee

JESSICA HERRERA-FLANIGAN, *Staff Director & General Counsel*
ROSALINE COHEN, *Chief Counsel*
MICHAEL TWINCHEK, *Chief Clerk*
ROBERT O'CONNOR, *Minority Staff Director*

SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY, AND SCIENCE AND TECHNOLOGY

JAMES R. LANGEVIN, Rhode Island, *Chairman*

ZOE LOFGREN, California
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
AL GREEN, Texas
VACANCY
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

MICHAEL T. MCCAUL, Texas
DANIEL E. LUNGREN, California
GINNY BROWN-WAITE, Florida
MARSHA BLACKBURN, Tennessee
PETER T. KING, New York *(Ex Officio)*

JACOB OLCOTT, *Director & Counsel*
DR. CHRIS BECK, *Senior Advisor for Science & Technology*
CARLA ZAMUDIO-DOLAN, *Clerk*
DR. DIANE BERRY, *Minority Senior Professional Staff Member*

CONTENTS

ADDRESSING THE NATION'S CYBERSECURITY CHALLENGES: REDUCING VULNERABILITIES REQUIRES STRATEGIC INVESTMENT AND IMMEDIATE ACTION

Wednesday, April 25, 2007

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY,
AND SCIENCE AND TECHNOLOGY,
Washington, DC.

The subcommittee met, pursuant to call, at 1:11 p.m., in room 1539, Longworth House Office Building, Hon. James R. Langevin [chairman of the subcommittee], presiding.

Present: Representatives Langevin, Etheridge, Green and McCaul.

Mr. LANGEVIN. The subcommittee will come to order.

The subcommittee is meeting today to receive testimony on Addressing the Nation's Cybersecurity Challenges: Reducing Vulnerabilities Requires Strategic Investment and Immediate Action.

Good afternoon, and I want to welcome you to the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology hearing on a need to reduce vulnerabilities in our national critical infrastructure through investment and action. I would like to begin by thanking witnesses who appear before us today, and I appreciate your testimony.

I think that last week was certainly an eye-opening experience for many of us up here. We learned that our Federal systems, in particular, and privately owned critical infrastructure are all extremely vulnerable to hacking. These vulnerabilities have significant and dangerous consequences.

We learned that the Federal Government has little situational awareness of what is going on inside our systems. We cannot be sure how much information has been lost from our Federal systems, and we have no idea if hackers are still inside our systems, and we learned that our laws are powerless to stop intruders, even if compliance with FISMA does not make our systems more secure—I should say even if best compliance with FISMA doesn't make our systems more secure.

Now, this week, we are going to continue our conversation from last week to hear about some promising initiatives that are designed to reverse this trend of government failure.

I would like to take the opportunity to particularly thank Dr. Maughan for his service to our country in this field. Dr. Maughan is leading the cybersecurity research and development effort at the Department of Homeland Security Science and Technology Directorate. Under his leadership, DHS S&T has funded research that has resulted in almost one dozen open source and commercial products that provided capabilities such as secure thumb drives, root kit detection, worm and distributed denial of service detection, defenses against phishing, network vulnerability assessment, software analysis and security for process control systems.

His research and development funding is targeting the critical problems that threaten the integrity, availability and reliability of our networks. Clearly, he plays a vital role in securing our natural cyberspace.

But despite the criticality of this mission and the success of the program, I am troubled that this administration continues its effort to do what Chairman Thompson calls homeland security on the cheap.

In the last 7 years, more than 20 reports from such entities as InfoSec, Research Council, the National Science Foundation and the National Institute of Justice, the National Security Telecommunications Advisory Committee, the National Research Council and the President's Commission on Critical Infrastructure Protection have all urged the government to do more to drive, discover and deliver new solutions to address cyber vulnerabilities. But look at what this administration has done to cybersecurity and the research budget at the Department of Homeland Security.

Though this program was slated to receive $22.7 million in fiscal year 2007, the actual number I received from S&T showed we only funded this program at $13 million. For fiscal year 2008, the President slashed the budget again, requesting $14.8 million. This is an $8 million cut from the previous year.

Just listen to some of the important programs that are being cut or reduced in fiscal year 2007: The budget for the DNSSEC program, which adds security to the main system, was reduced $670,000. The budget for the secure protocols for routing infrastructure was zeroed out from its original amount of $2.4 million. The budget for the next generation cybersecurity technologies program, which addresses a variety of topic areas aimed at preventing, protecting against, detecting, responding to and recovering from large-scale high-impact cyber attacks, was reduced $1,625,000.

Now, I don't know who is responsible for these cuts, Under Secretary Cohen or Secretary Chertoff or the White House, but reducing this funding is a serious strategic error by this administration.

Just to understand how little we are spending, for the sake of comparison, the FBI estimated that, in 2004, that cyber crime cost companies worldwide around $400 billion. In 2005, the agency estimated that U.S. businesses lost $67 billion. Of course, neither of these figures can measure the loss of Federal information off our networks which one day may cost us our technological advantage over other nations. And those figures don't count the potential environmental losses if a successful attack on our control systems were to be carried out.

I am deeply troubled by the lack of foresight this administration has demonstrated. These efforts are simply too important to be cut.

The Homeland Security Committee is working to demonstrate the importance of R&D funding in this administration. In our recent authorization bill, we included a provision that would increase the funding level for the DHS cybersecurity R&D portfolio to $50 million. Democratic efforts over the last several years have been endorsed by many notable cyber experts, and I appreciate all of their input and their support.

The tools that will improve or revolutionize our security will not just appear overnight. Investment today plants seeds for the future. But it is incumbent upon the Federal Government to take the leadership role in this effort.

Again, I want to thank our witnesses for appearing before us today, and I look forward to hearing your testimony.

PREPARED OPENING STATEMENT OF THE HONORABLE JAMES R. LANGEVIN, CHAIRMAN SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY, AND SCIENCE AND TECHNOLOGY

- Ladies and gentlemen, welcome to the Subcommittee on Emerging Threats, Cybersecurity, Science and Technology hearing on the need to reduce vulnerabilities in our national critical infrastructure through investment and action.
- I'd like to begin by thanking the witnesses who appear before us today, and I appreciate your testimony.
- I think last week was an eye opening experience for many of us up here.
- We learned that our federal systems and privately owned critical infrastructure are all extremely vulnerable to hacking. These vulnerabilities have significant and dangerous consequences.
- We learned that the federal government has little situational awareness of what is going on inside our systems. We cannot be sure how much information has been lost from our federal systems, and we have no idea if hackers are still inside our systems.
- And we learned that our laws are powerless to stop intruders—even the best compliance with FISMA does not make our systems more secure.
- This week, we're going to continue our conversation from last week, and hear about some promising initiatives that are designed to reverse this trend of government failure.
- I'd like to take the opportunity to particularly thank Dr. Maughan ("MAWN") for his service to our country in this field.
- Dr. Maughan is leading the cybersecurity research and development effort at the Department of Homeland Security's Science and Technology Directorate.
- Under his leadership, DHS S&T has funded research has resulted in almost one dozen open-source and commercial products that provide capabilities such as:
  - secure thumb drives,
  - root kit detection,
  - worm and distributed denial of service detection,
  - defenses against phishing,
  - network vulnerability assessment,
  - software analysis, and
  - security for process control systems.
- His research and development funding is targeting the critical problems that threaten the integrity, availability, and reliability of our networks. Clearly, he plays a vital role in securing our national cyberspace.
- But despite the criticality of this mission and the success of the program, I am troubled that this Administration continues its effort to do what Chairman Thompson calls "Homeland Security on the Cheap."
- In the last seven years, more than 20 reports from such entities as the INFOSEC Research Council, the National Science Foundation, the National Institute of Justice, the National Security Telecommunications Advisory Committee, the National Research Council and the President's Commission on Critical Infrastructure Protection have all urged the government to do more to drive, discover and deliver new solutions to address cyber vulnerabilities.

• But look at what this Administration has done to cybersecurity and the research budget at the Department of Homeland Security.
• Though this program was slated to receive $22.7 million dollars in FY 2007, the actual numbers I've received from S&T show that we are only funding this program at *$13 million dollars.*
• For FY 2008, the President slashed the budget again, requesting $14.8 million dollars. This is an $8 million cut from the previous year.
• Just listen to some of the important programs that are being cut or reduced in FY 2007:
  • The budget for the DNSSEC program—which adds security to the Domain Name System—was reduced $670,000 dollars.
  • The budget for the Secure Protocols for the Routing Infrastructure was zeroed out from its original amount of $2.4 million dollars.
  • The budget for the Next Generation Cyber Security Technologies program, which addresses a variety of topic areas aimed at preventing, protecting against, detecting, responding to, and recovering from large-scale, high-impact cyber attacks was reduced $1.625 million dollars.
• Now I don't know who is responsible for these cuts—Under Secretary Cohen, or Secretary Chertoff, or the White House—but reducing this funding is a serious strategic error by this Administration.
• Just to understand how little we're spending for the sake of comparison, the FBI estimated in 2004 that *cybercrime* cost companies worldwide *around $400 billion dollars.* In 2005, the agency estimated that *U.S. businesses lost $67 billion dollars.*
• Of course, neither of these figures can measure the loss of federal information off of our networks, which may one day cost us our technological advantage over other nations.
• And those figures also don't count the potential environmental losses if a successful attack on our control systems is carried out.
• I am deeply troubled by the lack of foresight that this Administration has demonstrated. These efforts are simply too important to be cut.
• The Homeland Security Committee is working to demonstrate the importance of R&D funding to this Administration.
• In our recent authorization bill, we included a provision that would increase the funding level for the DHS cybersecurity R&D portfolio to $50 million dollars.
• Democratic efforts over the last several years have been endorsed by many notable cyber experts, and I appreciate all of this support.
• Ladies and gentlemen, the tools that will improve or revolutionize our security *will not just appear overnight.* Investment today plants seeds for the future, but it is incumbent upon the Federal government to take the leadership role in this effort.
• I thank the witnesses for appearing before us today and look forward to their testimony.

Mr. LANGEVIN. It is now my pleasure to recognize the ranking member, my partner in this effort in the subcommittee, the gentleman from Texas, Mr. McCaul, for purposes of an opening statement.

Mr. MCCAUL. Thank you, Mr. Chairman.

I want to commend you again for holding this set of hearings on cybersecurity, which is a very important issue that, in my view, has been overlooked to a large extent since September 11th. Last week, we heard from several government agencies about their experiences with hackers breaking into their networks. It is a serious problem, and it is happening more often than we realize. As I have said before, I believe a cyber attack could be at least if not more devastating to our country than a weapon of mass destruction.

Unfortunately, right now, we are not doing what we need to do to defend ourselves from this threat. Today, we focus on how we respond to these attacks and how we develop the tools and procedures to protect the information upon which our Nation depends. Securing our networks may not get as much attention as going to war, but it is just as important when we consider the aspect of cyber warfare and the lack of our preparedness.

VerDate Nov 24 2008 12:16 Jun 23, 2009 Jkt 000000 PO 00000 Frm 00008 Fmt 6633 Sfmt 6601 H:\DOCS\110-HRGS\110-30\43566.TXT HSEC PsN: DIANE

We have gathered some of the best minds here today in this country to discuss how we as a country should respond to this challenge of defending our information systems, and I look forward to their testimony.

After our hearing last week, I met with a number of CEOs of leading cybersecurity companies and heard their perspectives on this complex issue; and it is clear that we must marshal our resources and focus on this problem. We have not provided information security the attention it deserves; and with the help of experts such as those we have before us here today, I believe we can improve the situation and provide the sense of urgency to stimulate new progress in securing the Nation's information systems.

I thank the Chair, and I look forward to the testimony.

Mr. LANGEVIN. I thank the gentleman.

All the members as they arrive will be allowed to submit, according to the committee rules, opening statements for the record, and then we will begin to questions after the testimony.

Again, I would like to turn to our panel right now. I want to welcome our first panel of witnesses.

Our first witness, James Lewis, directs CSIS Technology and Public Policy Program. He is a senior fellow. Before joining CSIS, he was a career diplomat who worked on a range of national security issues during his Federal service.

Our second witness, Dr. Daniel Geer, spent 10 years in clinical and research medical computing, followed by 5 years running MIT's Project Athena. Afterwards, he worked in the research division of the then Digital Equipment Corporation and then a series of entrepreneurial endeavors.

Our third witness is Mr. Sami Saydjari, who is the founder and chief executive officer of Cyber Defense Agency, creators of systematic defenses for high-value systems against aggressive cyber attack. Before founding this cyber defense agency, Mr. Saydjari was a senior staff scientist in SRI International's Computer Science Laboratory.

Our fourth witness, Dr. Douglas Maughan, is the Cyber Security Program Manager at the Department of Homeland Security Science and Technology Directorate. Prior to his appointment at DHS, Dr. Maughan was a program manager in the Advanced Technology Office of the Defense Advanced Research Projects Agency, or DARPA.

Without objection, the witness's full statements will be inserted into the record; and I will now ask each witness to summarize the testimony for 5µminutes, beginning with Dr. Lewis.

Before we do that, though, I just wanted to remind everyone of the committee rules that testimony is supposed to be submitted 48µhours in advance. DHS didn't get their testimony in to us until about 7:30 this morning. And I have said before I understand DHS and other government departments need to get—it is not solely on the witness's shoulders to get it in. I know OMB has to clear the testimony. But this is happening regularly from DHS. And I know Chairman Thompson is doing an internal investigation right now to find out what the problem is. We just can't do business like this if we don't have testimony in a timely fashion.

VerDate Nov 24 2008 12:16 Jun 23, 2009 Jkt 000000 PO 00000 Frm 00009 Fmt 6633 Sfmt 6601 H:\DOCS\110-HRGS\110-30\43566.TXT HSEC PsN: DIANE

Mr. LANGEVIN. With that, I will turn it over to Dr. Lewis for your opening statement. Thank you.

STATEMENT OF JAMES ANDREW LEWIS, DIRECTOR AND SENIOR FELLOW, TECHNOLOGY AND PUBLIC POLICY PROGRAM, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES

Mr. LEWIS. Thank you, Mr. Chairman. I would like to thank the committee for this opportunity to testify.

You heard last week about the problems at various agencies, and I think that testimony highlighted that securing networks in the United States for cyber attack is one of the greatest challenges we face.

Cyber security can seem intractable. It is a problem that in the past attracted exaggeration, and this combination of intractable and exaggeration can sometimes create indifference. One way to overcome this indifference is to put cybersecurity in the right context.

Our networks face two sets of risks. The first involves espionage. The second involves the potential interruption of services, particularly Federal services.

The most important for me is espionage cybersecurity, is primarily a spy story. Cyber espionage poses the greatest threat to the U.S. Hacking into computer networks, which are vulnerable and likely to remain so for years, provides new low-cost and low-risk opportunities for foreign intelligence agencies. U.S. networks are very vulnerable. Several nations have exploited these vulnerabilities to gain valuable information. These efforts and our inadequate response have damaged national security.

Unlike cyber espionage, the threat of disruption of services remains hypothetical. I would not take too much comfort from this, Mr. Chairman. Because if an opponent can hack into a network to steal information, they can hack into and plant malicious software that could be triggered during a crisis. We should assume in the event of a conflict our opponents will seek to disrupt our networks and data.

I would like to point out that, although we have a long litany of threats, the question as to whether the U.S. was better off before it depended so heavily on computer networks can be answered in the negative. The benefits from the greater use of networks and computers outweigh the damage from poor cyber security. However the porousness of our Federal networks reduces those benefits, and greater attention cybersecurity would improve both national security and economic performance and close off an avenue of asymmetric opportunity for our opponents.

While the U.S. is better off than it was 10 years ago, the improvement has been unequally distributed among agencies and companies. Some are secure; some are not. There have been serious efforts in the national security community to make networks more secure, and our most sensitive military and intelligence functions are probably secure. Some crucial civil networks are also more secure than they were.

Some efforts to improve cybersecurity have not had the benefits we expected. It is possible to hack into a computer running software that has met the common criteria, that has the common cri-

teria certification, on a network that has met the requirements of ISO 19779, the standard for cybersecurity, and at an agency that has gotten good marks on FISMA. In other words, you can meet all the formal requirements and still be vulnerable.

How do we change this? There is no silver bullet. There is no single program that will improve security. The Federal Government, for example, is a complex enterprise, with thousands of networks and hundreds of thousands of computers. No single agency controls this network; and while some Federal networks are among the most secure in the world, others are routinely penetrated. Some use advanced technologies, others are legacy systems dating back years and which, for all practical purposes, cannot be secured.

The core of the problem is organizational. The Department of Homeland Security, the Federal CIO Council, and the Office of Management and Budget all play a role in securing Federal networks. But cybersecurity remains a low priority at many agencies.

Along with a better organization for cybersecurity, the U.S. needs a better strategy. We did have a national cybersecurity strategy in 2003, but it is outdated. A new strategy would have to be more comprehensive, and I would like to detail some of the things I think that strategy should include.

First, we would benefit from streamlining government processes. There are too many groups and committees, and too few of them have any real authority.

Second, the U.S. can do more to improve agency practices for network security. Cybersecurity is still a third-tier priority at many agencies. If gangs of foreigners broke into the State or Commerce Departments and carried off dozens of file cabinets, there would be a huge outcry. When the same thing happens in cyberspace, we shrug it off. Agencies need to be held accountable for following best practices in network security.

Third, better identity management would improve cybersecurity security. As long as it is easy to impersonate someone on the Internet, networks will never be secure. HSBD 12 and Real ID can offer some benefits.

Fourth, the government should address software assurance. We recently did a study at CSIS that looked at how companies write software. While most of them do a pretty good job and all of them have some very useful practices, the practices aren't evenly applied; and if the government could find a way to spread these best practices to make software more secure, it would have a real benefit.

Finally, the U.S. can take steps to keep itself at the forefront of technology. This goes beyond funding cybersecurity research. While we spend more on R&D than other countries, it may not be enough to maintain our lead. These steps—better organization, better practices for coding, better identity management, attention to continuity of government and renewed support for technological leadership—can make networks more secure.

Congressional oversight is critical with this. Without Congress to press senior leadership at Federal agencies, we will wait much longer for progress than would otherwise be the case.

It has been 12 years since the U.S. became concerned with vulnerabilities in computer networks. There has been some im-

provement, but not enough. We have an opportunity to change this in the next few years.

I thank the committee for the opportunity to testify. Thank you for entering my comments into the record, and I will be happy to take your questions.

Mr. LANGEVIN. Thank you, Dr. Lewis.

[The statement of Mr. Lewis follows:]

PREPARED STATEMENT OF DR. JAMES A. LEWIS

I would like to thank the Committee for the opportunity to testify on the cybersecurity challenge the United faces. Cybersecurity is one of those problems that seem to be intractable. It is also a problem that, in the past, seemed to attract exaggeration and hyperbole. The combination is not ideal for creating effective policies, in part because the blend of intractability and exaggeration can create indifference.

One way to overcome this indifference is to put cyber security in the right context. The context is not an 'electronic Pearl Harbor' but the risk of loss of valuable information and the disruption of data and services. For Federal networks, the context for cybersecurity involves espionage and potential interruptions in the delivery of Federal services.

The security of Federal networks has serious implications for homeland security as Federal network security affects both continuity of government and the operations of critical infrastructure. This alone justifies extra attention to government networks. In addition, measures that improve the security of Federal networks will also benefit private sector networks. My own view is that the security of Federal networks is the most serious cybersecurity challenge we face, more serious than the risks to critical infrastructure or from cybercrime.

The most important of these challenges come from espionage. Cybersecurity is primarily a spy story. Cyber-espionage poses the greatest current threat to the United States. Hacking is the extension of signals intelligence into new and untrammeled areas. Foreign intelligence agencies must weep with joy when they contemplate U.S. government networks. We have thoughtfully placed sensitive information on these networks and then failed to secure them adequately. This is not a hypothetical problem. The last twenty years have seen an unparalleled looting of U.S. government's databases.

The reliance upon information technology has changed the nature of espionage. Information is more valuable. Nations will use the traditional means of espionage (infiltration and recruitment) to obtain access to information, but information technologies have created a gigantic new opportunity. Hacking into computer networks (which are vulnerable and likely to remain so for years) provides new, low cost and low risk opportunities for espionage. Eight or nine countries have the advanced technical skills needed for these operations and smaller countries could hire hackers from the criminal world—we know of at least one instance where this has occurred.

Conflict in cyberspace is clandestine, so it can be difficult to assess our opponents' intentions and capabilities. It is easier to assess the vulnerability of U.S. systems and the consequences of an information attack. U.S. networks are very vulnerable. Even highly sensitive networks used for command and control or intelligence are not invulnerable. From an intelligence perspective, several nations, have exploited the vulnerabilities of U.S. government networks to gain valuable information. These foreign intelligence efforts and the inadequate U.S. response have damaged national security.

You heard last week about some of the problems that some agencies face. Their testimony highlights that securing Federal networks from cyber attack is one of the greatest challenges facing the United States, and that the scope of the challenge and the threat to national security are difficult to appreciate fully. Several incidents that occurred in the past few months help to illustrate the scale of the problem. In December and January 2006, for example, the Naval War College, the National Defense University, and other DOD facilities had to take computer networks offline after a foreign entity infected them with spyware. Before the last shuttle launch, NASA had to block e-mail attachments to avoid outsider attempts to gain access before a Shuttle launch. And as you heard last week, the Department of Commerce had to all of the computers at the Bureau of Industry and Security offline after they were hacked and infected with spyware.

In contrast to espionage, the threat of the disruption of services remains hypothetical. Cyber-espionage is a routine occurrence, but there have been no disruption of services. We should not take much comfort from this, however. If an opponent

can hack in to Federal networks to steal information, they are likely to also be able to hack in to implant malicious software that could be triggered in a crisis to disrupt services or to scramble data. It is safe to assume that many of our potential opponents are planning informational attacks to disrupt U.S. government services and databases.

It is easy to overstate the effect of this disruption, but a cyberattack that increases uncertainty in the mind of an opponent degrades that opponent's effectiveness. This is a classic intelligence strategy, and cyber attacks on information systems provide new and expanded means to execute it. Denial and deception can make opponents certain that they know what is happening when, in fact, what they believe is wrong, or it can make them unsure that they know what is happening. Finding ways to inject false information into the planning and decision processes of an opponent, or manipulating information that is already in that system to make it untrustworthy, can provide military advantage. In the event of a conflict, our opponents will pursue an informational strategy that seeks to expand uncertainty and confusion and this will likely involve efforts to disrupt Federal networks.

This litany of threats and risks might lead some to ask if the U.S. was better off before it depended so heavily on computer networks. The answer to that question is no. The benefits to the U.S. that come from the greater use of networks and computers outweigh the damage from poor cybersecurity. It is better to have networks than to be without them, and the use of computer networks provides the U.S an advantage in its economy and its military operations. However, the porousness of our Federal networks erodes those benefits. Greater attention to cybersecurity would increase the benefits our nation gains from networks and close off an avenue of asymmetric advantage to our opponents.

There have been serious efforts in the national security community to make their networks more secure. Our most sensitive military and intelligence functions are probably secure. Some civil crucial networks are more secure—much attention has been paid to Fedwire, the Federal Reserves electronic funds transfer system, for example. But, as you heard last week, many agency networks remain poorly secured, and it is safe to say that reams of diplomatic, scientific, administrative and defense industrial information at the various agencies have not been adequately secured. In looking at the security of Federal networks, it is fair to say that while the U.S. is better off than it was five years ago or ten years ago, the improvement has been unevenly distributed among agencies. Some are secure, most are not.

Additionally, some efforts to improve cybersecurity have not had the benefits we expected. It is quite possible for our opponents to hack a computer running software that has Common Criteria certification, on a network that has met the requirements of ISO 19779, at an agency that has gotten good marks on FISMA. In other words, you can meet all the formal requirements and still be vulnerable.

Network security is also a dynamic situation, dynamic in the sense that attacks are continuous and continuously changing. We should applaud those agencies that have, after some months, discovered their networks have been hacked and have taken steps to undo that hack, but our next question should be, "and now what are you doing." Attacks on Federal networks are continuous, and fixing one problem does not mean that we have checked the box and can turn our attention elsewhere.

How doe we change this situation? There is no silver bullet, no single program or effort that will remedy this problem. Increased funding will not improve security. The Federal Government is a complex enterprise, with thousands of networks and hundreds of thousands of computers. No single agency has control of this collection of networks. Some Federal networks are among the most secure in the world, although even these are not immune from attack. Others are routinely penetrated. Some systems use the most advanced technologies. Others are legacy systems, running programs that may date back many years and which, for all practical purposes, cannot be secured.

Making networks more secure is a large and complex problem. The core of the problem is organizational. Although it has been more than a decade since the Marsh report on the risks posed by cyber attack to critical infrastructure, and although there has been progress, the Federal Government is still disorganized when it comes to cyber security. The Department of Homeland Security, the Federal CIO Council, and the Office of Management and Budget all play a role in securing Federal networks. But cybersecurity remains a low priority and an afterthought for many agencies, and the Federal response to cybersecurity remains largely ad hoc and dispersed.

Along with better organization, the U.S. also needs a better strategy. There is, of course, a National Cyber Strategy from 2003, but that strategy is now outdated. It shifted too much of the burden for security to the private sector and did not resolve key issues regarding responsibility within the government. A new, comprehen-

sive cyber security strategy for the Federal Government would need to include a number of complementary measures to reduce vulnerabilities. The following paragraphs provide a brief outline of some of the major elements of this approach.

Rationalizing and streamlining governmental processes for improving cybersecurity is essential. There are too many interagency groups and committees working on the same problem, often with the same people, and few of them have the authority to make any real progress. The U.S. does not need a new White House cyber czar, but it does need to do more to direct and coordinate efforts by the various agencies. The recent creation of a cybersecurity Policy Coordinating Committee at the National Security Council is an important first step.

Second, the U.S. can do more in the area of improving agency practices when it comes to networks security. Cybersecurity is still a third tier priority at many agencies. If gangs of foreigners broke into the State or Commerce Departments and carried off dozens of file cabinets, there would be a crisis. When the same thing happens in cyberspace, we shrug it off as another of those annoying computer glitches we must live with. Agencies need to be held accountable for breaches. Our current approach is to treat losses of information through inadequate security as something that is separate from the performance of senior officials.

The separation between the national security agencies and civilian agencies needs to be reduced. The national security agencies do better at security, but there is no good mechanism for sharing their expertise and experience with the civilian agencies. Developing better ways to coordinate network security efforts between agencies and to identify, share and enforce best practices for Federal network security across agencies would reduce risk and damage.

Better identity management would also help improve cybersecurity. As long as it is easy to impersonate someone else on the internet, networks will never be secure. In this, initiatives like HSPD 12 and the Real ID Act offer the possibility to reduce risk. HSPD–12 mandated strong identity procedures and credential for the Federal Government and its contractors HSPD–12, along with Real ID, lay the foundation for robust authentication of identity. Much remains to be done, but the U.S. has begun to adjust how it manages identities to fit digital technologies and this will improve security.

Continued attention to continuity of operations and continuity of government can mitigate the risk of disruption of Federal services. As part of a Federal cybersecurity strategy, this would entail measures to keep networks operating at some minimal level and to provide continued access to data. This is an area where there has also been some progress.

One new area the government can begin to address is how to improve software assurance. This means creating processes for transparency, evaluation and coordination in the production of more secure software for government use. In considering this, let me refer to an episode from American history, when the U.S. faced a similar problem and what it did about it. This story has an unlikely hero—Herbert Hoover. Hoover may have been a terrible or unlucky President, but he was a great Secretary of Commerce. One of the things he did in the 1920's as Secretary of Commerce was call a number of leading companies from different sectors - automobiles, electrical equipment and so on, to the Commerce Department and say that they had to come up with a means to improve quality and interoperability in their products. This was the start of the industry-led standards process.

We need something similar to happen for security and software production. There are existing standards bodies for software. These standards are aimed at products—how they perform and how they interoperate. The U.S. does not need to duplicate them. What we need is a new means for understanding how to produce software in ways that can assure security.

CSIS recently did a study that looked at how some of the larger IT companies write software. We found considerable attention to security among the companies, and that each company had a set of 'best practices' for software assurance that make their products more secure. We also found that each company's best practices were somewhat different, and that these practices were sometimes unevenly applied.

Finding a way to extend commercial best practices for assurance would benefit both Federal networks and the private sector. The procedures companies use as part of their software production process internal reviews and testing for performance and security, external testing and red-teaming, and the use of software review tools (some commercial, some proprietary and developed by the software company itself) to find vulnerabilities or errors. These practices offer the building blocks for an approach that could reduce vulnerabilities.

The key to these new processes should be to build upon what is already done within the private sector when it comes to software. Software producers realize the

importance their customers place on assurance and security and have adjusted their internal procedures to meet this market demand. While there is much commonality and overlap in what companies do, each company approaches the issues of assurance and security somewhat differently. From these differences, we can extract best practices and requirements that will address, as part of a larger solution set, the risks posed by foreign involvement in software production.

Please note that I am saying best practices, not standards. An attempt to have the government mandate standards for software production and then enforce them would damage the American economy without producing any benefit for security. So new regulations, new government standards are not the solution. However, the government could encourage industry to use best practices for making secure software by linking practices to its acquisitions policies. If the Federal Government gave preference in its acquisitions to software that was developed with trustworthy processes, it would provide an incentive that would benefit both the Federal and the commercial markets.

Companies are making serious efforts to improve software assurance, but the government needs to be able to understand and guide those efforts. Traditional approaches to governance—command and control or heavy regulation—would increase assurance at an unacceptable cost. Software assurance may be the effort that promises the greatest returns to cybersecurity. The U.S. needs news ways to let the government and the private sector work together to develop some generalized set of best practices for software production, and the Departments of Defense and Homeland Security are involved in some interesting work in this area.

Finally, the U.S. can take steps to keep itself at the forefront of technology. This goes beyond simply funding more cyber-security research. Overall, the U.S. invests more than other nations in research, but this investment may not be enough, in an era of increased international competition, to preserve leadership. Federal investment in the research that undergirds technological innovation offers tremendous returns for both the economy and for security. Innovation makes life more difficult for opponents. Measures that improve the climate for innovation in the U.S. also help build a skilled domestic workforce.

These steps—better Federal organization, best practices for coding combined with acquisitions, better identity management, attention to continuity of government and renewed support for technological leadership—can form a coherent strategy for improving the security of Federal networks and cybersecurity in general. Being able to articulate a strategy is important, but implementation will always be a challenge. In this, Congressional oversight is critical to this. Without Congress to press senior leadership at Federal agencies to do better, progress will take much longer than would otherwise be the case.

It has been more than twelve years since the U.S. became concerned with the vulnerabilities created by its use of computer networks. There has been some improvement in that time, but not enough. We have an opportunity in the next few years to change this with improved Federal organization and better strategies. Our goal should not be perfect security, but to gain more advantage than our opponents from the use of information technology.

I thank the committee again for the opportunity to testify. I ask that my entire statement be entered into the record, and I will be happy to take your questions.

Mr. LANGEVIN. Dr. Geer.

STATEMENT OF DANIEL E. GEER, JR., PRINCIPAL, GEER RISK SERVICES, LLC

Mr. GEER. Thank you.

I don't do this every day, so I am just going to start with what I know of as the four verities of government, which is most exciting ideas are not important, most important ideas are not exciting, not every problem has a good solution, and every solution has a side effect. And that is amazingly true in the field that I work in, cybersecurity. Every bit of that is true.

I am going to try to give you five priorities from my point of view.

The first is, we need a system of security metrics, metrics that actually work. One of the great scientists of all time, Lord Calvin, said, and I have to read this:

When you can measure what you are talking about, and express it in numbers, you know something about it; but when you cannot measure it, when you cannot express it in numbers, your knowledge is a meager and unsatisfactory sort; it may be the beginning of knowledge, but you have scarcely, in your thoughts, advanced to the stage of science.

As we stand here today, we do have some metrics. Most of them are imperfect—all of them are imperfect. A few are good enough for decision making.

In late 2003, the NSF held a sequestered invitation-only workshop to determine the 10-year "grand challenges" in cybersecurity. One of those four grand challenges that we came up with one speaks directly to this: Within a decade, we must have a body of quantitative information risk management as sophisticated as quantitative financial risk management. That item actually was mine, and it was my pleasure to present it to House Science.

Good metrics aren't cooked in the kitchen. They don't appear on demand. Like statistics, they can mislead. The purpose of risk management is to improve the future, not to explain the past. Security metrics are the servants of risk management, and risk management is about making decisions under uncertainty. Therefore, the metrics I am talking about, the only ones we are interested in, are those that support decision making about risk for the purpose of managing that risk.

I would recommend that some sort of clearinghouse review of what we know how to measure and in particular how good what we know how to measure is at predicting the future would be a good thing to do right away.

Second priority. The demand for security expertise outstrips the supply.

Information security is, in my view, the hardest technical field on the planet. Nothing is stable, surprise is constant, and defenders are at a permanent structural disadvantage compared to the attack side. There is no fixing that.

But because the demand for expertise so outstrips the supply, the fraction of practitioners who are charlatans is rising. Because the demands of expertise are so difficult, the training deficit is critical. We don't have the time to create all the skills that are required. We have to steal them from other fields.

The reason cybersecurity is not worse than it might otherwise be is because a substantial majority of those who are currently practicing were trained in other fields and, therefore, they bring the expertise of those other fields to this one. We are lucky that that is true. Civil engineers, public health people, actuaries, aircraft designers, lawyers, you name it, all of them can contribute something.

We do not have the facility to train people from scratch at the rate at which we need it; and so anything you can do to encourage people to come into this field who are themselves smart, analytic, willing to operate under a high degree of uncertainty and convinced that this is worth doing, anything you can help with that, please do.

Third priority. What you can't see is more important than what you can.

Perhaps you got a taste of it last week. I was not aware of that hearing. I don't follow this kind of thing. Let me be clear, the opposition is professional. It is not joyriders. It is not braggarts. It used to be, but it isn't now. Because of the sheer complexity of modern networks, there is any number of places for people of ill-will or for computer software of ill-will to hide. And that is not getting better, and it won't get better.

The complexity for the most part is because product manufacturers are under competitive pressure to keep inserting new features into their products. This is not going to go away, and it is not something I would suggest that you attack. Were there no attackers, the way in which software is built would be a miracle of efficiency. The fact that there are attackers, the fact there are sentient opponents, the fact that this is not evolution but intelligent design of a nasty sort, that is what we have to work on.

Complex systems tend to fail in complex manners. It is very hard to figure that out in advance. It is exceptionally hard. That is why I say it is probably the hardest field there is.

In particular, I think what you need to do is to do something that I don't like the sound of but I will say. Ignorance of the law is no defense on my part. My swimming pool is an attractive nuisance, whether I like it or not. I don't think we can go much farther and say that I didn't know it had a flaw is any kind of defense. And software licenses, to the last one of them, have that built into them, and it has to be addressed.

The fourth one is we have to have some sort of information sharing. You all know about all of this. I am not going to belabor it. The model I would recommend to you is the Centers for Disease Control. They only have three things that matter: the mandatory reporting of communicable disease, the skill to separate statistical anomalies from true hot spots, and an away team to handle things like an outbreak of ebola. Beyond that, nothing matters.

I would suggest that something like that needs to be done here. No general counsel acting rationally will ever share attack data. There is nothing but downside risk from where they are.

So if I can give you a research grade problem to work on, the research grade problem is this: Find some way to do technical deidentification of attack data so that general counsel's rational fear of sharing that data can be put aside under a technical guarantee. They do not and they will not believe your procedural guarantees. We have got to have a technical guarantee. This is a research grade problem that needs to be done.

The fifth one and last one is perhaps the hardest of all, and that is accountability rather than access control. Access control is who you are, authentication, what you are allowed to do given who you are, authorization. It doesn't scale. And if we try to make it scale—that is not to say everybody does it well as it is, but if we try to make that scale, the rate at which data and facilities and knobs to adjust are increasing is out of our ability to add to that full-blown access control going forward.

We have to do something else. This is a free country. I didn't have to ask anyone's permission to be here, to get on the bus or what have you. But if I sufficiently badly screw up, then I will have to pay for it. We are in the physical world committed now to sur-

veillance, whether we like it or not. You can't live your life without metal detectors and cameras. We are going have to do that in this world.

And if I may say so, please make sure that the surveillance we have to do is directed at data and computers and not at people. It is a choice we have to make, and it is an ugly choice.

I will just say the five things again and be quiet.

We need a system of security metrics, and it is a research grade problem.

The demand for security expertise outstrips the supply, and it is both a training and a recruitment problem.

What you can't see is more important than what you can, and you can never mistake the absence of evidence for the evidence of absence.

Information sharing that matters does not happen and cannot happen until we have technical guarantees, rather than procedural ones.

And accountability is an idea whose time come, but—to steal Leon Uris' phrase—it has a terrible beauty.

Thank you.

Mr. LANGEVIN. Thank you, Dr. Geer.

[The statement of Mr. Geer follows:]

PREPARED STATEMENT OF DANIEL E. GEER

Introduction

The Nation's cybersecurity challenges are profound and not easily addressed. Perfection is not possible; rather this is entirely a matter of risk management, not risk avoidance. Easy to say.Hard, though not impossible, to do. Starting yesterday would be good. Money alone will not solve anything. Policy alone will not solve anything. Fixing what isn't broken will waste money capital and policy capital; fixing what is broken will require both. Wishful thinking, whether explicit or implicit, intentional or delusional, will allow the problem to get bigger.

In the testimony which follows, I make no attempt to argue from first principles or to provide every supporting footnote that would be required to prove the assertions made; I don't think you want it and the page limit prevents it. I do, however, have all the proof that can be had, and stake my professional reputation on what is said here. I trust that you have invited me because you are aware of that reputation and my bona fides in these matters. The material is brief in the hope that brevity increases the likelihood it will be read. This is not your last chance to get my attention; I hope it is not my last chance to get yours.

Priority number one: A system of security metrics.

"You cannot manage what you cannot measure" is a cliché, but, happily,one of the great scientists of all time, William Thompson, Lord Kelvin, put it as well as it can be put:

> When you can measure what you are speaking about, and express it in numbers, you know something about it; but when you cannot measure it, when you cannot express it in numbers, your knowledge is a meagre and unsatisfactory kind; it may be the beginning of knowledge, but you have scarcely,in your thoughts, advanced to the stage of science.

As we stand here today,we have some security metrics. None of them are perfected though many are good enough for decision making if, and only if, they are collected by persons whose aim is truth rather than positioning. In late 2003, the Computing Research Association and the National Science Foundation held an invitation-only workshop to determine the ten-year "grand challenges" for NSF investment in cybersecurity. Of the four grand challenges settled upon, one speaks directly to this: Within a decade, we must have a body of quantitative information risk management as sophisticated as the then existing body of financial risk management. That item was mine, and I had the honor of presenting it to this body immediately after the conclusion of the workshop.

Good metrics are not cooked in the kitchen. They are not created simply because the Congress demands them. Like statistics, they can mislead. In your line of work,

you doubtless know this better than I and I know it well. The purpose of risk management is to improve the future, not to explain the past. Security metrics are the servants of risk management, and risk management is about making decisions under uncertainty.Therefore, the only security metrics we are interested in are those that support decision making about risk for the purpose of managing that risk. I urge the Congress to put explaining the past, particularly for the purpose of assigning blame, behind itself. Demanding report cards, legislating under the influence of adrenaline, imagining that cybersecurity is an end rather than merely a means—all these and more inevitably prolong a world in which we are procedurally correct but factually stupid. A clearinghouse review of what we know how to measure and how good what we know is at predicting the future would be a good start as we do not even know what it is that we do not know.

Priority number two: The demand for security expertise outstrips the supply.

Information security is perhaps the hardest technical field on the planet. Nothing is stable, surprise is constant, and all defenders work at a permanent, structural disadvantage compared to the attackers. Because the demands *for* expertise so outstrip the supply,the fraction of all practitioners who are charlatans is rising. Because the demands *of* expertise are so difficult, the training deficit is critical. We do not have the time to create, as if from scratch, all the skills required. We must steal them from other fields where parallel challenges exist. The reason cybersecurity is not worse is that a substantial majority of top security practitioners bring other skills into the field; in my own case, I am a biostatistician by training. Civil engineers, public health practitioners, actuaries, aircraft designers, lawyers, and on and on—they all have expertise we can use, and until we have a training regime sufficient to supply the unmet demand for security expertise we should be both grateful for the renaissance quality of the information security field and we should mine those other disciplines for everything we can steal. If you can help bring people into the field, especially from conversion, then please do so. In the meantime, do not believe all that you hear from so-called experts. Santayana had it right when he said that "Scepticism is the chastity of the intellect; it is shameful to give it up too soon, or to the first comer."

Priority number three: What you cannot see is more important than what you can.

The opposition is professional. It is no longer joyriders or braggarts. Because of the sheer complexity of modern, distributed, interdigitated, networked computer systems, the number of hiding places for unwanted software and unwanted visitors is very large. The complexity,for the most part, comes from competitive pressure to add feature-richness to products; there is no market-leading product where one or a small group of people knows it in its entirety,and components from any pervasive system tend to be used and re-used in ways that even their designers did not anticipate. Were there no attackers, this would be a miracle of efficiency and goodness. But unlike any other industrial product, information systems are at risk not from accident, not from cosmic radiation, and not from clumsy operation but from sentient opponents. The risk is not, as some would blithely say, "evolving" if by evolving the speaker means to invoke the course of Nature. The risk is due to intelligent design, and there is nothing random about it.

Because complex systems fail complexly, it is not possible to anticipate all the failure modes of large and therefore complex information systems. This complexity provides both opportunity and hiding places for attackers. Damping out complexity is not something that even the Congress can take on, but security failures come from it as surely as dawn comes from the east. Given that most software license agreements are an outrage, it is high time that security failures in software systems be deemed *per se* offenses. Just as my ignorance of the law is no defense and my swimming pool is an attractive nuisance whether I like it or not, ignorance of installed vulnerabilities can no longer be a defense for any party.

Priority number four: Information sharing that matters.

On the Internet every sociopath is your next door neighbor; you can never retreat to a safe neighborhood. Your ability to defend depends on your ability to know what the current threat profile is, both generally to all and specifically to yourself. For any given attack, you have zero ability to know whether you are a target of choice or a target of opportunity unless you share attack data with others.

Our Centers for Disease Control lead the world, full stop. There are only three things that make this so: (1) Mandatory reporting of communicable disease, (2) Longitudinal analysis and the skill to separate statistical anomalies from genuine harbingers of important change, and (3) Away teams to handle outbreaks of, say, Ebola.

All the rest is details. Of the three, the one that matters most is the mandatory reporting of communicable disease, and explicitly on the grounds that individual medical privacy must yield when the public risk is above threshold.

No General Counsel will share information risk data willingly, and no Chief Information Security Officer outranks his/her GC. Shared information does always carry some acute chance that it contains a previously unknown embarrassment, while any benefit from sharing is diffuse and delayed. Any person is risk averse when they don't know what risk they are taking and more so when the risk is involuntary; the GC is rational to not share data, in other words. The Congress should be wary of legislating irrationality, as always.

To get information shared the need is for a technical guarantee of harmlessness rather than a procedural guarantee. This is, in other words, a straight-up research question: How to provide technical de-identification of useful cybersecurity data so that that data can be shared with low or no risk to its source. Such technical protection should be open-sourced so that its strength can be independently evaluated *á priori* rather than the "trust us" nature of a procedural guarantee. Fund this research.

Priority number five: Accountability,not access control.

Information is the coin of the economic realm, and information that is used is information that moves about. Winners have the most information in play; losers have too much. Security technology is the fine line between the most information in play and too much information in play. The conventional answer to protecting information is to in some way limit who can do what and to which. Authentication (who you are) and Authorization (what you can do, given who you are) represent the conventional approach, sometimes jointly called Access Control. The problem is, these technologies do not scale and if you try to have ever finer control over the avalanche of new data items appearing by the second, you will be contributing to the complexity that is the bane of security.

What does scale is Accountability. In a free country,you don't have to ask permission for much of anything, but that freedom is buttressed by the certain knowledge that if you sufficiently screw things then up you will have to pay. The economics of the access-control model of information security do not scale; rather economics favor an accountability model focused on the monitoring of information use rather than the gatekeeping of information access. This means surveillance of data use in the sense of being able to reconstruct how information is used when it is used badly. This does not mean to throw away our existing investment in access control, but further investment in that will only produce inefficiency and a false sense of security.

We are, sadly if necessarily, making surveillance a commonplace of physical security; it is no longer possible to live in a world without cameras. We will have to, sadly if necessarily, make surveillance a commonplace of cybersecurity. As you consider how to make these dreadful choices, I suggest that the unit of observation be a datum, not a person, that if a surveillance system has to protect the digital world, that that surveillance be directed at data, not persons. If anything, this is risk management applied to risk management.

Summary

- We need a system of security metrics, and it is a research grade problem.
- The demand for security expertise outstrips the supply,and it is a training problem and a recruitment problem.
- What you cannot see is more important than what you can, and so the Congress must never mistake the absence of evidence for the evidence of absence, especially when it comes to information security.
- Information sharing that matters does not and will not happen without research into technical guarantees of non-traceability.
- Accountability is the idea whose time has come, but it has a terrible beauty.

Mr. LANGEVIN. Mr. Saydjari.

STATEMENT OF O. SAMI SAYDJARI, PRESIDENT, PROFESSIONALS FOR CYBER DEFENSE CHIEF EXECUTIVE OFFICER, CYBER DEFENSE AGENCY, LLC

Mr. SAYDJARI. Chairman Langevin, Ranking Member McCaul, members of the subcommittee, it is a pleasure to have this opportunity to testify today on this matter of utmost national importance.

I come to you as the leader of the Professionals For Cyber Defense, a nonprofit group of recognized national cybersecurity leaders advocating for sound U.S. cyber defense policy.

I have a written statement which, with your permission, I would like to enter into the record. I will briefly summarize it and look forward to responding to the committee's questions.

In 2002, more than 50 leading cyber defense experts signed a letter, feeling compelled to warn President Bush of strategic threat to our Nation from attacks to our information infrastructure. Our message was simple. I am going to repeat that message to you today. The U.S. faces a national strategic threat requiring a national strategic response, and you can help today.

First, to a strategic threat. The lack of a strategic response must come, in our opinion, from a lack of belief in an established strategic threat. Even an uncertainty and a possibility of the strategic threat that we see demands immediate action to resolve that uncertainty to move forward on sound policy. Because of this, the Professionals for Cyber Defense developed and vetted a simulated strategic attack campaign against the United States to help establish the nature and effect of such an attack.

Our findings are sobering. The U.S. is vulnerable to strategically crippling cyber attacks from nation-state adversaries. The level of devastation to our economy and to our way of life is potentially disastrous. The ripping of our social fabric will be on an order that we only glimpsed in the aftermath of Hurricane Katrina. We will move from being a superpower to a third world country practically overnight. We are a Nation unprepared to defend ourselves against this strategic threat and recover from it when it happens.

Therefore, the PCD recommends that the United States engage in a national threat assessment immediately to verify our findings and move forward. The critical IT infrastructure is as legitimate a part of our territory as physical land. We depend upon it now for our survival, just like land in the industrial and agrarian ages. Cyberspace controls real-world critical assets like power generators, power distribution, oil and gas pipelines. The information age requires us to defend this digital territory. Therefore, the government must provide for the common defense of this new territory.

This is not a matter of big government versus small government. It is not a matter of interfering or controlling the private sector. The private sector openly has declared that they desperately need the government's help against defending against nation-state adversaries. There are a lack of incentives for the private sector to solve this problem on their own, just as there is a lack of incentive to solve this problem to defend our land.

Second, the strategy response. An effective strategy response is a multi-billion dollar national priority investment run by the country's best expert focused on defensive capabilities as soon as possible. This will require an unprecedented level of collaboration between government and the private sector. Think in terms of a national cyber militia, where our private sector and government are working hand in hand to defend our critical systems against nation-state adversaries.

We must start now. The capabilities will take a minimum of 3-years to establish and will take beyond that to put into effect. We

cannot wait until we are in the middle of a disaster to begin this development of these capabilities.

A program of this order requires a very, very large ante. We estimate a $500 million ante to begin this program is essential.

The organization is inherently multi-agency. Ultimately, we will need a centralized national level, top talent, agile, small special projects office to coordinate and run this effort throughout this program.

Third, Congress can help today by doing three things:

First, support required funding levels. We are talking about $50 million for the Department of Homeland Security R&D. That is an order of magnitude off for the ante. We are in deep trouble.

Second, advocate this initiative to agency heads in a formal letter to motivate immediate discretionary investment to begin to jump start this program right away.

Third, lead the way by commissioning blue ribbon panels and special investigative committees to help establish momentum. Inaction isn't an option for any of us who know the stakes and are entrusted by the people to provide for the common defense and to protect the future of this great Nation.

The PCD stands ready to help.

Thank you.

Mr. LANGEVIN. Thank you, Mr. Saydjari.

[The statement of Mr. Saydjari follows:]

PREPARED STATEMENT OF O. SAMI SAYDJARI

Chairman Langevin, Ranking Member McCaul, and Members of the Subcommittee, it is a pleasure to have this opportunity to testify before you on an issue that is of utmost national urgency. I come to you as the leader of the Professionals for Cyber Defense, a non-profit group of recognized national cyber security leaders dedicated to advocating for the development of a sound cyber defense policy for the United States.

Summary. (1) The US is vulnerable to a strategically crippling cyber attack from nation-state-class adversaries. Cyber space primarily controls our real-world critical assets and is as legitimate a part of our territory as physical land, thus the government must *provide for the common defense* of this new territory. (2) A strategic multi-billion-dollar investment run by the country's best experts can mitigate this risk if we start now with $500 million. (3) Congress can help today by supporting this funding level, advocating this initiative to Agency heads in a formal letter to motivate immediate discretionary investment, and leading the way by commissioning blue-ribbon panels and special investigative committees to help establish momentum.

Imagine the lights in this room suddenly go out, and we lose all power. We try to use our cell phones, but the lines of communication are dead. We try to access the Internet with our battery-powered laptops, but the Internet, too, is down. After a while, we venture out into the streets to investigate if this power outage is affecting more than just our building, and the power is indeed out as far as the eye can see. A passer-by tells us the banks are closed and the ATMs aren't working. The streets are jammed because the traffic lights are out, and people are trying to leave their workplaces en masse. Day turns to night, but the power hasn't returned. Radio and TV stations aren't broadcasting. The telephone and Internet still aren't working, so there's no way to check in with loved ones. After a long, restless night, morning comes, but we still don't have power or communication. People are beginning to panic, and local law enforcement can't restore order. As another day turns to night, looting starts, and the traffic jams get worse. Word begins to spread that the US has been attacked—not by a conventional weapon, but by a cyber weapon. As a result, our national power grid, telecommunications, and financial systems have been disrupted—worse yet, they won't be back in a few hours or days, but in months. The airports and train stations have closed. Food production has ceased. The water supply is rapidly deteriorating. Banks are closed so people's life savings

are out of reach and worthless. The only things of value now are gasoline, food and water, and firewood traded on the black market. We've gone from being a superpower to a third-world nation practically overnight.

We saw what happened to the social fabric when Hurricane Katrina wiped out the infrastructure in a relatively small portion of our country: chaos ensued and the impact lasted a long time. What would be left after months of recovery from such devastation nationwide? Such strategic cyber attack scenarios are plausible and thus worthy of urgent attention. We are a nation *unprepared* to properly defend ourselves and recover from a strategic cyber attack.

My purpose today is to make a case for congressional action to support a major government initiative that could mitigate the risk of a devastating strategic cyber attack against the US. To understand the plausibility of such attacks without undertaking any action would be unconscionable. Even uncertainty by government leaders regarding such plausibility demands immediate action to remove the uncertainty and enable responsible policy decisions. The only rational approach to address a problem of this magnitude and scale is a concerted high-priority government program on the order of the Manhattan Project. Failure to embark on such a program now will have disastrous consequences to our national interests sooner rather than later.

I will now review the **case for action** our group made in a letter to President George W. Bush in 2002, highlight the true nature of the **national strategic threat** in a realistic cyber attack campaign called Dark Angel, outline the only reasonable **strategic countermeasure** in the form of an urgent, high-priority, multi-billion-dollar national program that we've dubbed the "Cyber Manhattan Project," point to some recent promising but woefully underfunded **cross-agency analysis and planning that affirms** both the grave situation and the need for a national program, and then I'll close with some recommendations on moving forward.

Background. In 1939, Albert Einstein felt duty-bound to warn President Franklin Roosevelt of a strategic threat to the country from nuclear weapons and the need for immediate action. In 2002, more than 50 leading cyber defense experts similarly felt compelled to warn President Bush of a strategic threat of a different kind, one to our critical information infrastructure. On 11 September 2001, terrorists used our air transport infrastructure against us and made a serious impact on both our economy and sense of security. Against a strong country such as the US, frontal attacks make little sense, but our vulnerability to infrastructure attacks makes such attacks increasingly likely.

The signers included a former Director of Central Intelligence, a former Director of the National Security Agency, a former Director of the Defense Advanced Research Projects Agency, and many of the nation's leading scientists and engineers. We warned President Bush that (a) the situation was grave, with nation-states such as China developing serious offensive capabilities, (b) a national initiative with priority, top talent, funding, and focus on par with the Manhattan Project was urgently needed to create cyber defense capabilities in close partnership with industry, (c) threading together components of national exercises, results from accidental information system failures, and actual cyber attacks, one could create devastating scenarios of strategic damage to the US, and (d) that the private-sector economy wouldn't solve the problem without government leadership because of a lack of incentive to do so. Since we signed the letter, little has changed with respect to the situation or the trend. It's time to move forward.

A subset of the signers formed a group called the Professionals for Cyber Defense (PCD) to engage in continuous advocacy. In summer 2002, the PCD panel reviewed the President's draft National Strategy to Secure Cyberspace. They found that the plan offered valuable advice to counter lower-grade threats but that it had a fundamental flaw in its unstated premise that there was no strategic national threat. In response, ***we recommended that the government urgently initiate a scientific process to establish the scale, gravity, and validity of the national strategic threat of cyber war against our nation.*** We expected that such a process would validate the repeated warnings from the technical community in reports from the Defense Science Board, National Academy of Sciences, and the President's Commission.

But in our dialogue with the government, we learned of two barriers to aggressive action: (1) the perception that government investment would require "big government" private-sector interference, and (2) the case for national strategic vulnerability wasn't yet credible to senior leadership. In retrospect, on the first issue, we failed to realize that government leadership simply did not see cyber space as a territory on which we deeply depend and that must be protected and defended—rather, some people in leadership positions viewed it as an optional digital playground of

bits and bytes for exchanging personal messages or looking at hobby information. But this isn't a matter of "big government" versus "small government"; it's a matter of our government stepping up to its constitutionally required duty to defend the US against threats beyond the capabilities and means of the private sector. We deeply understood the second issue, which is why we advocated for an urgent national-scale analysis of the vulnerability as the starting point for a program plan. In September 2002, the panel decided to sketch a case for action in the form of a realistic strategic cyber attack campaign against the US called "Dark Angel." This sketch was intended to be a starting point because it could demonstrate the problem's gravity.

The Threat: Dark Angel. What is the problem, and what is the solution? For the problem, we must ask if a strategic national vulnerability exists, what its scope is, and how bad "bad" can get. Without understanding the detailed nature of the problem, the efficacy of any proposed strategy is unknown. We must also ask why any proposed national strategy will solve the problem, and what happens if it doesn't. These seem like childishly simple questions, but the answers have been elusive. Indications are that national economic devastation is quite possible, and when we're in the middle of the disaster isn't the time to start thinking about how to respond. Preparing for cyber war will take in excess of three years and require infrastructure instrumentation for critical computer systems, experienced cadres of defenders who are well trained and exercised, control systems to execute strategic responses, effective architectures to mitigate risk, and a national program to create defensive capabilities. Thus, *understanding* the problem is an immediate need.

Planning. The small PCD planning team included a campaign planner, two experts in the financial sector, three in electrical power, and one in transportation. We assumed only unclassified critical infrastructure vulnerabilities. Our intent was to illustrate the damage a robust campaign that used multiple attack paths could cause and to create a plan with sufficient detail to convince experts in the domain. The plan took roughly 30 days to create. We assumed the adversary had three years of preparation, $500 million, and 30 days to actually execute the attack. The attack campaign's goal was to destabilize the US and depress the economy with attacks on critical infrastructure, thus reducing our ability to project military power, depleting our will to fight, and creating panic and distrust in the government.

Our strategic campaign objectives included crippling rail transportation, rupturing oil and gas pipelines with improper control (for example, with cyber attacks similar to the one on the Soviet Trans-Siberian pipeline causing a three kiloton explosion, as described in "At the Abyss" by Thomas Reed), and creating widespread power outages by destroying hard-to-replace generators and power-line transformers with improper computer control commands. We also simulated attacks on financial services sectors, thus creating mass confusion in transaction settlement systems, flooded 911 systems with computer-controlled false alarms to create widespread panic, and disabled Internet service by performing denial-of-service attacks on the 13 main Domain Name Servers (as has already been partially done in actual cyber attacks).

In the simulated campaign, we spoofed attack attribution when possible to focus attention in the wrong direction; used lethal first strikes (for example, by hitting first responders and backups before hitting primary cyber targets); used a rolling attack barrage to interfere with recovery processes; delayed attacking instruments, such as the Internet, until that means was no longer needed in the campaign; bought cyber mercenaries and insiders as needed to gain capabilities and access; used non-cyber (physical) attacks on "tough" targets as needed; used psychological operations to create distrust in infrastructure and manipulate public opinion; and hampered the military by disrupting civilian re-supply chains.

Our simulated attacks were vetted with experts in each of the key critical infrastructure domains. The essence of the plan and its likely effects were verified. There was some uncertainty about the consequences of some attacks—even now—but this was due to a lack of knowledge among the entire community to fully assess such consequences. ***It would be hubris to think our adversaries don't already have a plan in place that's substantially better than our brief sketch or that their capabilities to execute such an attack aren't improving.***

Follow-on. A proper national strategic threat assessment would parallel that of Dark Angel, and would involve top industry experts and business leaders, mix in military campaign planners, and mix in economists, policy makers, and others as needed. Sharing across industry should be encouraged and rewarded. From a management perspective, the assessment should carry presidential authority and priority. There should be three separate teams: one for planning and completing a concrete plan, one to execute the plan to the extent needed for demonstration purposes, and one to review the results for validity.

The assessment must start from the premise built into Dark Angel: that cyber warfare will be economic and social warfare. Diagnosis of the source of vulnerabilities must be included and reflect that the organization and design of our production systems will often be more important than cyber defense technology in determining the nature and extent of the destruction. What to defend and what kinds of damages to prevent are *not* self-evident without such an assessment.

For illustrative purposes, we estimate the resources needed for six critical infrastructure domains would take about $70 million, 300 top-talent experts, and 9 calendar months. ***The final report would be a definitive estimate of our true national strategic vulnerability to cyber attacks, a compelling case for action, and the basis of a prioritized program plan.***

Countermeasure: Cyber Manhattan Project. As part of our dialogue with the government in 2002, we elaborated on the proper solution to the strategic vulnerability sketched out by our Dark Angel analysis. Cyber war defense requires orders of magnitude more government involvement and resources to avoid overwhelming national damages from strategic attacks. We recommended that the government (1) step up to a strong defense role against serious attacks, (2) focus on countering strategic attacks that have real-world effects, (3) develop a top-down architecture and engineered approach to the defined problem, (4) acknowledge that current technology is insufficient to defend against cyber war, and (5) divide the cost burden between the owner (to protect critical private cyber assets) and the government (to protect the integrity of the national commons).

As mentioned earlier, we chose the name "Cyber Manhattan Project" to reflect the urgency, priority, focus, top-talent, and funding levels needed. We acknowledge that aspects of the analogy are inapt, such as the fact that (1) there is no single, easily measurable artifact (such as a bomb), (2) a broad spectrum of talent and organizations must be involved, (3) much of the work must be conducted without classification constraint, and (4) once an initial capability is achieved, a continued investment will be needed to maintain our cyber defense's effectiveness. We sketch the program below.

Vision. We must rapidly overcome our nation's vulnerability to coordinated strategic cyber attacks from serious enemies.

Project Description. We need an aggressive, goal-directed, high-priority, national program to address the high-level threats that endanger the national well-being. To do this, we must engage the brightest scientists, business experts, and engineers, and provide them with adequate resources. To guide the program with strategic objectives, we need a top-down architecture that establishes concrete cyber defense capabilities on a specific timeline, including near-term capabilities within three years.

Capabilities. Some cyber defense capabilities to include are as follows: (1) capability to create system resiliency and quickly recover from inevitable partially successful attacks; (2) a national cyber Command, Control, Communication, and Computer Intelligence, Surveillance, and Reconnaissance (C4ISR) system to measure and control mechanisms at multiple echelon levels; (3) a national threat assessment capability to drive decisions at some "required" level; (4) cyber firebreak mechanisms and architectures to slow down attacks and reduce potential damage; (5) capability to gather intelligence and inject uncertainty through strategic deception; (6) capability to model and simulate the enemy, thereby honing our defenses before incurring damaging strategic cyber attacks; and (7) capability to identify and understand available and acceptable responses from technical, strategic, legal, economic, and political perspectives.

Urgency. Major potential adversaries are actively pursuing cyber war capabilities, which indicates the increasing probability of future cyber campaigns. Moreover, (a) current cyber defenses and best practices are ineffective, (b) active measures to shut down our adversaries' abilities to attack through physical access will drive them to cyber space, and (c) we face potentially greater vulnerability and lethality from combined cyber and physical attacks. Finally, ***developing a defense to this threat is a multiyear effort, so we can't wait until we find ourselves suffering in the midst of our first major strategic attack campaign.***

Priority. A major initiative on the order of the Cyber Manhattan Project is *the* right path to address our current situation. The offensive threat is growing, so defense must be fielded at a faster rate. A top-down approach with a driving architect can address the problem and achieve the requisite objectives, but bottom-up efforts, even if coordinated, leave gaps because there's no ownership of key parts of the problem. Cyber defense mechanisms must integrate into a coordinated system, and cyber defense operations must comprise a fully integrated defensive force. For suc-

cess, the creation of national cyber defense capabilities must be a national funding priority. Can you imagine the original Manhattan Project succeeding without such a focus?

Feasibility. Not only is the creation of national cyber defense capabilities critically urgent and important, it's also feasible. (1) *Technically,* many effective defensive technologies exist but are in research stages and must be transitioned to operational use; some already have limited field testing, and others already exist to address broad classes of novel attacks. Moreover, the required computational resources for intensive activities such as correlation of attack and modeling/simulating attack strategies and tactics are available today. Ongoing research sponsored by the likes of NSA, NSF, DOD, DNI, DHS, and others is beginning to address additional hard science problems. (2) *Economically,* we can make a national business case for investing in a program intended to avoid the expected financial losses from strategic cyber attacks and ensure the proper public-private sharing of the burden. (3) *Operationally,* we can manage the complex infrastructure though judicious use of automation with a capable cadre of defenders. Through a combination of reasonable fire-code-like cyber security standards, improved operational guidance, and trained/experienced personnel, we would also be able to contain mission and cost impacts in the short term while we develop new capabilities. (4) *Politically,* public awareness of the threat is likely to make needed investments and standards acceptable. Industry is increasingly aware that nation-state-level attacks are a concern beyond their current ability to handle, yet they threaten business continuity. With proper financial incentives and partnering for workable solutions, industry is likely to openly embrace government involvement and protection. (5) Finally, from a *schedule* perspective, a phased rollout of capabilities based on threat prioritization and available technologies is also feasible. Success is certainly not assured, but the alternative is to begin radically reducing our dependency on computing systems, which would seriously degrade our national competitiveness and suppress economic growth. The cyber vulnerabilities in our infrastructures have become deeply embedded and widespread through the economic forces that drive individual companies to reduce costs by adopting the most widely available and interoperable technologies. It won't be easy to develop a cyber infrastructure that can resist strategic attacks—it will require short-term actions as well as a long-term plan and a willingness to keep that plan in focus over a number of years.

Plan of Action. We recommend assigning a government lead responsible for creating a plan. The PCD offers to work with this lead and recommends a three-month deadline for developing a "blueprint" to launch the project, including technical and program management aspects. We also recommend jumpstarting a multiyear program now with as much seed funding as possible.

The PCD hasn't worked out a full recommendation for how a Cyber Manhattan Project, which would inherently involve multiple agencies, ought to be organized and managed. A few points of consensus, though, appear to be emerging. (1) Distributing a surge of funding to the myriad bureaucracies that currently fund cyber defense won't work in the long run. Each bureaucracy pulls in a different direction, making focused investment nearly impossible, although a jumpstart in 2007/2008 might have to start this way out of sheer practicality. (2) Centralizing funding and government-wide responsibility in one existing department or agency with its own mission will likely cause the funding to be spent by that bureaucracy's priorities, to the detriment of national interest. (3) Creating a whole new department or agency might fall into the too-hard-to-do pile, given the tremendous distractions and delays involved (as we've seen with the startup of the Department of Homeland Security).

Eventually, what we need is a centralized, light-weight, high-level controlling body to create a focused effort on national cyber defense capabilities. One thought has been to create a special projects office accountable to and operating with the authority of the White House, with an elite staff of 200 people, at least half of the overall program budget, and some purview over the spending of the other half distributed and executed by existing organizations.

Recent Developments. Recent activities tend to echo and affirm the PCD's earlier findings. In November 2006, in response to concerns of inherent computer system vulnerabilities and escalating threats, more than 60 experts in system security, processor design, operating systems, programming languages, networking, and applications from diverse backgrounds in academia, government, and industry met to consider past, current, and possible future approaches to building systems with improved security. Findings from this Safe Computing Workshop included the following: (1) attackers rule, disasters are likely; (2) short-term measures are essential but insufficient; (2) market forces won't change the balance; (3) usability and man-

ageability must be part of the solution; (4) new technology can catalyze major changes; and (5) only a national initiative will make a real difference.

The workshop participants also concluded that the timing of such an investment is particularly good now because (1) significant advances in technology have dramatically increased hardware processing, memory, and communication capacity; (2) there's a growing understanding of the problem among the public and government leadership as everyday cyber attacks like spam, phishing, and identity theft become increasingly painful; (3) industry's interest in cyber security continues to grow as the community becomes more adept at making a business case for improvements; (4) escalating attacks and damages are increasing across the globe; (5) major software vendors are willing to delay the release of their products for more than a year to forestall security embarrassments; and (6) without a major change in direction, adversaries will be able to exploit current weaknesses in US cyber security and could deal a critical blow to our country's major industrial sectors, such as banking, energy, and telecommunications. ***The workshop participants found a compelling and urgent need to dramatically reduce the vulnerability of the national information infrastructure to attack, and that major, strategic investments could significantly reduce our vulnerability over a five-year period.***

Closing Remarks.

Smoking Gun. Some of you might think, what's the rush? Where's the smoking gun—the indication of a major assault on US cyber infrastructure? Surely, it's coming, and it's no doubt already in its planning stages. We suggest three reasons for why this is so. First, strategic long-term damage requires substantial planning and very well-timed execution. Creating the capabilities and placing the required assets (such as insiders) takes time, certainly years. Second, when such a cyber attack weapon is created, it's in some sense a one-time-use strategic option. One wouldn't use it lightly, nor would one want to tip one's hand about it until it's really needed: such weapons may well be deployed already, and we wouldn't know it (perhaps a sleeper cell of insiders and/or malicious software embedded in our critical infrastructure). Finally, our current cyber infrastructure offers a wealth of highly valuable knowledge (such as advanced research results). As adversaries conduct espionage, they're also mapping our cyber space and gaining great experimental and training experience that will enable future strategic attacks. It's in the interests of our adversaries to preserve their upper hand for as long as possible and keep tapping into these important attributes. Moreover, such nation-state network exploitations are becoming increasingly obvious to the point that the mainstream press regularly covers them.

Secrecy. We don't advocate that a Cyber Manhattan Project be shrouded in secrecy: doing so would be unnecessary and deleterious to the program goals. The nation's best minds must work on this difficult problem, and many of them are to be found outside government in academia and industry. Excluding those minds by making the program secret would only decrease our chances of success. Obviously, it makes some sense to maintain the element of surprise about the details of some of our planned defenses, but these should be carefully thought out and very limited in scope. A design that counts on its own secrecy to succeed isn't a robust design at all: we all know how fleeting secrets can be.

Stakes. But what if we don't do this? Ladies and gentleman, based on the vetted Dark Angel scenarios, we could compromise our country as we know it if we make a misstep today. Inaction isn't an option for any of us who now know these stakes and are entrusted by the people to *provide for the common defense* and protect the future of our great country. Thank you.

Mr. LANGEVIN. Dr. Maughan.

STATEMENT OF DOUGLAS MAUGHAN, PROGRAM MANAGER, CYBER SECURITY R&D, DEPARTMENT OF HOMELAND SECURITY, SCIENCE AND TECHNOLOGY DIRECTORATE

Mr. MAUGHAN. Chairman Langevin, Ranking Member McCaul, members of the subcommittee, thank you and good afternoon.

Today, I will be sharing with you information on the cybersecurity research and development program in the Department of Homeland Security Science and Technology Directorate. I also will outline for you critical areas where new research and development

efforts are needed. Details of the Directorate's program are included in my written testimony. I will provide a brief summary.

The program's mission is to drive cybersecurity improvements in existing and emerging technologies; discover solutions to detect, prevent and respond to attacks on our critical infrastructure; and deliver new, tested solutions for cybersecurity threats, making them widely available to all sectors.

Unlike other government programs, we cover all phases of the R&D lifecycle, not just research, but research, development, testing, evaluation and transition. Because our research is unclassified, we produce solutions that can be implemented for our customers in both the public and private sectors. We aim for results that can have impact in every home and business in the U.S. and throughout the world because cyber threats affect everyone.

Consider the following: Cybersecurity breaches have real economic consequences. Internet users who shop online spend an estimated $8 billion per month. But according to a recent Consumer Reports survey, 86 percent of American internet users have changed their behavior due to fears of online theft; 25 percent have stopped shopping online altogether for that reason.

A 2005 Cybersecurity Industry Alliance study found that 65 percent of American voters indicated that the government needs to do more to protect our information and systems from cybersecurity threats. Worldwide cyber attacks were estimated by the Congressional Research Service at a cost of $226 billion in 2003. The cost impact of these attacks is most certainly higher today.

The DHS Cybersecurity Research and Development Program budget totaled $13 million in fiscal year 2007. The President has requested $14.8 million for fiscal year 2008. I would like to share with you some positive results that we have accomplished.

We have funded small businesses and universities to solve near-term cybersecurity problems, such as malicious code detection, insecure wireless networks, open source software vulnerabilities and identity theft.

We have funded research that has led to more than 10 open source and commercial products in the past 3 years alone. Examples include secure thumb drives, root kit detectors and security solutions for process control systems. We have brought together entrepreneurs, venture capitalists and system integrators to speed the transition of these innovative cybersecurity solutions for commercial and government use.

We have created a cybersecurity testing environment comprised of a test network and test data sets containing real traffic data to support the research community.

And we have led an international effort to advance the deployment of critical solutions required to secure the Internet infrastructure as called for in the National Strategy to Secure Cyber Space.

We need to continue our efforts to bring these important cybersecurity solutions forward, but more is needed. The DHS Science and Technology Cybersecurity Program, in concert with our customers, has identified five research areas as priorities which we will continue to address as we face the future.

We need to develop more secure versions of basic Internet protocols and architectures to ensure that the Internet works safely the way users expect it to.

We need to create new ways to detect and contain attacks and develop resilient systems and detect and mitigate insider threats.

We need to build research infrastructure and tools to support cybersecurity research and development efforts.

We need to find new technologies to reduce the vulnerabilities in our process control systems that underlie our Nation's critical infrastructure.

And we need to develop trusted systems and the metrics to assess them.

Mr. Chairman and members of the subcommittee, the good news is we are making progress. The Directorate's research and development results show promise, and I look forward to working with you to address the security needs of the Nation's critical infrastructure.

Thank you. I look forward to answering any questions you may have.

[The statement of Mr. Maughan follows:]

PREPARED STATEMENT OF DR. DOUGLAS MAUGHAN

Chairman Langevin, Ranking Member McCaul and Members of the Subcommittee, thank you and good afternoon. Today, I will be sharing with you three important aspects of our work in cyber security research and development in the Department of Homeland Security (DHS) Science and Technology (S&T) Directorate, including our efforts to:

- **Drive security improvements** in existing technologies and emerging systems.
- **Discover solutions to detect, prevent and respond to cyber attacks** on the Nation's critical infrastructure.
- **Deliver new, tested solutions for cyber security threats** and make them widely available to all sectors through technology transfer and other methods.

The S&T Cyber Security R&D goes through the full R&D lifecycle—research, development, testing, evaluation and transition—to produce unclassified solutions that can be implemented for our customers in both the public and private sectors. Therefore, we are able to move these solutions from the lab to real life, so they reach the U.S. businesses and citizens who need them to secure their networks. It means that the results of our research can have an enormous impact in every home and business in the United States, as well as throughout our government and the world. In the past three years alone, the DHS Science and Technology Directorate has funded research that today is realized in more than 10 open-source and commercial products that provide capabilities such as: secure thumb drives, root kit detection, worm and distributed denial of service detection, defenses against phishing, network vulnerability assessment, software analysis, and security for process control systems.

Cyber threats pose an ever-growing risk to our national and economic security. We face enormous challenges in our ability to meet or even anticipate those threats. Today, I hope to describe briefly for you: the scope of the problem; and the positive steps we are taking to drive, discover and deliver new solutions.

The events of September 11, 2001, made clear that the security of our Nation and our economy are intertwined. The majority of government communications utilize private-sector networks, including critical infrastructures—such as information technology, communications, financial services, electricity, and oil and gas systems. These networks have proven interdependencies that are critical to response capabilities as well as business operations. The systems of these sectors have converged and are interconnected. For example, if the electrical grids fail, that failure impacts the communications systems, which in turn can hamper financial networks.

The Internet connects all other networks, including our Nation's critical infrastructure. It has become the central nervous system for our government, our citizens and our industries. When it is attacked, the effects can ripple far and wide. Although the Internet was developed to provide "essential minimum communications" in the event of a nuclear attack, it was not designed with security in mind. Thus, the technology that is deployed over most of the Internet today has vulnerabilities

that can be exploited, endangering all the connecting networks, including our critical infrastructures.

Beyond the Internet, few of the technologies we use every day are adequately protected against malicious attacks. Cell phones, PDAs, and wireless networks are vulnerable, as are the supervisory control and data acquisition (SCADA) systems underlying our critical infrastructure. Attacks on these technologies have forced us into a defensive posture, and the financial costs are significant. Attackers can reach our business and government systems through the maze of networks connected by the Internet.

A 2004 Congressional Research Service (CRS) report stated that cyber attacks on publicly traded firms resulted in losses of 1 percent to 5 percent on the firms' stock price in the days following an attack. For the average New York Stock Exchange company, this means shareholder losses in the range of $50 million to $200 million. CRS reported that total losses worldwide in 2003 attributed to viruses, worms, and all other hostile digital attacks were $226 billion. These attacks can come from rogue actors (such as script kiddies, disgruntled employees, and organized crime), terrorists, insiders, and other nation states.

But it is not just companies and governments at risk: Our citizens also are vulnerable. Government action can help protect U.S. consumers who, in many cases, cannot adequately protect themselves from threats that come from our cyber infrastructure. Countering these threats requires the deployment of new technologies across the global infrastructure.

Americans make extensive use of the Internet. March 2007 global statistics indicate there are more than 210 million Americans—70 percent of our total population—using the Internet. On their private computers, our citizens are targeted by viruses, worms, and phishing schemes. Their computers may be used as launching pads for attacks against other systems, unbeknownst to the computer owner. To date, more than 150 million records containing personally identifiable information have been exposed since January 2005, according to the Privacy Rights Clearinghouse.

According to a 2005 *Consumer Reports* survey in the U.S., 86 percent of Americans who go online have made at least one behavior change due to fears about online theft. 29 percent have cut back on shopping online, and another 25 percent have stopped shopping online altogether. A 2006 survey from the Cyber Security Industry Alliance (CSIA) found that Internet users who do shop online indicate that they spend an average of $116 per month per person—an estimated $8 billion per month in total—but that half of all users avoid making purchases because of fear of identify theft or compromise of financial information.

Indeed, citizens want the Federal government to bring forward cyber security protections. A 2005 survey of U.S. voters—both Internet users and non-users—conducted by CSIA found that respondents look to the U.S. government to help with cyber security issues. Sixty-five percent of the respondents indicated that the government needs to do more to protect information and systems.

In fact, the Department of Homeland Security's Science and Technology Cyber Security program serves all of these customers, which include both DHS internal components and private sector entities: Cyber Security and Communications (which includes the National Cyber Security Division and the National Communications System), U. S. Secret Service, DHS Chief Information Officer (CIO), Internet infrastructure owners and operators, critical infrastructure providers, and the information security research community. The Directorate leads the government's charge in funding cyber security research and development that results in deployable security solutions, as directed by the President in the *National Strategy to Secure Cyberspace.* Our research and development funding is targeting the critical problems that threaten the integrity, availability, and reliability of our networks. We provide solutions and research resources that advance our understanding of cyber security risks. Our goals are:

- To protect our national and economic security interests and secure our homeland.
- To enable the government, industry, and citizens to make better-informed decisions about cyber security risks.
- To provide the resources needed to counter and mitigate these risks.

The United States played a formative role in the Internet's creation, and is home to ten of the thirteen root servers that control the communications flowing over the Internet. However, today's security vulnerabilities cannot be addressed in isolation. Today, there are 243 countries connected to the Internet and approximately 1.2 billion online users worldwide. It is a global problem that affects governments, businesses, and citizens. To get this important work done, the S&T Cyber Security R&D program carefully collaborates with private industry, Federal agencies and other

governmental entities, and private-sector partners in other nations, reflecting the truly global nature of the Internet.

There are legal issues and international coordination issues that need to be addressed, but there are also complex technical problems that need to be solved. The price tag for this research and development is high, but it is minimal compared to the cost of cyber attacks today. Let me restate for the members of the Subcommittee that worldwide cyber attacks were estimated by CRS at a cost of $226 billion in 2003. The cost impact is most certainly higher today. The Department of Homeland Security's Science and Technology Directorate's cyber security research and development budget totaled $13 million in FY 2007 and the President has requested $14.8 million for Fiscal Year 2008.

Today, I'm going to discuss three important areas where we are:

- Driving security improvements to address critical weaknesses in the Internet's infrastructure
- Discovering new solutions for emerging cyber security threats, by incubating ideas and innovation in safe testing environments and public-private partnerships
- Delivering new technologies tested in a real-world environment and making them widely available for real-world users in all sectors

I also will describe for you those research areas identified in concert with our customers that are ongoing priorities which we will continue to address in FY2007, FY 2008 and beyond:

Driving Security Improvements to Address Critical Weaknesses

The Department of Homeland Security's Science and Technology Directorate is leading efforts to secure two of the Nation's major technology vulnerabilities: security weaknesses in the Internet's domain name system, or DNS, and vulnerabilities in the Internet routing system. Attacks against these two parts of the Internet infrastructure are particularly insidious because computer users cannot detect them. Attack traffic is estimated to have skyrocketed 150-fold since 2000.

Both domain name system and routing vulnerabilities can deny service to small or large portions of the Internet, make tracking and tracing Internet communications very difficult, or allow communications to be redirected without the user's knowledge. In the dot-com and dot-net domains alone, domain name queries are made an average of 24 billion times a day, yet Internet users have no guarantee that they will reach the Web site they want when they enter its address in a browser. Symantec's most recent *Internet Security Threat Report* notes that, in the first six months of 2006, spam made up 54 percent of all monitored e-mail traffic. Much of that spam takes advantage of weaknesses in the routing system, and uses it to mask spammers' identities, making it difficult, if not impossible, to track them down and prosecute them.

U.S. government leadership in addressing these critical vulnerabilities is essential, and the President's *National Strategy* calls on DHS to drive the efforts to bring solutions forward. By working in a collaborative effort across Federal agencies, private industry, and global Internet owners and operators, the DHS Science and Technology Directorate has made progress toward addressing these problems. In cooperation with NIST and the Department of Commerce, our Directorate leads the effort to develop domain name security extensions (DNSSEC), and we work with international counterparts and key technical groups to develop improvements to the standards that govern addressing and routing.

Both of these infrastructure security problems have, or soon will have, solutions driven by our government's leadership. The remaining challenge lies in convincing the many owners and users of the Internet to *deploy* them, from private industry and foreign governments to our own state, local and federal agencies in the U.S. New requirements under the Federal Information Security Management Act (FISMA) call for DNS security extensions to be deployed across all federal agencies and their contractors. A few other countries, notably Sweden, have already deployed the important DNS security solution.

The private sector also is starting to follow the government's lead. Two major corporations working in software and information security also have announced plans to include DNS security extensions in their products going forward. Microsoft, which supplies the operating system for the vast majority of the U.S. government's desktop computers, will include the new DNS security protocols in a forthcoming upgrade of its software. VeriSign also has announced that it will include the DNS security protocols as part of an expansion that will enable it to handle more than four trillion domain name system queries per day. Many more government agencies and industries must take similar steps if we are to secure the Internet infrastructure.

VerDate Nov 24 2008 12:16 Jun 23, 2009 Jkt 000000 PO 00000 Frm 00031 Fmt 6633 Sfmt 6621 H:\DOCS\110-HRGS\110-30\43566.TXT HSEC PsN: DIANE

The government has a special role to play in coordinating the deployment of these solutions. The S&T Cyber Security R&D program is positioned to carry this work forward. Building on our research and development efforts, the government can play an even greater leadership role by taking steps to ensure the government-wide deployment of DNS security extensions and secure routing technologies, when available.

Discovering New Solutions for Emerging Cyber Security Threats

We cannot focus solely on known problems. One of the most important aspects of cyber security R&D involves understanding new threats and risks, and discovering solutions that will help us protect our Nation's cyber infrastructure. Because the research we conduct is unclassified, it can be deployed by the private sector. The S&T Cyber Security R&D program funds two efforts that provide a safe environment for cyber security research. Using small business innovation research funding and other programs in our Directorate, we also provide funding that helps bring forward the next generation of cyber solutions so they can be adapted for wider use against emerging threats. With more than 30 small business innovation research grants in progress today, as well as other funds, we are incubating ideas that emanate from small companies and devising solutions for emerging problems that will affect major sectors.

The need to create, test, and learn from potential threats poses a problem in itself. We want to test threats to the Internet, but if we conduct such R&D testing on the actual Internet, we could inadvertently put it at risk. To provide scientifically rigorous testing for next-generation cyber defense technologies, the DHS Science and Technology Directorate funds a cyber security testing environment, comprised of a test network, and test data sets containing real-traffic data.

The network, called the Cyber Defense Technology Experiment Research Testbed Program, or DETER, offers cyber security researchers a way to run experiments on a secure "virtual Internet," keeping the Internet safe. This testbed was jointly funded with NSF and now more than 50 organizations from more than 20 states—which includes major research universities, national laboratories and high-tech companies—are using the DETER test bed. The test bed began with 200 systems, and has been increasing by 200 per year with a goal of 1,000 systems spread across six sites by FY09.

In addition to a test network, researchers need data sets to use for testing their solutions. These data sets, however, have not existed, impeding effective testing of potential technologies. For example, the most widely used data source today was created in 1998 by the Defense Advanced Research Projects Agency (DARPA). Traffic data that is nine years old cannot be used to analyze today's attacks, viruses, malicious code, and traffic patterns.

The S&T Cyber Security R&D program created and funded the Protected Repository for Defense of Infrastructure Against Cyber Threats, or PREDICT program, to serve as a repository for a collection of datasets that can be used for testing new ideas and solutions. PREDICT provides datasets for information security testing and for the evaluation of maturing network technologies, to help advance them toward commercial development. The PREDICT data repository also is designed to hold datasets which can be collected from private companies, without violating their proprietary concerns, for sharing with network security researchers. The PREDICT program has taken groundbreaking steps to ensure that data privacy is protected, including reviewing the project with major privacy organizations.

As I noted earlier, another critical area of focus for the DHS Science and Technology Directorate is the development and deployment of the next generation of cyber security technologies that we need if we are to effectively face emerging threats to our Nation's critical infrastructure. We solicit research proposals for new technologies, prototype technologies and mature technologies, so that our investment yields solutions that are poised for commercial adoption. Under the first round of this research funding effort, we awarded $13.8 million. The $13.8 million funded projects in 12 states: California, Delaware, Georgia, Massachusetts, Maryland, Michigan, Minnesota, New Hampshire, New Jersey, New York, Texas, and Virginia.

Let me give you some examples of projects we've funded in this area:

- In California, Stanford University researchers are identifying and fixing serious bugs in open source code for freely available software. Widely used, open source software makes up a large part of the Nation's cyber-infrastructure, and this effort has lead to tools that are available through a commercial company named Coverity, located in San Francisco and Boston.
- In Ann Arbor, the University of Michigan's researchers are working on a secure crisis response system using handheld devices. Using low-cost disposable handheld devices, first responders will be able to have a secure mobile coordina-

tion and syndication channel—a lightweight means for interagency communication and coordination using industry-standard wireless and cell phone technologies, while keeping data transmission secure. This project partners with Lucent Technologies for commercial deployment.

• At Dartmouth College, researchers are analyzing wireless traffic to detect and respond to attacks on a WiFi network. The project is working with Aruba Networks of Sunnyvale, California, a very large wireless vendor in the United States, to develop and deploy an operational prototype and evaluate it with real-time users.

Additionally, we are partnering with the financial sector to assess the economic impact that a cyber security attack might have on individual enterprises, and developing tools to help financial companies assess and manage the risks that such a disruption of service could create.

Working with companies like Citigroup and Pershing LLC, a brokerage subsidiary of the Bank of New York, we have created a prototype of a risk management tool for the finance sector. It is designed to help create a computer simulation of a financial enterprise and its value chains, and how they interconnect with other institutions. Once it is finalized, the tool will allow them to create and run disruption scenarios tailored to their business operations, using their own proprietary data as well as generic data for the rest of the financial sector. In this way, they can find out specifically how a cyber security event or attack will affect their business, using real-time sector data while protecting their companies' proprietary data.

I want to underscore the special role that government funding has played in developing this prototype. No single financial company would build such a tool and share it with competitors; however, because of support from our Directorate, the entire financial sector will be able to assess and protect itself against emerging cyber security threats, protecting our Nation's critical infrastructure.

Delivering New, Tested Technologies Widely Available for All Sectors

New cyber security solutions do not appear in products automatically. Technology transfer from the lab to the marketplace is a vital and unique aspect of our Directorate's cyber security R&D effort. The S&T Cyber Security R&D program extends beyond knowledge and the proof of whether security solutions are feasible. Based on this foundation of rigorous research and development, we create public-private partnerships, acting as a catalyst to deliver new, tested technology solutions for cyber security threats and make them widely available for use in all sectors.

One important test we have conducted focused on handheld wireless devices, like the BlackBerry and other mobile data communications devices. These devices are expected to proliferate within government agencies. According to a 2005 survey in *Government Computing News*, 40 percent of all government managers report that they use some form of handheld wireless device. Hundreds of thousands of these devices are currently employed in government business, yet today, most mobile data architectures cannot sufficiently assure high-level government security.

To address those issues, and to identify the needs in infrastructure protection and border security, we conducted an experiment under the bilateral Public Security Technical Program between the United States and Canada. It is just one of many efforts by the DHS Science and Technology Directorate to evaluate technologies in a real-world environment and pass on the results to real-world users. Our research was looking for new technology for mobile data encryption across the US-Canada border, to learn whether additional security measures would slow down communications across the borders, and to help first responders tackle their tasks efficiently while keeping their messages secure. We tested four products of interest, including the BlackBerry, and learned a great deal about what does and doesn't work, particularly situations in which messages were delayed, or data were not transmitted.

Another important public-private partnership is Project LOGIIC, which stands for Linking Oil and Gas Industry to Improve Cyber security. The goal is to reduce vulnerabilities in the oil and gas process control system environments. The first demonstration under this project showed how to correlate and analyze abnormal events to identify and prevent cyber security threats.

Project LOGIIC is a model for government-industry technology integration and demonstration efforts to address critical research and development needs. The oil and gas industry contributed the requirements, operational expertise, project management, and product vendor channels. DHS provided the national security perspective on threats, access to long-term security research, independent researchers with technical expertise, and testing facilities. Technology pilot deployments under this program were launched in June of 2006. A planning meeting for the second phase of the LOGIIC partnership took place in March of this year.

Our Directorate also convenes a group called the Identity Theft Technology Council, which meets three times a year to bring together government, venture capital firms, financial sector representatives, academics working in identity theft, and entrepreneurs. Together, we discuss problems, research issues, available technologies, and stay abreast of emerging threats and new opportunities. As a result, venture capital firms and the companies that they fund can connect with government and larger private-sector entities to move emerging security solutions forward. The Council also works closely with the Anti-Phishing Working Group, and has issued two reports: one on phishing and one on malware.

To help technology move out of government research and development, we have sponsored three different types of transition forums:

- At the System Integrator Forum, researchers funded by the DHS Science and Technology Directorate were provided an opportunity to demonstrate their technology to an audience of major system integrators, including Perot Systems/EDS, Northrop Grumman, and General Dynamics, all of whom responded enthusiastically.
- The Emerging Security Technology Forum provided an opportunity for commercial developers to demonstrate their technology to an audience of government early adopters. Our Directorate evaluated 24 commercial technology products to defend against distributed denial of service and worm attacks, and selected 12 for presentation to an audience of government and industry CIOs and potential customers.
- Finally, the IT Security Entrepreneurs Forum—jointly sponsored with the Kauffman Foundation—provided small businesses and entrepreneurs an opportunity to learn value propositions and business plan development from the venture capital community and how to open doors into government procurement channels. Chief information officers attended from companies like Sun and Oracle.

The impact of these forums cannot be overstated. They are unique within the federal system. We bring researchers directly to the private sector, so they can demonstrate their technologies in front of more than 100 companies at a time. As I mentioned earlier, this has led to more than 10 commercial cyber security products—real cyber security solutions that can be widely used by government, industry and citizens around the world. These forums assist projects funded by our Science and Technology Directorate to transfer technology to larger, established security technology companies. Finally, they also help commercial companies provide technology to DHS and other government agencies.

Driving, Discovering and Delivering Cyber Security Solutions: The Path Forward

In the last seven years, more than 20 reports from such entities as the INFOSEC Research Council, the National Science Foundation, the National Institute of Justice, the National Security Telecommunications Advisory Committee, the National Infrastructure Advisory Council, the National Research Council and the President's Commission on Critical Infrastructure Protection have urged the government to do more to drive, discover and deliver new solutions to address cyber vulnerabilities. More recently, academic organizations, such as the Computing Research Association, and industry groups, such as the Cyber Security Industry Alliance and the Internet Security Alliance, also have called for increased funding for cyber security research and development. In addition, the Federal Government has recently produced the Federal Plan for Cyber Security and Information Assurance Research and Development, which includes cyber security R&D priorities of all agencies and departments that participate in the Network and Information Technology Research and Development (NITRD) committee.

To date, I believe that the Department of Homeland Security's Science and Technology Directorate has made excellent progress toward meeting some of the goals outlined in the *National Strategy to Secure Cyberspace.* We need to stay the course and bring these important research and development products into the marketplace. But more needs to be done if we are to counter the negative forces that threaten our cyber security.

Based on the previously cited reports which reflect the views of the professional community and in concert with our customers, the DHS S&T Cyber Security program has identified the following research areas as priorities which we will continue to address in FY2007, FY 2008 and beyond:

- We must continue to advance the development and accelerate the deployment of **more secure versions of fundamental Internet protocols and architectures,** including those for the domain name system and routing protocols described earlier.

• We must improve and create **new technologies for detecting attacks or intrusions,** including monitoring technologies.
• We must improve and create **new methods for mitigation and recovery,** including techniques for containment of attacks and development of resilient networks and systems that degrade gracefully.
• We must develop and support **infrastructure and tools to support cyber security research and development efforts,** including modeling and measurement, test beds, and data sets for assessment of new cyber security technologies, such as the DETER and PREDICT programs I described earlier.
• We must assist the development and support of **new technologies to reduce vulnerabilities in process control systems.**
• We must test, evaluate, and facilitate the transfer of **new technologies associated with the engineering of less vulnerable software and securing the IT software development lifecycle.**
• We need research to identify **new solutions to address malicious software,** such as botnets and other "malware," for which no secure solutions currently exist.
• We must **develop trusted systems,** new hardware and software architectures for security, and **develop cyber security metrics.**
• We must **develop tools that will allow us to visualize network data** so we can see where attacks are coming from and diagnose cyber security problems faster and with more accuracy.
• We must **develop new ways to detect and mitigate insider threats** in cyber security.
• We must develop the **architecture and solutions that will allow us to handle identity management on a wider scale** than is currently possible.

I want to stress for the Subcommittee that research and development involves both promise and progress. The promise lies in our ability to identify threats and potential solutions. But as long as these vital research and development questions remain unanswered, they threaten all of the progress we have made to date, creating weaknesses and vulnerabilities that further complicate our task. The same is true for the areas where we have already made valuable steps forward.

We need to deploy the important infrastructure protections we have helped to develop—across the government and throughout the private sector—and provide incentives for industry to partner in R&D efforts. We need to move forward the already identified next-generation cyber technology research projects that take aim at weaknesses we know today. And we must continue to deliver tested technologies that can become commercially available products, to extend the benefits of our research and offer protection against cyber threats to homes and businesses across the Nation.

The good news, Mr. Chairman and Members of the Subcommittee, is that our research and development efforts show promise in addressing the Nation's cyber security needs. I look forward to working with you to advance our R&D efforts and address the security needs of our Nation's critical infrastructure.

Mr. LANGEVIN. I want to thank the panel for their testimony.

I want to remind each member he or she will have 5 minutes to question the panel, and I now recognize myself for questions.

Dr. Saydjari, let me begin with you. You gave a pretty sobering assessment which you laid out. I would like to ask the panel to comment on what Dr. Saydjari testified to and if you agree with the assessment. If not, would you expand on that? Dr. Geer.

Mr. GEER. Well, sure. The threat is real. We have been, to a large degree, lucky that we haven't seen it in grander form, that there hasn't been a major episode.

One could say that—it is quite natural for most people—I expect everybody in this room, certainly my family, for example, to say that, because nothing big has happened that they are aware of, that somehow the risk must not be as great as people like Dr. Saydjari or myself or other members of the panel say it is.

If you would accept the idea that if we have ever escaped a bad event sheerly by luck, that at least you can put behind yourself the argument that the absence of any major episode to date is reassuring, I can give you one thought experiment that illustrates that

we have at least once avoided major disaster by accident. It would be this.

9/11 riveted the country. Everybody paid attention, et cetera. A week later a then-the-worst-we-had-ever-seen virus came by, something called Nimda. Like most virus writers, the person involved—like most good virus writers, amongst other things this person left behind what is called a back door, an ability to reenter the computer that they had previously invaded, but by simpler means. So even if it turned out we knew how Nimda got in in the first place and we closed that door, there would be another door remaining behind. A little bit like if I broke into your house and made a house key.

That idea of leaving behind a new back door is interesting. Nimda at the time spread faster than we had ever seen anything spread. Hands down the fastest we had ever seen. Since then, there have been faster still, but at the time it was the fastest we had ever seen.

Since all old viruses can be found somewhere on the Internet at any given time, they never actually go away, let me bring one of them up.

In 2001, a great deal of the Internet was still dial-up. A lot of people accessed it by dial-up. There is a virus called E911 which causes your modem to dial 911 constantly. When I call you on the telephone, the line doesn't drop until I hang up. When I call 911 on the telephone, the line doesn't drop until you hang up, because you don't want the police to be able to say who was I talking to when somebody cuts the wire. Consequently, you can saturate a 911 console.

Where we got lucky, no clown had the bright idea to chase the Nimda virus using its newly installed back door and install the E911 virus cross-country. Because, if they had, all 911 services in the U.S. would have gone off the air in a matter of a couple of hours. That would have had, if nothing else, been a gran mal seizure of the public confidence.

So if you accept the argument that we have at least once escaped a major event by dumb luck, then I think you can put behind yourself any argument that is it really a big deal or not. It really is a big deal if at least once we can show we have escaped a major problem by dumb luck, and I think I just gave you one.

Mr. LANGEVIN. Thank you.

Dr. LEWIS.

Mr. LEWIS. Thank you.

I am the skunk at the party here because I don't really agree with this. Part of the reason I don't agree with it is because I do have some military experience, not as a member of the military but as somebody who worked closely with them; and I know how hard it is to derail a country. Even a third-world country turns out to be much harder than we might suspect. Let me tell you the reasons that I do think that.

While we do face serious problems on the informational side, on the intelligence side, I think some of the other risks are easy to overestimate. Some of the research that I would base this on comes out of the strategy bombing survey that was conducted at the end

of the World War II by the United States, and I would be happy to provide the committee with additional information.

The first thing you have to ask yourself, though, is how resilient is a country? If there is one attack, people don't sit around; they respond. And so how long will it take people to get back on line or to restore some kind of service?

The second thing you want to ask is, a very big country turns out to be hard to derail; and you have all had this experience. The experience I usually refer to is Charlotte, North Carolina, which was taken off line for a week. No one knows about it because of snowfall and they had electronic power outrageous and all that.

You can remove major cities from the power grid and telecommunications network. It has no effect on our military power or, honestly, on our economy. A lot of this has to do with political leadership and culture.

One of the things I have said in the past is, if we were perhaps one of the more feeble European countries, if we were a more excitable country, when there was an outbreak maybe we would collapse. We have seen that happen. We have seen it happen in the past. But I think Americans are a little tougher. A lot depends on the leadership they see. If their leaders say the right things, they will respond the right way.

Finally, you want to ask yourself how interconnected are networks. There are few networks that are tightly interconnected, whether it is electrical, telecom, the financial network. These are things where you could have a national level attack and you could have that kind of affect, but most of the other stuff isn't that connected. So if you knock out one city or one State or one water company, you are not going to have a national effect.

So, for me, we need to look at the informational attacks, we need to look at espionage, and we need to look at a few critical networks that are interconnected. That is where there is risk. I am a little more relaxed on some of the other things.

Mr. LANGEVIN. Dr. Maughan.

Mr. MAUGHAN. I would have to say I agree with Mr. Saydjari in his discussion.

I will remind you that our enemies are going to continue advancing their capabilities and their technologies. And so while we may decide to sit still and that we are OK they are going to continue to advance and things are only going to get worse. I believe the investment that he called for is at a bare minimum to just keep up and may not even get us ahead.

Mr. GEER. May I add something, if I could, on this?

Mr. LANGEVIN. Briefly, please.

Mr. GEER. This is a definitional question, perhaps, back to you.

An attack that breaks things versus an attack that breaks public confidence, what I spoke to was something that breaks public confidence. I think the public confidence in, for example, our financial networks can be broken without making the entire network lay down and stay down. And so I guess perhaps what we should be pushed about is define collapse or define breakage. We may be in violent agreement once we get past that.

Mr. LANGEVIN. Dr. Saydjari, would you care to comment on what you heard, particularly with Dr. Lewis' comments?

Mr. SAYDJARI. Yes, I would.

I think, first, I would point out there are 50 of the Nation's leaders signing this letter of the President estimating this risk at this level, including a former DCI, a former director of NSA and a former director of DARPA. That is no small level of talent in making this estimation.

The second thing I would point out is that we did a very detailed analysis for this very reason, because there are people who believe that the threat is overestimated. We took a risk in developing this mock campaign against the United States to develop it to prove that this is possible, and so we believe that there is evidence that stands that says that this threat is possible. Every part of that attack analysis was vetted with various government agencies and the various sectors that were involved in the attack, including power, including oil and gas, financial service sectors and telecommunications.

We believe firmly in our analysis, and we believe that it stands on its own merits, and we invite an independent evaluation and an extension. That is indeed what we meant by calling for a national threat assessment to validate our findings and extend them so that we can develop sound policy and settle this debate as to whether the threat is higher or lower than what we are estimating.

Mr. LANGEVIN. Thank you.

I am going to have other questions for the panel that you may have to respond to in writing, but my time is expired so I am going to yield to the gentleman from Texas, Mr. McCaul, for 5 minutes.

Mr. MCCAUL. I thank the Chair.

There is so much to talk about here I sometimes don't know where to start. I am going to have to leave after this for a briefing from General Petraeus. So if the Chair would indulge me, I would like to throw everything out in one question.

Dr. Geer, you said what you can't see is more important than what you can; and I agree with that. I think the threat of the Trojan horse in this scenario is perhaps more devastating than what we can see.

Dr. Lewis, you talked about foreign agents broke into the Department of Defense and stole file cabinets. That would cause hysteria in the media. And yet we know we have intrusions in the Federal Government's networks, and I don't know if we have an idea as to what is being stolen.

You talked about metrics. I don't think we can gauge or hold accountable if we don't know what they are taking. A technical idea of attack data. We don't know where these attacks are coming from, but we know they are coming. And there are several levels of these attacks. One may be purely for mischief, one could be criminal, another espionage. As you point out, I think we talked a little bit about China and its willingness and capacity to steal information, steal secrets, intellectual property theft.

But the last scenario that Mr. Saydjari really kind of focuses on is one that really keeps me up at night, and that is the idea of a cyber attack that is along the lines of warfare. An attack we know that our own military is capable of doing and shutting down power grids in other countries, yet we don't know what some of these rogue nations, what their capacity and capability really is. We do

know that any nation with a power grid can probably figure out how to shut it down.

I think the ramifications are—I know, Dr. Lewis, maybe there has been some exaggeration, but maybe not. To the extent this country could be shut down, albeit temporarily, I think the destruction it would cause is very clear.

The idea of a national threat assessment just to gauge where are we, you threw a number out that is about 10 times more than what we authorize in R&D for cybersecurity. And I throw this out to the panel, and I appreciate the Chair indulging me on the time, but if you could talk, first of all, Mr. Saydjari, about the threat assessment that you did and what the results were and then possibly talk about—when you say vulnerable to nation-state adversaries, who do you think they are, specifically? And then I will open it up to the panel for just a full discussion.

Mr. SAYDJARI. Sure. The development that we do is called Dark Angel. This was a mock attack by seven of the leaders, Professionals for Cyber Defense, this nonprofit group; and we developed a detailed attack tree against our Nation. The purpose of it was to do a strategic blow to our country; and we looked at various domains, including the financial services sector, telecommunications, power, oil and gas. We looked at all of them.

One of the things that has been lacking to date is sort of an isolated look at each of the domains. What we looked at is looking at it from a nation-state's perspective about doing strategic damage and looking at the interconnections between those domains and doing a campaign, including rolling attacks on various symptoms. Once they recover, attack them again. Attack in a way that actually disables physical things, like power generators.

We are not talking about small-scale power outages for a day or two. We are talking about destroying power generators by improper control. We are talking about blowing up transformers by improper control. And these generators and transformers take months to remanufacture. And, oh, by the way, some of them we can't manufacture in the United States anymore. We have to go to Europe to get it. So if that attack happens in Europe at the same time, guess who is going to get priority on those transformers and power generators?

So we did this detailed analysis. We have this very, very sophisticated attack tree that has been deeply vetted by various domain experts. We did this over the course of 30 days in response to a comment on the President's national strategy to sort of put up our position that there was a serious national threat and we were forced into developing this scenario. And we believe it is absolutely compelling.

Again, we don't make this publicly available, but we invite a limited review to say, OK, you don't think the threat is this bad? Great, come look at what we did, extend what we did.

Mr. LANGEVIN. Will the gentleman yield for one second?

You said this is in the context of an attack from a nation-state. Could it also translate over into a rogue individual or individuals such as a terrorist group carrying out the same level of attack with the same type of catastrophic consequences?

Mr. SAYDJARI. Our assumption was a $500 million budget and about 3 years of preparation. So an individual certainly could not do this. But a transnational terrorist group like al-Qa'ida certainly could. In fact, that was our model as a transnational terrorist organization or a small nation-state. Certainly a large nation-state is well within their means and well within their patience.

And I point out also that we are not just assuming cyber attacks, we are assuming insider attacks, we are assuming malicious code, we are assuming lifecycle attacks, where somebody attacks the code that is being developed and gets code that blows up on us on the fly at their discretion. So we are talking about a very sophisticated attack from a military perspective against the United States.

Mr. MCCAUL. Again, that is my greatest fear, particularly if it comes from a terrorist rogue nation. Did you brief the Department of Homeland Security on this assessment?

Mr. SAYDJARI. Yes, sir. In about the March or April time frame of 2005 we did do that briefing. And they politely heard our briefing, and we saw no follow-up activity or actions from that briefing.

Mr. MCCAUL. Is that correct, Dr. Maughan? Was there no response?

Mr. MAUGHAN. That briefing was provided to the National Cybersecurity Division, not to the Science and Technology Directorate.

Mr. MCCAUL. And so you can't answer on behalf of anything outside your Directorate?

Mr. MAUGHAN. Correct.

Mr. MCCAUL. Do you think the idea of a national threat assessment is a good idea?

Mr. MAUGHAN. Yeah. The Department has been out doing physical assessments of a lot of the critical infrastructure owned and operated by the private sector. We should do a similar from a cyber perspective, both government and industry, given that industry owns and operates a significant portion of that infrastructure.

Mr. MCCAUL. I personally think it would be a good idea to be able to measure that, as Dr. Geer talks about, the metrics. Can you comment about this kind of worst-case scenario?

Mr. GEER. Sure. You mean, give you an example of one?

Mr. MCCAUL. Yes.

Mr. GEER. Do you want to take the Internet down this afternoon?

Mr. MCCAUL. I kind of would like to stay out of jail.

Mr. GEER. Well, so would I. Figure out how to worm IOS, which is the operating system for Cisco routers, which dominate the top level of the Internet. Go in and have them rewrite the EPROMs as fast as you can go. 50,000 cycles, they burn out, you now have to have to visit it with a soldering iron 3 minutes.

Mr. MCCAUL. Dr. Maughan, do you consult with experts like Dr. Geer in terms of anticipating vulnerabilities?

Mr. MAUGHAN. We do, and we try to bring in the experts every chance we can.

Mr. MCCAUL. I would highly recommend it.

Dr. Lewis, any comment.

Mr. LEWIS. I want to take the contrary view again. Some of us call these weapons of mass annoyance. If we are talking in military terms, let's talk in military terms. I am China and I go to make your traffic lights blink on and off for a week or so. Is that going

to stop the carrier battle groups from going to the Taiwan Straits? Is it going to reduce American military capabilities? Is it going to damage the American economy over the long term? The answer is no.

So if you are a Chinese leader, you think I am going to do something, it is going to really irritate them, they will be mad, and I am not going to get any military benefit from it. And that is how I think about it.

Now a rogue state, perhaps their calculus will be a little different. It is hard to predict when they are so crazy like in North Korea or Iran. A terrorist group probably doesn't have the capabilities.

But when you look at the people who are likely to do this, they are asking themselves, what do I get out of it? How likely is it to make me better off in a conflict? And, right now, they don't think it is going to make them better off.

Mr. MCCAUL. And I agree with you. China is all about espionage and intellectual property. But there are other organizations out there. And when teenagers can hack into computers, it is a little disturbing to think of the destruction that could be caused by someone who has this ability, someone who has it in the wrong hands. And I think when we know the terrorist's main goal is to destroy preliminarily our financial markets, it raises the bar.

That is really all I have, Mr. Chairman, but I want to thank all the witnesses for being here today. It has been very insightful. Thank you.

Mr. LANGEVIN. The gentleman from Texas, Mr. Green, is recognized for 5 minutes.

Mr. GREEN. Thank you, Mr. Chairman; and thank you for hosting these important meetings and hearings.

My question has to do with punishment. What has been your experience in terms of persons who are caught? How are they punished?

Someone gave the example of someone breaking into an administrative office and taking files. My suspicion is we call that a felony and the person would be severely punished. What is your experience with reference to cyber theft?

Mr. LEWIS. I have done a little research on that, and my experience and what I have learned from the FBI and from other law enforcement agencies is you are not going to be caught, and it is almost a risk-free crime. We don't have a good metric. It is true. So is it 95 percent of the people who do this escape? Is it closer to 100 percent? Is it a bit less? But the odds are, if you engage in a cyber attack, if you steal information, if you break into someone's network, particularly if you do it from overseas, it is a risk-free event.

Mr. GREEN. Any other opinions? Everybody is in agreement that it is risk free?

What about encoding? Is that something that we can hope to have some sort of safety with, some sort of encryptions for specific areas of security concerns?

Mr. GEER. I can say that, in the commercial sector, adoption of encryption at one level or another is going about as fast as it can go. That is not to say it is slow. They are spending money like crazy to encrypt.

The common thing that appears in the newspaper is I lost the laptop in the cab kind of thing or somebody broke into my house. That kind of thing is going as fast as it can go. I think that you probably will see in a matter of years nearly nothing that isn't encrypted, where the general counsel is aware that the company has it.

Beyond that, do you want all transactions and so forth, all communications over the net to be encrypted? Maybe. It is not a be-all and an end-all. It helps.

I think that you should remember that encryption is, generally speaking, no solution to the insider problem. So you might be able to get rid of a degree of the outsider problem, but you would not get rid of the insider problem by adopting full tilt encryption ideas.

Mr. SAYDJARI. I would like to add to that.

So encryption is a very valuable tool, particularly protecting information in transit. But one of our biggest problems is the security at the host. And, ultimately, the data has to be decrypted at the end machines to actually do something with it; and these are the places that we are most vulnerable. So I am a very strong advocate of getting encryption out there in a widespread way and making it available to the private sector and having it proliferate, and it will help. But I just want to make sure that we all understand that processing at the host and things like denial-of-service attacks on the availability of those hosts are affected in no way by encryption.

Mr. MAUGHAN. I would agree with what Mr. Saydjari has said. Cryptography is only going to do a small amount for us in a big picture. There are bigger problems to our end system's vulnerability. Encryption is only one tool in the quiver of arrows that we have.

Mr. GREEN. Is it fair to say that we may never be able to become completely secure because as we get better it seems that there is always a new thought or hype, idea, in terms of making the invulnerable vulnerable?

A comment please. I like your smile, Dr. Geer. Let me hear your comment.

Mr. GEER. No. Perfection is impossible because it involves dividing by zero and you can't afford the cost. This is purely a risk management problem.

If you really want my car, you can probably get it. I can lock it in the garage, I can lock the car, et cetera, et cetera. The guy with a blowtorch and a tow truck and a heavy lift helicopter can still probably get it. I can, however, make my neighbor's car a lot more attractive than mine; and to a degree that is all that we can do here. All we can do is make it such that the people who want stuff that we do not want them to have, have to go somewhere else.

Mr. GEER. And I know that sounds unfortunate, but I think that is the right mindset to have. Maybe you will have a happy surprise, and you do actually solve a problem on getting rid of smallpox or polio or something, but generally speaking, you cannot get rid of it. What you can do is make it harder. You can make them go somewhere else.

Mr. GREEN. I see other smiles, so let us go with the next smiling face.

Mr. SAYDJARI. I completely agree with Dan. I think the threat is always going to be escalating. There is always going to be higher degrees of integration of our systems and new capabilities in our systems that will be attackable, and one thing, I think, we all have to understand here is that this is not a one-shot investment. So, when I talk about a multi-billion dollar program establishing a capability in 3 years, it is not done in 3 years. It is a sustaining investment to be actively engaged in the escalation that will inevitably happen as we have seen over the last 10 years. The level of sophistication of attacks has risen dramatically over the last 10 years. The kinds of attacks we have seen in the wild are amazingly complex and amazingly sophisticated, and we will only see them get worse in terms of the level of damage they do.

Mr. MAUGHAN. I was only going to agree with them.

It is a cat-and-mouse game that we are playing with the bad guys, and we are never going to be able to secure our systems 100 percent, and so the best we can do, as Dr. Geer said, is risk management and try to defend our systems as best we can.

Mr. LEWIS. We are all in tremendous agreement here, but I want to put a little different cast on it, which is let us not think defensively. We cannot make them perfectly secure, but we just want to be in a position where we do better than our opponents. So that is a good goal. If we get more out of this than our opponents do, we win.

Mr. GREEN. Thank you, Mr. Chairman. I yield back.

Mr. LANGEVIN. Thank you.

The gentleman from North Carolina, Mr. Etheridge, is recognized for 5 minutes.

Mr. ETHERIDGE. Thank you, Mr. Chairman, and let me thank you for holding this hearing.

Gentlemen, what we are seeing in the 21st century is going to be a huge challenge. Last week, before this committee, we heard from Federal agencies—Commerce and State—talking about the attacks on their systems that were unexpected, but they may not have even been aware of them until well after they had occurred, and further, even after the illegal access was noticed, the date and duration of attacks could not be determined, and the extent of information compromised may never be known. That is what they shared with us. So my question to you is:

Is it ever possible to determine after an attack the extent of the damage? You know, for example, can logs be altered or so-called rogue tunnels be constructed to hide the nature of the attack? Do you agree? The answer is "yes"? Everybody agrees. OK.

So my next question is: What tools do we have available to us to identify the attacks, which seem to me to be critical, and to check the authenticity of the date so that we know when the attacks occurred, and to the extent we know that, how can we deal with it?

Who wants to tackle that first?

Mr. GEER. One of the hardest questions for most of us in the commercial sector is: If you know something is going on, how do you pursue it? Because it is a very fine line between noticing it and then somehow finding yourself engaged in a countermeasure. You know, do I have the right to—I was at a workshop 2 weeks ago,

and there are a couple of other people in the room who were at this same workshop. If I discover what is called a "robot network"—or a botnet—in my firm, if I discover that in my firm someone has taken over a number of computers and they are being used for purposes nefarious, do I have a right to disable that botnet? Do I have a right to poison the command and control system that it uses to operate? Do I have a right to take them off the air from where I sit?

Now, at the moment, that is, I think, roughly equivalent to, "well, if nobody knows, your general counsel would advise you not to," but in this space, there is a very fine line between how do you defend yourself and what somebody else will later charge as vigilantism.

Mr. ETHERIDGE. Let me interrupt you if I might.

If, prior to the computer, my files were in file cabinets and you come and lift out those files and, in fact, take them with you, you are in trouble.

Mr. GEER. Yes.

Mr. ETHERIDGE. This is the same kind of thing except you are doing it electronically from a remote site which may be two times removed.

Mr. GEER. Yes, but the difference there is, if I steal your car or your files, you know they are gone. If I steal your data, you may not know it is gone until it is misused. So I have to be able to react when I discover that it is going on. Whether this is "the home is the castle, and I can shoot the intruder or not," I mean, I do not know quite what to say here, but this is a problem. This is the fundamental problem on the commercial side.

Mr. ETHERIDGE. Please. We are looking for some R&D, some way we can get there because this, to me, seems to be that key we have got to find to either lock the lock or unlock the lock that we have got to get to.

Mr. SAYDJARI. So I think this is partly a question of intrusion detection systems, and the intrusion detection systems that are out there today really count on the attack's having been seen in the wild before. They are called "signature-based schemes," and they are ineffective in the sense that they are after the fact, and so a majority or certainly a very large number of attacks that are out there are not visible by these kinds of mechanisms, and that is a bad thing, and there is research, for example, on anomaly-based detection schemes that can characterize normal behavior and then look for the abnormal behavior, which is a deviation for that. So there is hope on that research line.

I will also add that the community has been using what I would consider ad hoc sensors, sorts of things that were not really designed to be sensors for the most sophisticated kinds of attacks like the ones that we imagine and work through in the dark angel campaign. So what we really need to do as a community is to work backwards from the kinds of attacks we are most worried about to the kinds of sensors that we require to detect those. I mean it is like, you know, if we were trying to detect a nuclear launch just to kind of look for, you know, some warm sensations from somebody nearby. I mean we cannot just use those kinds of off-the-shelf kinds of sensors. We really need to rethink the way we do sensors.

VerDate Nov 24 2008 12:16 Jun 23, 2009 Jkt 000000 PO 00000 Frm 00044 Fmt 6633 Sfmt 6601 H:\DOCS\110-HRGS\110-30\43566.TXT HSEC PsN: DIANE

Mr. LEWIS. Let me offer you a suggestion that is maybe a little less expensive and will not cost as much money.

One of the problems that I think we have seen is sometimes there is knowledge in the national security communities and the national security agencies like defense or the intelligence community that does not get shared or does not get shared promptly or adequately with the civilian agencies. That might be an interesting thing for you to look at. So, if DOD figures out there is a problem, how does that percolate through the rest of the Federal system?

Mr. ETHERIDGE. How do we get out of the tunnels and start sharing at the highest level?

Mr. LEWIS. Exactly. So better coordination, better information—sharing, breaking that firewall between, say, some of the national security folks. That would help.

The other thing that would help would be better network hygiene for lack of a better term. Now, that will not solve the problem, but it will reduce the number of incidents, and what you have got is some network administrators do a great job; other network administrators do not do as good a job. How do you get them all up to the a basic level? We have seen some cases where, at NASA or at DOD, grabbing the low-hanging fruit has significantly reduced the number of incidents. The systems are not secure. People are still intruding, but it is at a much lower level.

Mr. SAYDJARI. If I could extend my remarks at one more level, a colleague of mine who is an expert in the power system advises me that, if we had an attack on our power control systems, we would never know it because there are no intrusion detection systems within those networks. So, when Dr. Lewis talks about the focus on the networks that are connected, I will tell you that every network is connected to every other network in some way, shape or fashion, whether it is through software development or actual connections, and so those networks are just as likely to be attacked. Well, of course, you need some insiders or you need some malicious software, but you can attack those networks, and those networks which are controlling our most critical assets are least sensored. That is a very bad thing that needs to change immediately.

Mr. GEER. I like numbers. Can I give you a couple?

Mr. ETHERIDGE. Please.

Mr. GEER. For average desktop machines—I am not talking about, for example, the power grid. For average desktop machines, my own calculation is that about 30 percent of them have something unwanted running on them. Vent Surf says 40 percent; Microsoft says two-thirds; IDC says three-quarters. So it is not like we are trying to preserve innocence. It is a little harder.

Mr. ETHERIDGE. Yes. Well, you have scared me to death. Thank you.

Mr. LANGEVIN. Well, gentlemen, I want to thank you for your testimony today. You, obviously, addressed and raised some very sobering and very serious issues, and we obviously have a lot of work to do. We look forward to speaking with you further.

I am sure that other members of the committee, myself included, will have additional questions that we might want to pose to you, and we ask that you respond, if you would, in an expeditious man-

ner. If you could help us with that, we would be very grateful and would much appreciate it. Thank you very much, and I want to thank the witnesses for their testimony.

Hearing no further business before the subcommittee, the subcommittee is adjourned.

[Whereupon, at 2:20 p.m., the subcommittee was adjourned.]

VerDate Nov 24 2008 12:16 Jun 23, 2009 Jkt 000000 PO 00000 Frm 00046 Fmt 6633 Sfmt 6601 H:\DOCS\110-HRGS\110-30\43566.TXT HSEC PsN: DIANE

Appendix I: For the Record

PREPARED STATEMENT OF THE HONORABLE BENNIE G. THOMPSON, CHAIRMAN, COMMITTEE ON HOMELAND SECURITY

- I thank the Chairman for holding another important hearing on cybersecurity.
- It is clear that our government, working together with the private sector and academia, must do more to ensure that cybersecurity is a priority in our nation's homeland security strategy.
- In 1996, the United States government undertook the first national effort to secure our networks.
- Unfortunately, I don't believe that we are any further along today in our efforts to secure cyberspace.
- Programs and initiatives that were developed over the past ten years have been dismantled and, in certain instances, are just now being re-created by the government.
- We heard in last week's hearing that "coordinating better cyber security practices across the Federal government" is one of Secretary Chertoff's "highest priorities."
- But this rings hollow to me when I think about how long it took him to appoint an Assistant Secretary for Cybersecurity.
- I also wonder why the Secretary believes that the Department will be able to coordinate better cyber security practices across the Federal government, when his own Chief Information Officer just received a "D" in the recent FISMA grades.
- So we have a lot of work to do, but fortunately we have some very capable people who can help.
- I thank the witnesses for being here today and for their commitment to helping the Federal government move this issue in the right direction.
- Thank you Mr. Chairman.

Appendix II: Selected Major Reports on Cyber Security Research and Development

---

Biometric Research Agenda: Report of the NSF Workshop. Morgantown, West Virginia, April/May 2003, http://64.233.167.104/search?q=cache:xweu9dx2qMsJ:www.wvu.edu/bknc/BiometricResearchAgenda.pdf+Biometric+Research+Agenda:+Report+of+the+NSF+Workshop&hl=en&ct=clnk&cd=3&gl=us.

Coordination of Federal Cyber Security Research and Development, U.S Government Accountability Office, GAO–06–811, Sept. 2006, *http://www.gao.gov/new.items/d06811.pdf.*

Creating a National Framework for Cybersecurity: An Analysis of Issues and Options, Eric A. Fischer, Congressional Research Service, Feb. 22, 2005, *http://www.au.af.mil/au/awc/awcgate/crs/rl32777.pdf.*

Critical Foundations: Protecting America's Infrastructures. President's Commission on Critical Infrastructure Protection, October 1997, *www.fas.org/sgp/library/pccip.pdf.*
Critical Information Infrastructure Protection and the Law: An Overview of Key Issues. Computer Science and Telecommunications Board, National Research Council, 2003, *http://www.cstb.org/pub__*ciip.html.

Critical Infrastructure: Challenges Remain in Protecting Key Sectors, Testimony of Eileen R. Larence, Director, Homeland Security and Justice Issues, and David A. Powner, Director, Information Technology Management Issues, Before the Subcommittee on Homeland Security, Committee on Appropriations, House of Representatives, U.S. Government Accountability Office, GAO–07–626T, March 20, 2007, *http://www.gao.gov/new.items/d07626t.pdf.*

Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems, Testimony of Robert F. Dacey, Director, Information Security Issues, Before the Subcommittee on Technology Information Policy, Intergovernmental Relations and the Census, House Committee on Government Reform, U.S. Government Accountability Office, GAO–04–628T, March 30, 2004, *http://www.gao.gov/new.items/d04628t.pdf.*

Critical Infrastructure Protection: Challenges in Addressing Cybersecurity, Testimony of David A. Powner, Director Information Technology Management Issues, Before the Subcommittee on Federal Financial Management, Government Information, and International Security, Senate Committee on Homeland Security and Governmental Affairs, U.S. Government Accountability Office, GAO–05–827T, July 19, 2005, http://www.gao.gov/new.items/d05827t.pdf.

Cyber Security Research and Development Agenda. I3P, Dartmouth College, January 2003, *http://www.thei3p.org/repository/2003__*Cyber__Security__RD__Agenda.pdf.

Electronic Crime Needs Assessment for State and Local Law Enforcement, National Institute of Justice Research Report, March 2001, *http://www.ncjrs.org/pdffiles1/nij/186276.pdf.*

Embedded, Everywhere: A Research Agenda for Networked Systems of Embedded Computers. Computer Science and Telecommunications Board,National Research Council, 2001, http://www7.nationalacademies.org/cstb/pub__embedded.html.

Hard Problems List. Infosec Research Council. September 1999 (and draft revision as of September 2004) Information Technology Research for Crisis Management. Computer Science and Telecommunications Board, National Research Council, 1999, *http://www7.nationalacademies.org/cstb/pub__*crisismanagement.html.

High Confidence Software and Systems Research Needs. High Confidence Software and Systems Coordinating Group, Interagency Working Group onInformation Tech-

nology Research and Development, January 2001, *http://www.nitrd.gov/pubs/hcss-research.pdf.*

IDs-Not That Easy. Questions About Nationwide Identity Systems. Computer Science and Telecommunications Board, National Research Council, 2002, *http://www7.nationalacademies.org/cstb/pub__*nationwideidentity.html.

Information Sharing/Critical Infrastructure Protection Task Force Report, National Security Telecommunications Advisory Committee, May 2000, *http://www.ncs.gov/nstac/reports/2000/ISCIP-Final.pdf.*

Information Technology for Counterterrorism. Computer Science andTelecommunications Board, National Research Council, 2003, *http://www7.nationalacademies.org/cstb/pub__*counterterrorism.html.

Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors, Michelle Keeney, Dawn Cappelli, et al, Carnegie Mellon Software Engineering Institute, May 2005, *http://www.cert.org/cert/work/organizational__*security.html.

Internet Domain Names: Background and Policy Issues, Lennard G. Kruger, Congressional Research Service, Sept. 22, 2005, *http://www.au.af.mil/au/awc/awcgate/crs/97–868.pdf.*

The Internet Under Crisis Conditions: Learning from September 11. Computer Science and Telecommunications Board, National ResearchCouncil, 2003, *http://www7.nationalacademies.org/cstb/pub__*internet911.html.

*National Security Telecommunications Advisory Committee, Research and Development Exchange Workshop, Atlanta, Georgia, March 2003, http://www.ncs.gov/nstac/rd/nstac__*03__bos.html.

National Security Telecommunications Advisory Committee, Research andDevelopment Exchange Workshop. Tulsa, Oklahoma, September 2000, *http://www.ncs.gov/nstac/reports/2001/R&D__*Exchange2000Proceedings.htm.

National Security Telecommunications Advisory Committee, Research and Development Exchange Workshop. West Lafayette, Indiana, October 1998, http://www.ncs.gov/nstac/reports/1998/R&DExchange.pdf.

National Strategy to Secure Cyberspace, The White House, February 2003, *http://www.whitehouse.gov/pcipb/.*

Protecting Systems Task Force Report on Enhancing the Nation's Security Efforts, National Security Telecommunications Advisory Committee, May 2000, *http://64.233.167.104/search?q=cache:JkJUKZ9OmYsJ:www.ncs.gov/nstac/reports/2000/PSTF-Final.pdf+Protecting+Systems+Task+Force+Report+on+Enhancing+the+Nation%E2%80%99s+Security+Efforts,+National+Security+Telecommunications+Advisory+Committee,+May+2000,&hl=en&ct=clnk&cd=1&gl=us.*

Robust Cyber Defense. Study commissioned for DARPA ITO, Fall 2001. Slides available at:
http://www.cs.cornell.edu/fbs/darpa.RobustCyberDefense.ppt.

Technology Assessment: Cybersecurity for Critical Infrastructure Protection, U.S. Government Accountability Office, GAO–04–321, May 2004, *http://www.gao.gov/new.items/d04321.pdf.*

Trust in Cyberspace. Computer Science and Telecommunications Board,National Research Council, 1999, *http://books.nap.edu/readingroom/books/trust/.*

Understanding the Insider Threat, Richard C. Brackney, Robert H. Anderson, Conference Proceedings of a March 2004 Workshop, RAND, National Security Division, *http://www.rand.org/pubs/conf__*proceedings
/2005/RAND__CF196.pdf.

Who Goes There? Authentication Through the Lens of Privacy. Computer Science and Telecommunications Board, National Research Council, 2003, *http://www7.nationalacademies.org/cstb/pub__*authentication.html.

Workshop on Scalable Cyber-Security Challenges in Large-Scale Networks: Deployment Obstacles. Large Scale Networking Coordinating Group,NITRD, Landsdowne, Virginia, March 2003, *http://64.233.167.104/search?q=cache:mWKvtoq—xLoJ:cs.yale.edu/homes/jf/LSN-report.pdf+Workshop+on+Scalable+Cyber-Security+Challenges+in+Large-Scale+Networks:&hl=en&ct=clnk&cd=1&gl=us.*

○

VerDate Nov 24 2008 12:16 Jun 23, 2009 Jkt 000000 PO 00000 Frm 00051 Fmt 6601 Sfmt 6011 H:\DOCS\110-HRGS\110-30\43566.TXT HSEC PsN: DIANE