SPEAKERS CONTENTS INSERTS

Page 1 TOP OF DOC

75–565PS
2002

CYBER SECURITY—HOW CAN WE PROTECT AMERICAN COMPUTER NETWORKS FROM ATTACK?

HEARING

BEFORE THE

COMMITTEE ON SCIENCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTH CONGRESS

FIRST SESSION

OCTOBER 10, 2001

Serial No. 107–41

Printed for the use of the Committee on Science

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

Page 2 PREV PAGE TOP OF DOC

COMMITTEE ON SCIENCE

HON. SHERWOOD L. BOEHLERT, New York, *Chairman*

LAMAR S. SMITH, Texas
CONSTANCE A. MORELLA, Maryland
CHRISTOPHER SHAYS, Connecticut
CURT WELDON, Pennsylvania
DANA ROHRABACHER, California
JOE BARTON, Texas
KEN CALVERT, California
NICK SMITH, Michigan
ROSCOE G. BARTLETT, Maryland
VERNON J. EHLERS, Michigan

DAVE WELDON, Florida
GIL GUTKNECHT, Minnesota
CHRIS CANNON, Utah
GEORGE R. NETHERCUTT, JR., Washington
FRANK D. LUCAS, Oklahoma
GARY G. MILLER, California
JUDY BIGGERT, Illinois
WAYNE T. GILCHREST, Maryland
W. TODD AKIN, Missouri
TIMOTHY V. JOHNSON, Illinois
MIKE PENCE, Indiana

Page 3 PREV PAGE TOP OF DOC

FELIX J. GRUCCI, JR., New York
MELISSA A. HART, Pennsylvania
J. RANDY FORBES, Virginia

RALPH M. HALL, Texas
BART GORDON, Tennessee
JERRY F. COSTELLO, Illinois
JAMES A. BARCIA, Michigan
EDDIE BERNICE JOHNSON, Texas
LYNN C. WOOLSEY, California
LYNN N. RIVERS, Michigan
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
BOB ETHERIDGE, North Carolina
NICK LAMPSON, Texas
JOHN B. LARSON, Connecticut
MARK UDALL, Colorado
DAVID WU, Oregon
ANTHONY D. WEINER, New York
BRIAN BAIRD, Washington
JOSEPH M. HOEFFEL, Pennsylvania
JOE BACA, California
JIM MATHESON, Utah
STEVE ISRAEL, New York
DENNIS MOORE, Kansas

Page 4 PREV PAGE TOP OF DOC

MICHAEL M. HONDA, California

C O N T E N T S

October 10, 2001
Hearing Charter

Opening Statements

Statement by Representative Sherwood L. Boehlert, Chairman, Committee on Science, U.S. House of Representatives
Written Statement

Statement by Representative Ralph M. Hall, Minority Ranking Member, Committee on Science, U.S. House of Representatives
Written Statement

Prepared Statement of Congresswoman Constance Morella, Member, Committee on Science, U.S. House of Representatives

Prepared Statement of Congressman J. Randy Forbes, Member, Committee on Science, U.S. House of Representatives

Prepared Statement of Congresswoman Zoe Lofgren, Member, Committee on Science, U.S. House of Representatives

Page 5 PREV PAGE TOP OF DOC

Prepared Statement of Congresswoman Sheila Jackson Lee, Member, Committee on Science, U.S. House of Representatives

Panel

Dr. William A. Wulf, President, National Academy of Engineering; Vice-Chair, National Research Council
Written Statement

Dr. Eugene H. Spafford, Professor of Computer Sciences; Director, Center for Education and Research in Information Assurance and Security (CERIAS)
Written Statement
Biography

Ms. Terry C. Vickers Benzel, Vice President, Advanced Security Research, Network Associates, Inc.
Written Testimony
Biography

Mr. Robert Weaver, Assistant Special-Agent-in-Charge, New York Field Office, U.S. Secret Service; Head, New York Electronic Crimes Task Force
Written Testimony

Biography

Page 6 PREV PAGE TOP OF DOC

Discussion

Appendix 1: Additional Material for the Record

Letter to Chairman Hollings from the Association for Computing Machinery Regarding Copyright Protection Technologies

CYBER SECURITY—HOW CAN WE PROTECT AMERICAN COMPUTER NETWORKS FROM ATTACK?

WEDNESDAY, OCTOBER 10, 2001

House of Representatives,

Committee on Science,

Washington, DC.

The Committee met, pursuant to call, at 10:20 a.m. in Room 2318 of the Rayburn House Office Building, Hon. Sherwood L. Boehlert (Chairman of the Committee) presiding.

HEARING CHARTER

COMMITTEE ON SCIENCE

U.S. HOUSE OF REPRESENTATIVES

Page 7 PREV PAGE TOP OF DOC

Cyber Security—How Can We Protect

American Computer Networks From Attack?

WEDNESDAY, OCTOBER 10, 2001

10:00 A.M.–12:00 P.M.

2318 RAYBURN HOUSE OFFICE BUILDING

1. Purpose

On Wednesday, October 10, 2001 at 10:00 a.m. the House Committee on Science will hold a hearing to

examine the vulnerability of our Nation's computer infrastructure as well as research-related challenges and opportunities facing the Nation's computer networks.

Testifying before the Committee will be witnesses representing industry, academic, government and non-profit organizations. Witnesses will comment on gaps in research and education in the computer security field. Since most of the information infrastructure in the United States is owned and controlled by the private sector, witnesses will also comment on ways to encourage collaborative approaches to shoring up our ability to predict, prevent, and mitigate attacks.

2. Background

Page 8 PREV PAGE TOP OF DOC

The terrorist attacks of September 11, 2001 brought into stark relief the Nation's physical and economic vulnerability to attack within our borders. The relative ease with which terrorists were able to implement their plans serves as a pointed reminder of the need to identify critical 'soft spots' in the Nation's defenses. Among the Nation's vulnerabilities are our computer and communications networks, on which the country's economic and critical infrastructures for finance, transportation, energy and water distribution, and health and emergency services depend. The existence of these vulnerabilities has called into question the extent to which the Nation's technological research programs, educational system, and interconnected operations are able to meet the challenge of cyber warfare in the 21st century. *The Los Angeles Times* in a recent editorial emphasized the importance of meeting this challenge: "A cyberterrorist attack would not carry the same shock and carnage of September 11. But in this information age. . .one could be more widespread and just as economically destructive."

Vulnerabilities of the National Information Infrastructure

The Internet serves as a powerful mechanism for collaboration and interaction between individuals, regardless of geographic location. The Internet has proven to be a tremendous success—connecting more than 100 million computers and growing—far outstripping its designers' wildest expectations.

The Internet was not originally designed to control power systems, connect massive databases of medical records or connect millions of home appliances or automobiles, yet today it serves these functions. It was not designed to run critical safety systems but it now does that as well. We now heavily rely on an open network of networks, so complex that no one person, group or entity can describe it, model its behavior or predict its reaction to adverse events.

Page 9 PREV PAGE TOP OF DOC

The porous fabric of the Nation's network infrastructure leaves open the constant possibility of cyber attack. Attacks can take several forms, including: defacement of web sites and other electronically stored information in the United States and other countries to spread disinformation and propaganda; distributed denial of service attacks, which use unprotected "zombie" computers anywhere as conduits for wide-scale

distribution of destructive worms and viruses throughout the computer network; and unauthorized intrusions and sabotage of systems and networks belonging to the U.S. and allied countries, potentially resulting in critical infrastructure outages and corruption of vital data.

Along with the increase in network usage come more frequent more frequent security problems. Carnegie Mellon University's CERT® Coordination Center, which serves as a reporting center for Internet security problems, received 1,090 vulnerability reports last year, more than double the number of the previous year. In the first half of 2001, CERT received 1,151 reports with at least 2,000 reports expected by the end of the year. Similarly the number of specific incidents reported to CERT has grown from about 1,300 in 1993 to more than 21,000 in 2000. CERT estimates that this may represent only about 20% of the incidents that actually have occurred.

The recent wide-scale attack by the so-called "Nimda" worm is one example of a technique that modifies web documents and certain executable files found on the systems it infects, and then creates numerous copies of itself under various file names. This followed attacks by "Code Red," "Code Red II," and "SirCam," which affected millions of personal, commercial and government computer users, shut down web sites, slowed Internet service, and disrupted business and government operations, causing billions of dollars of damage.

Page 10 PREV PAGE TOP OF DOC

Interdependence of Critical Infrastructures

The power of the Internet lies not only in its power as a communications tool but also in its ability to link other systems together in ways that vastly improve their productivity and efficiency. Nowhere has this been more evident than in the linking together of our Nation's critical infrastructures.(see footnote 1) Critical infrastructures include electric power, natural gas and petroleum production and distribution, telecommunications (information and communications), transportation, water supply, banking and finance, emergency and government services, agriculture, and other systems and services critical to the security, economic prosperity, and social well being of the Nation. These critical infrastructures are now highly interconnected and mutually dependent in complex ways, both physically and through a host of cyber technologies.

In order to better understand our vulnerabilities to cyber terrorism and understand the potential consequences of cyber attacks, the Internet must no longer be studied solely as separate system but also as one of a network of interdependent critical infrastructures. While some research is being done to better understand the threats to the Internet itself, little has been done to assess and project the dramatic or subtle impact that these threats may have on other critical infrastructures. These problems are not hypothetical. While not the result of a cyber attack, the 1998 failure of the Galaxy 4 communications satellite disrupted the use of 90% of the Nation's pagers and disrupted credit card purchases and ATM transactions. The failure also disrupted the communications of health care providers and emergency workers.

Information Warfare Simulations—"Eligible Receiver"

In 1997, the U.S. conducted an information warfare exercise that illustrated some of the implications of infrastructure interdependence. Known as Eligible Receiver, the scenario depicted a rogue state attempting to attack vulnerable U.S. information systems. A "Red Team" comprised of 35 National Security Agency computer specialists used off-the-shelf technology and software to simulate attacks against power and communications networks in Oahu, Los Angeles, Colorado Springs, St. Louis, Chicago, Detroit, Washington, D.C., Fayetteville, and Tampa. According to the Congressional Research Service, it is generally believed that government (including unclassified military computer networks) and commercial sites were easily attacked and penetrated. Air Force Major General John H. Campbell, U.S. Space Command, commander of the DOD Joint Task Force—Computer Network Defense wrote that the exercise "clearly demonstrated our lack of preparation for a coordinated cyber and physical attack on our critical military and civilian infrastructure." Officials familiar with the exercise later said that Eligible Receiver showed in "real terms how vulnerable the transportation grid, the electricity grid, and others are to an attack by people using conventional equipment."

Underlying Causes of the Nation's Vulnerability to Cyber Attack

There are several underlying reasons for the national information infrastructure's vulnerability. The problems, and therefore the solutions, are not only technical but also involve human factors. Network users too often fail to implement readily available, relatively simple security precautions: installation of up-to-date anti-virus software, use of passwords that cannot be easily stolen, and application of intrusion-detection software. In fact, workplace and user community training in basic security procedures may be the weakest link in the cyber security chain. Even the best technological tools are ineffective if they are not used because they are too difficult to manage or are perceived as overly inconvenient.

However, weaknesses in the current state of research and development in the cyber security arena are also a significant factor contributing to the vulnerability of the Nation's information infrastructure. While a number of information technology companies support R&D on network security, some inadequacies in our security arsenal cannot be addressed solely through short-term industry-based applied research. Instead, industry relies on the fundamental research supported by the Federal Government and the training of future researchers—computer scientists, mathematicians, and many others—that these federally funded research programs support.

Unfortunately, with the possible exception of encryption related research, cyber security research is under-funded and basic research into the fundamental technological cyber security challenges is not robust enough to support the Nation's needs. Many experts believe that as a result of these historic funding patterns there are only 45 to 75 researchers in the country with the experience and expertise needed to conduct cutting edge research in cyber security. To put this in perspective, a computer science department at a single research university may have 60 or more faculty members.

This shortage of personnel is not merely a problem for the academic and research community. Federal agencies are finding it increasingly difficult to recruit and hire professional staff with the knowledge and experience needed to analyze risks and manage and secure their own computer networks. The National Science Foundation, with encouragement from the National Security Council, established in July, 2000 a scholarship for service program designed to increase the number of students becoming part of the Federal Cyber Service of information technology specialists who ensure the protection of the Federal information infrastructure. NASA has requested scholarship for service authority to recruit students with expertise in computer science and other technical fields. Other agencies are pursuing similar authority.

Page 13 PREV PAGE TOP OF DOC

Federal Responses to Possible Cyber Attack

Presidential Decision Directive 63 (PDD–63). On May 22, 1998, President Clinton issued Presidential Decision Directive 63 (PDD–63), which called for a national effort to assure the security of the increasingly vulnerable and interconnected infrastructure of the United States, especially cyber-based infrastructure. These infrastructures include telecommunications, banking and finance, energy, transportation, water systems, and essential government services. The directive required the Federal Government to immediately assess the vulnerabilities of the Nation's computer-based systems and remedy deficiencies, and to produce a detailed plan to protect, critical infrastructures and defend against information warfare. It ordered the Federal Government to serve as a model to the rest of the country for how infrastructure protection is to be attained, and called for joint public-private action to protect critical infrastructures. The directive set 2003 as the target date for full implementation of a "reliable, interconnected, and secure information infrastructure."

While largely relying on individual Federal agencies and departments to oversee internal critical infrastructure improvement, the directive also created a number of new organizations aimed at improving the Nation's ability to prevent, detect, and respond to breaches of information security. Among these are the:

National Coordinator for Security, Critical Infrastructure and Counter Terrorism, which, as part of the White House's National Security Council, oversees national policy development and implementation for critical infrastructure protection.

Page 14 PREV PAGE TOP OF DOC

Critical Infrastructure Assurance Office (CIAO), an interagency office housed at the Department of Commerce that works to integrate assurance plans from each critical infrastructure sector (e.g., energy, telecommunications, finance and banking) into a single national plan, assist agencies in identifying their reliance on critical infrastructures, and coordinate a national education and awareness program.

National Infrastructure Protection Center (NIPC), an interagency office at the FBI that serves as a threat assessment center focusing on threat warnings, vulnerabilities, and law enforcement. The NIPC includes representatives from the FBI, Department of Defense, U.S. Secret Service, intelligence agencies and other government agencies.

Information Sharing and Analysis Centers (ISACs), which serve as mechanisms for gathering, analyzing, and, where appropriate, disseminating information to and from infrastructure centers and the NIPC. The ISACs include industry representatives from sectors such as information and communications, banking and finance, energy, and transportation.

However, despite the development of this strategy, a recent General Accounting Office report concluded that PDD–63 has yet to yield significant progress, in part because of funding constraints and because agencies are not yet aware of the applicability of PDD–63 to their own agency security requirements.

Information sharing between the government, the private sector and academia on critical infrastructure does occur through other means not originally mandated by PDD–63. An important example of public-private partnership in the law enforcement sector is the New York Electronic Crimes Task Force, led by the United States Secret Service. The Task Force includes major stakeholders in the Nation's cyber-infrastructure —industry, academia, law enforcement and government laboratories. According to recent testimony to the House Judiciary Committee, Crime Subcommittee, by Mr. James A. Savage, Jr. of the Secret Service, "[T] he task force provides a productive framework and collaborative crime-fighting environment in which the resources of its participants can be combined to effectively and efficiently make a significant impact on electronic crimes."

Page 15 PREV PAGE TOP OF DOC

Office of Homeland Security. The attacks of September 11 and the heightened expectation of future terror attacks, whether cyber-mediated or more conventional, have elevated concerns of national security to a new level. Reflecting this, on September 20, 2001 President Bush announced the creation of an Office of Homeland Security, a cabinet-level organization now headed by former Pennsylvania Governor Tom Ridge. The office will coordinate 40 Federal agencies and departments and oversee everything from the interaction between the FBI and the CIA in developing and using intelligence to the interaction between governors and state agencies to prepare for potential attacks.

While details of its organizational structure and budgetary authority remain unclear, the President yesterday appointed Richard Clarke, formerly the National Coordinator for Security, Infrastructure, Protection, and Counter-terrorism at the National Security Council, Special Advisor for Cyberspace Security. Dr. Clarke will coordinate interagency efforts to secure information systems and in the event of a disruption, coordinate efforts to restore critical systems. Dr. Clarke will also serve as chairman of a government-wide board that will coordinate the protection of critical information systems. The President is expected to sign an Executive Order soon establishing the board.

The creation of a Homeland Security Office had been recommended by a blue-ribbon panel chartered by Congress and co-chaired by former Senators Gary Hart and Warren Rudman, which reported its recommendations just over two years ago. The panel, which had been asked to examine national security threats in the post-Cold War world, recommended that a "Homeland Security Agency" be formed with broad powers that would coordinate the efforts of existing agencies such as the Federal Emergency Management Agency, Customs Service, Border Patrol and Coast Guard. The panel identified cyber security threats as serious and called current efforts to prevent attacks and generate a prompt response to any future attacks

"uneven at best."

Page 16 PREV PAGE TOP OF DOC

Another panel, the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, or the "Gilmore Commission," was chartered in 1998 by the FY 99 National Defense Authorization Act (P.L. 105–261) and is expected to release its latest report on anti-terrorism, part of which is expected to address cyber security issues.

Federal Cyber Security Research Efforts

Office of Science and Technology Policy. PDD–63 made the White House's Office of Science and Technology Policy, through the National Science and Technology Council, responsible for developing research and development efforts related to national security. Eight Federal R&D priorities were subsequently identified:

Establishment of an Institute for Information Infrastructure Protection;

Education and training of research personnel;

Interdependency analysis;

Threat, vulnerability, and risk assessment studies;

System protection and information assurance;

Reconstitution of damaged or compromised systems;

Page 17 PREV PAGE TOP OF DOC

Security of automated infrastructure control systems; and intrusion detection and monitoring.

Federal Agencies and Departments. Federal R&D efforts to enhance cyber security cut across many agencies and tend to give emphasis to traditional agency missions. For example, the *National Science Foundation* (NSF) supports research on technical issues that underlie the design, validation, and evolution of software-based systems, and recently announced a new program, "Trusted Computing," that will provide grants for research aimed at building a scientific foundation and technological basis for managing information security and privacy. NSF also funds research into cryptography, which is based in mathematics and is a key mechanism for ensuring the security of electronic transmissions. In addition, NSF's Scholarship for Service program recently awarded grants to six universities in order to help train more computer security and information assurance professionals.

The *National Institute of Standards and Technology* (NIST) within the Department of Commerce provides grants to fund research to develop commercial solutions to IT security problems central to critical

infrastructure protection. NIST recently announced the award of a number of grants under the Critical Infrastructure Protection Grants Program aimed at accelerating efforts to make the computer and telecommunications systems that support essential services more secure.

In addition, through its national laboratories, the *Department of Energy* has supported projects that have developed information security tools for network inspection and workstation protection, and the *National Aeronautics and Space Administration* develops advanced methods for the specification, design, and verification of complex software systems used in critical aerospace applications.

Page 18 PREV PAGE TOP OF DOC

The *Department of Defense* funds a significant amount of information technology R&D, including cyber security-related research. The *Defense Advanced Research Projects Agency* (DARPA) alone funds more than 100 individual research projects in this area. The *National Security Agency* funds the bulk of the Nation's critical infrastructure protection programs and has "accredited" 23 Academic Centers of Excellence in universities around the country that have developed advanced computer and network security curricula at the graduate and post-graduate level (see Appendix 1 for a list of these universities). The value of these designations is not primarily financial but organizational. In order to earn the accreditation, an institution must develop a program that is multidisciplinary and that fully integrates research, education, and training.

On a broader scale, the Interagency Working Group on Information Technology Research and Development formed the Networking and Information Technology Research and Development (NITRD) program (see Appendix 2), which includes 15 agencies dedicated to advanced IT R&D. The multi-agency approach is intended to leverage the expertise and perspectives of scientists and technology users from agencies, Federal laboratories, universities, and corporations who are working on a broad range of IT research questions.

3. Witnesses

The following witnesses will address the Subcommittee:

William A. Wulf, President, National Academy of Engineering and Vice Chair of the National Research Council, the principal operating arm of the National Academies of Sciences and Engineering. He is on leave from the University of Virginia, Charlottesville, where he is AT&T Professor of Engineering and Applied Sciences and a nationally recognized expert in computer architecture and network security.

Page 19 PREV PAGE TOP OF DOC

Dr. Eugene Spafford, Professor of Computer Sciences, Professor of Philosophy, and Director of the Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue University, where he is also the interim Information Systems Security Officer.

Ms. Terry A. Benzel, Vice President of Advanced Security Research for Network Associates, Inc. As Director of the Network Associate labs, she is responsible for leading a staff of 100 researchers performing

leading-edge research on perceived security issues two-to-five years in the future.

Mr. Robert Weaver, Assistant Special-Agent-in-Charge, New York Field Office, United States Secret Service; Head, New York Electronic Crimes Task Force. The New York Electronic Crimes Task Force is a Secret Service led, 250-member task force with representatives from 45 law enforcement agencies, prosecutors, academe, and 200 experts from the business world in the areas of cyber security and related fields.

4. Questions

Panelists will be asked to discuss the following questions in their testimony:

1. What are the current and potential threats to cyber security and how equipped are we to address them?

Page 20 PREV PAGE TOP OF DOC

2. How can industry, academia, and Federal and State governments work more effectively to improve network security? What are the barriers to effective cooperation and are their successful models in which these barriers are being overcome?

3. What technological challenges in computer/network security can be addressed through short-term efforts to "push" to the market innovations that are already in the R&D pipeline? What investments must be made over the long-term to ensure the future security and stability of computer networks?

4. What is the current state of information security education and training? Is there a sufficient number of well trained researchers and professionals to meet both academic and industry personnel needs?

APPENDICES

Appendix 1

The 23 universities designated as NSA Centers of Academic Excellence in Information Assurance Education are:

Carnegie Mellon University

Drexel University

Florida State University

Page 21 PREV PAGE TOP OF DOC

George Mason University

Georgia Institute of Technology

Idaho State University

Information Resources Management College of the National Defense University

Iowa State University

James Madison University

Mississippi State University

Naval Postgraduate School

Norwich University

Purdue University

Stanford University

Syracuse University

Page 22 PREV PAGE TOP OF DOC

University of California at Davis

University of Idaho

University of Illinois at Urbana-Champaigne

University of Maryland, Baltimore County

University of North Carolina, Charlotte

University of Tulsa

U.S. Military Academy, West Point

West Virginia University

Appendix 2

NITRD Agencies

National Science Foundation
National Institute of Standards and Technology
National Oceanic and Atmospheric Administration
Department of Energy
DOE National Nuclear Security Administration

National Aeronautics and Space Administration
National Institutes of Health
Environmental Protection Agency
National Security Agency
Department of Defense
General Services Administration
Agency for Healthcare Research & Quality
Bureau of Labor Statistics
Defense Advanced Research Projects Agency
Executive Office of the President

75565a.eps

75565b.eps

Chairman **BOEHLERT.** What is happening, or more appropriately, what is not happening. The Democratic conference is meeting right now to determine a leadership position. As many of you probably know, the current whip has announced his intention to run for Governor and has resigned his position as whip, I think, effective 1 January. So in a spirited contest, they are now determining who will be the replacement for Mr. Bonior.

In view of that, we are waiting for our Democratic colleagues to join us before commencing the hearing. And we quite frankly have no idea, with any certainty, just how long it will be. But is a very important part of the process and so we are just going to defer launching the hearing until some of our Democratic colleagues are free from that conference. So that explains where we are. And then once they arrive, we will get going and we will be all set.

And for our expert witnesses, I appreciate so much your being a resource for the Committee and your outstanding testimony. If you would like, we have a lounge. We can get you a cup of coffee or anything you would like. We want to make it comfortable for you. Mr. Weaver, it is good to see you, friend. So we will start as soon as we are able to do so under the circumstances. Thank you very much.

The hearing will come to order. And let me restate the situation. The Democrats are meeting in caucus now to determine a leadership position and it is obviously very important business. They did not anticipate it going beyond ten o'clock, but obviously it has. I could make a cheap joke by saying, you know how Democratic elections are. There are only two candidates, so I wouldn't think there would have to be a run-off, but maybe there will be.

In any event, in deference to the schedules of our distinguished witnesses, we have the okay from the minority side to proceed with the hearing, which we will do. So let me say at the outset that I—we have the testimony. All the members of the Committee have been given the testimony of all of the witnesses, and I

am sure they will do what I did, look at it very carefully. But there is no substitute for having the real live bodies before us with an opportunity to have a good interchange. And we expect a good interchange here.

Let me say it is a pleasure to welcome everyone here today to discuss the fascinating and, often times, troubling issue of computer security. The events of September 11 have made all Americans more conscious of security issues. Our job in Congress is to ensure that we are focusing adequate attention and resources on security matters while, at the same time, preserving the openness that is the hallmark of American society. It is not an easy balance to achieve, and we need to guard against the worst kind of failures, those that will leave us more encumbered, but no more secure.

Page 25 PREV PAGE TOP OF DOC

In talking to experts on matters within this Committee's jurisdiction, the security issue that came up repeatedly was computer security. It is easy to state the problem in general terms. American society has become vastly more dependent on computers and the Internet in recent years, making us more vulnerable to criminal or terrorist attacks on our computer networks. Yet, research and development on computer security have not kept pace with the growing significance of the threat.

But laying out the problem is far easier than figuring out what to do about it. So today, we will hear from a variety of experts who will guide us as we decide what legislative and other steps are needed to increase the focus on computer security, in terms of R&D, risk assessment, and implementation.

For starters, it is clear that we have to devote greater resources, not only money, but also our individual and collective attention, to computer, and especially network security. To put it simply, we need more people to do more creative thinking about computer security. That is what our adversaries are doing.

I am pleased that the President has taken some initial steps in this direction by appointing Dr. Richard Clark as a Special Advisor for Computer Security. I anticipate working with Dr. Clark and with my good friend, Governor Tom Ridge, on these issues, and also with Dr. Jack Marburger, whose confirmation hearing I testified at yesterday. We will never have the coordinated, focused Federal effort on computer security that we need without clear, firm, and continuing guidance from the White House. We now have some key players in place to help develop that clear, firm, and continuing guidance.

Page 26 PREV PAGE TOP OF DOC

We will also be providing continuing guidance of our own. We expect to have another hearing on computer security next week, and intend to follow up with a legislative proposal. In addition, the Committee will hold a hearing later this month examining security issues regarding our Nation's physical infrastructure, including water supplies.

And, of course, our Committee is hardly alone in focusing on this issue. I want to especially note the work of our Committee Member, Lamar Smith, who has held three hearings on cyber crime in his Judiciary Subcommittee this year.

The purpose of our hearings is not to gain attention or to spread frightening scenarios, which, by their very nature, are virtually limitless. We want to focus on real, concrete problems and develop specific solutions. I am optimistic that this hearing will help us do just that.

As I introduce today's distinguished witnesses, I want to extend a special welcome to Special Agent Bob Weaver of the Secret Service. Bob and his team on the New York Electronic Crimes Task Force were located at Seven World Trade Center and they were directly touched by the tragic events of September 11. Thankfully, all the Task Force members have been accounted for and are safe. Welcome, Bob, in so many, many ways, right from the heart, and thanks for being here.

The Task Force has been at the forefront of the effort to combat all forms of electronic crime, especially the financial networks that support terrorism. I am proud to note that the National Institute of Justice's Cyber Science Laboratory at Rome, New York, in my District, is a key partner with the Task Force. The laboratory has been working with the Task Force in the days since September 11 to get things up and running again, to help track down the financial assets of terrorists.

Page 27 PREV PAGE TOP OF DOC

Until the tragic events of September 11 intervened, New York Governor Pataki had been planning a National Cyber Crime, Cyberterrorism Summit, which was to have taken place in the financial district next week. That summit is being rescheduled for early next year, but I can't let this go by without applauding the foresight and leadership of Governor Pataki, and I look forward to working with him and participating in that very important summit.

Our other witnesses this morning are among the Nation's leaders in computer science, and what a pleasure it is to welcome each of them here. With that, I now am privileged to turn the Chair over to the distinguished Ranking Member from Texas, Mr. Hall.

[The prepared statement of Mr. Boehlert follows:]

PREPARED STATEMENT OF CHAIRMAN SHERWOOD BOEHLERT

It's a pleasure to welcome everyone here today to discuss the fascinating and troubling issue of computer security.

The events of September 11th have made all Americans more conscious of security issues. Our job in Congress is to ensure that we are focusing adequate attention and resources on security matters while at the same time preserving the openness that is the hallmark of American society. It's not an easy balance to achieve, and we need to guard against the worst kinds of failures—those that will leave us more encumbered but no more secure.

In talking to experts on matters within this Committee's jurisdiction, the security issue that came up repeatedly was computer security. It's easy to state the problem in general terms: American society has become vastly more dependent on computers and the Internet in recent years, making us more vulnerable to

criminal or terrorist attacks on our computer networks. Yet research and development on computer security have not kept pace with the growing significance of the threat.

Page 28 PREV PAGE TOP OF DOC

But laying out the problem is easier than figuring out what to do about it. So today we'll hear from a variety of experts who will guide us as we decide what legislative and other steps are needed to increase the focus on computer security, in terms of R&D, risk assessment and implementation.

For starters, it's clear that we have to devote greater resources—not only money, but also our individual and collective attention—to computer and especially network security.

To put it simply, we need more people to do be doing more creative thinking about computer security. That's what our adversaries are doing.

I'm pleased that the President has taken some initial steps in this direction by appointing Dr. Richard Clarke as a Special Advisor for Cyber Security. I anticipate working with Dr. Clarke and with my good friend Governor Tom Ridge on these issues, and also with Dr. Jack Marburger, whose confirmation hearing I testified at yesterday. We will never have the coordinated, focused federal effort on computer security that we need without clear, firm and continuing guidance from the White House.

We will also be providing continuing guidance of our own. We expect to have another hearing on computer security next week, and intend to follow up with legislation. In addition, the Committee will hold a hearing later this month examining security issues regarding our nation's physical infrastructure, including water supplies.

Page 29 PREV PAGE TOP OF DOC

And, of course, our Committee is hardly alone in focusing on this issue. I want to especially note the work of our Committee member Lamar Smith, who has held three hearings on cybercrime in his Judiciary subcommittee this year.

The purpose of our hearings is not to gain attention or to spread frightening scenarios—which, by their very nature, are virtually limitless. We want to focus on real, concrete problems and develop specific solutions. I'm optimistic that this hearing will help us do just that.

As I introduce today's distinguished witnesses, I want to extend a special welcome to Special Agent Bob Weaver of the Secret Service.

Bob and his team on the New York Electronic Crimes Task Force were located at 7 World Trade Center and was directly touched by the tragic events of Sept. 11. Thankfully, all Task Force members have been accounted for and are safe. Welcome Bob—thanks for being here.

The Task Force has been at the forefront of the effort to combat all forms of electronic crime, especially the financial networks that support terrorism. I'm proud to note that the National Institute of Justice's

CyberScience Laboratory at Rome, New York in my district is a key partner in the Task Force. The Laboratory has been working with the Task Force in the days since September 11 to get things up and running again, to help track down the financial assets of terrorists.

Until the tragic events of September 11 intervened, New York Governor Pataki had been planning a National Cybercrime—Cyberterrorism Summit, which was to have taken place in the financial district next week. The summit is being rescheduled for early next year and I applaud the foresight and leadership of Governor Pataki and look forward to participating.

Page 30 PREV PAGE TOP OF DOC

Our other witnesses this morning are among the nation's leaders in computer science.

Mr. **HALL.** Mr. Chairman, thank you very much. And because of the lateness of the day and very few Democrats here—we have been in a whip race over across the way—I won't read my opening statement, and if I read it, I would be reading it for the first time. So I will just very briefly say how pleased I am to join you today in welcoming our witnesses and congratulate you on calling this hearing on security of cyber space.

And I have a lot of thoughts about it. I am very confident in the leadership we have in this country and I am confident in the scientific input that we will have at the top level. And I think that we need to know that we have been fortunate so far in avoiding a cyber attack. Richard Clark, the President's new cyber terrorism czar said that the government has to make cyber security a priority or face a digital Pearl Harbor, and we don't want that.

I know that we need to look at every source that could attack us and to know that those who attacked us will—use the cheapest route to attack us. When they attacked September the 11th they used our airplanes, our people, our fuel. They didn't put 15 cents into it, and probably didn't even pay for their tickets when they finally went through. We just have to look at them from every angle. And I think it is good to have this hearing and I certainly support this thrust. And I thank the Chairman and those on your staff and on my staff that have brought us to this stage. I yield back my time, but I would like to have my 22-page speech put in the record.

[The prepared statement of Mr. Hall follows:]

Page 31 PREV PAGE TOP OF DOC

PREPARED STATEMENT OF REPRESENTATIVE RALPH M. HALL

Mr. Chairman, I am pleased to join you today in welcoming our witnesses, and I congratulate you on calling this hearing on the security of cyber space. It goes without saying that national security is on everyone's mind. As we work to improve our country's security, it is important to look at systems that are vital to the functioning of the Nation. A good starting point would be systems that can be attacked anonymously and from far away using computer networks. Examples of systems that rely on computer

networks include the electric power grid, rail networks, and financial transaction networks.

We are all aware of the growing number of Internet security incidents, involving such things as computer viruses, denial of service attacks, and defaced web sites. These events have disrupted business and government activities, and have sometimes resulted in significant recovery costs. While we have been fortunate so far in avoiding a catastrophic cyber attack, Richard Clarke, the President's new cyber terrorism czar, has said that the government must make cyber security a priority or face a "digital Pearl Harbor".

The Science Committee has an important role in addressing this challenge. First, we need to consider how to strengthen the security of federal information systems. The National Institute of Standards and Technology has an important role to play here. It is responsible for developing security standards and best security practices. It should assist agencies in training their computer security personnel and help assess their security weaknesses.

Unfortunately, NIST has never requested or received the resources it needs to effectively carry out its statutory role in these areas. The Science Committee has developed bipartisan legislation over the past three congresses to correct this problem. Mr. Chairman, I encourage you to dust off this legislation. I would be glad to work with you to pass it into law during this Congress.

Page 32 PREV PAGE TOP OF DOC

Another important area for the Committee to consider is how to make improvements in information security for the long-term. I believe a key to this is a vigorous and creative basic research effort focused on the security of networked information systems. Unfortunately, that is not the current state of research in this field.

I share the views of Dr. Wulf and Dr. Spafford, two of our witnesses this morning, on the inadequacy of the scale of current research programs and the lack of a critical mass of researchers in this field. I will be interested in hearing the views of our witnesses on how we might proceed to build up our research capabilities. I also would welcome our panelist comments and suggestions on how to ensure that new discoveries coming from research find their way into security products and applications.

I appreciate the attendance of our witnesses, and I look forward to our discussion.

Chairman **BOEHLERT.** And I can assure that 22-page speech will be read very carefully by every member of this distinguished Committee. We will move right on to our distinguished witnesses. And without objection, all members will be allowed to insert opening statements at this point.

[The prepared statement of Congresswoman Constance Morella follows:]

PREPARED STATEMENT OF CONGRESSWOMAN CONSTANCE MORELLA

Page 33 PREV PAGE TOP OF DOC

Securing our Nation's computer networks is now more important than ever:

As we prepare as a nation to face a new world of potential threats to our security, our well-being, and our way of life, we must redouble our efforts to protect our Nation's vital computer networks, among which so many of us depend for our commerce, productivity, and personal communication.

The "weakest link" threatens all:

The interconnectedness of global computer and communications networks necessitates a well-thought out, global strategy that involves governments, businesses, academics, and consumers.

Piece-meal or partial efforts will not suffice in today's networked environment.

Cyber security is a constant and evolving process.

Effective cyber security measures require a cognizance of what we don't know as much as what we do know.

The nature of potential cyber threats and attacks can change on a day-to-day basis.

Cyber security means acknowledging and being prepared for the threats that exist today as well as being cognizant of the fact that we don't know what threats may exist tomorrow.

Page 34 PREV PAGE TOP OF DOC

Advanced security research and development is now more critical than ever:

With this process in mind, advanced security research and development becomes even more critical if we are to stay current in what it takes to protect our Nation's information infrastructure. Only by investing into new security tools capable of discerning and combating new security threats will our networks be adequately protected today and in the future.

Tackling network security will require a significant "joint venture":

We must generously fund advanced security research and development and seek out innovative partnerships therein among government, industry, and academia. No one sector has all the answers—we are all in this together.

We are joined today by top experts in this field:

I would like to acknowledge, in particular, Ms. Terri Benzel, Vice President of Advanced Security Research of Network Associates, Inc. Network Associates is one of the world's leading developers of network security and availability solutions.

Their PGP security business unit is located in my district of Montgomery County, Maryland.

Ms. Benzel is one of the Nation's leading experts on advanced security research and I know that her

testimony will be extremely useful to us today.

Page 35 PREV PAGE TOP OF DOC

[The prepared statement of Congressman J. Randy Forbes follows:]

PREPARED STATEMENT OF CONGRESSMAN J. RANDY FORBES

Thank you, Mr. Chairman and Ranking Member, Mr. Hall, for holding this important hearing today and assembling this panel of experts to discuss the threats to America's cyber infrastructure.

As America focuses on how we can better protect against terrorist attacks on our Nation and our way of life, the news is full of reports about weapons of mass destruction—whether weapons by design or by invention, such as transcontinental aircraft; biological weapons; and chemical weapons. Without a doubt, all of these threats are very real and deserve our serious attention.

Cyber attacks, though they won't bring the death and destruction of these other threats, are just as real. They hold the power to disrupt our way of life, harm people's personal interests, and cause tremendous losses for businesses. Regrettably, they also may be the area in which we are most vulnerable.

Computers, unlike aircraft, dangerous chemicals, weapons, and biological toxins, can be found in the possession of individual citizens. These people may depend upon their home computers to balance their checkbooks and connect them to friends by e-mail, but they are not conversant in the signs of cyber crime and terrorist attacks. It is imperative, therefore, that whatever mechanisms our scientists develop to guard against these threats be understandable to the layman, as well as to the experts in business and government.

Page 36 PREV PAGE TOP OF DOC

I appreciate our witnesses taking the time to join us today, and I look forward to working with my colleagues on this panel to improve our research and development efforts in this important area of study.

[The prepared statement of Congresswoman Zoe Lofgren follows:]

PREPARED STATEMENT OF CONGRESSWOMAN ZOE LOFGREN

Chairman Boehlert and Ranking Member Hall, thank you for having this hearing today.

I am pleased to welcome one of the panelists, Terry Benzel, vice president for Advanced Security Research for Network Associates, Inc. of Santa Clara, California. This company, whose employees I know well, has a very strong track record in manufacturing software and implementing research to curb information security breaches. Welcome, Terry.

I look forward to hearing your testimony and the testimony from each panel member.

The challenge before us is to develop a more secure system to prevent cyber terrorism. We know that the Internet and information infrastructure are susceptible to man-made havoc. Hackers and other mischief-makers have released the "Love Virus," clogged the Internet and manipulated websites to spread misinformation.

Page 37 PREV PAGE TOP OF DOC

We also know that the information infrastructure was never designed to thwart user access. In fact, the first systems were set up to share information with a maximum amount of users. Unfortunately, information systems security has too often been applied as a band-aid, rather than an integral system part. We should have devoted more attention to this deficiency from the very beginning.

There are many positive steps that can be taken to increase cyber security. Some are as simple as installing or updating anti-virus software on our home computers. Others are more systemic such as increasing research and development for this neglected information discipline as well as broadening our knowledge base by encouraging more people to become information security experts.

[The prepared statement of Congresswoman Sheila Jackson Lee follows:]

PREPARED STATEMENT OF CONGRESSWOMAN SHEILA JACKSON LEE

Thank you, Mr. Chairman and Ranking Member Hall, for holding this important hearing on *Cyber Security: How Can We Protect American Computer Networks From Attack?* We are fortunate to have a distinguished panel of witnesses who have given their time to speak about ways to protect this Nation from cyber attacks.

Mr. Chairman, in the wake of the horrible terrorist attacks on our country that took place on September 11, 2001, it would be very easy for us to focus all of their attention on the types of attacks we saw on that day, and on what needs to be done to prevent their reoccurrence. That is, of course, an extremely important issue, and it is crucial that we take steps such as improving aviation security to prevent similar attacks in the future. But it is also vitally important that we pay attention to the other types of threats to our Nation's security that are just as significant, and just as likely, today as they were before September 11. Among those threats are potential cyber attacks against our information infrastructure.

Page 38 PREV PAGE TOP OF DOC

Federal facilities, electric power plants and other portions of the nation's critical infrastructure are highly vulnerable to cyber attacks from terrorist groups, rogue nations, disgruntled employees and hackers from across this country. This hearing today provides us an opportunity to discuss the vulnerability of our computer infrastructure and to discuss an approach to prepare our Nation to defend against such attacks.

The information revolution has surpassed the expectations of the some of the brightest minds, enabling so many to reap the benefits of a booming economy. The question today, however, if not to restate our mutual commitment to the development of computer technology and information. Rather, we are here to discuss the

cumbersome challenges that cyber attacks have compelled all American to consider.

The recent cyber attacks designed to disrupt major web networks represents a serious weakness in security. It exposes how the vulnerabilities at one place on the Net can create risks for all. These recent cyber attacks demonstrate the need for us to work together to develop a strategy to strengthen cyber security.

All Americans have a vested interest in balancing the policing of cyber crimes with the protection of civil liberties and a speech on the Internet. Finding the right balance is crucial.

Yet as devastating as computer crimes can be, in combating them we must remember to preserve the same rights as provided to traditional criminal defendants. As a member of the House Committee on the Judiciary, I am always concerned about the protection of individual rights of all Americans. The Constitution has always been a flexible document, written to accommodate changes in society, and so we must act accordingly.

Page 39 PREV PAGE TOP OF DOC

Last year we held a hearing on the series of well-planned and coordinated cyber attacks on several of the nation's biggest Internet sites. Two popular sites, Yahoo.com and Buy.com, were shut down for several hours, while sites such as CNN.com, ZDNet.com, Amazon.com, eBay.com, and E*Trade were similarly terrorized. These cyber attacks effected millions of Internet users and resulted in revenue losses for several sites. While this damage was relatively minimal in proportion to volume of the Internet, these events were a wake-up call to many of us as to the extent of cyber crime, and the degree to which we are all vulnerable.

The world of electronic communications is a developing one. Clearly, there is a growing need for enforcement, and in many instances, strengthening of our laws so that our law enforcement professionals can do their jobs and keep us all safe from cyber criminals.

Having said this, we must also recognize the need to heed the warnings from the examples of deprivations of civil liberties that are more and more abundant as the Internet continues to grow, and law enforcement struggles to keep up.

In a recent case in the state of Texas, which I represent, law enforcement, acting on a tip from a local business, confiscated all of its competitor's business computers based on the accusation that the competitor engaged in electronic "spamming." As a result, the accused business, against which charges were eventually dropped, lost months of business while incurring legal and other costs to get its equipment back.

To balance enforcement with protections, there must be a concerted effort to coordinate law enforcement between Federal, state and local entities. We must provide them with the equipment and training to enable them to keep up with the criminals who are operating in the cyber environment. In the process, we must protect the rights of Americans to free political, commercial, and other speech over the Internet.

Page 40 PREV PAGE TOP OF DOC

To this end we have many challenges. We need a balanced international strategy for combating cyber crime. We need round-the-clock Federal, state and local law enforcement officials with expertise in, and responsibility for, investigating and prosecuting cyber crime. We need new and more expansive procedural tools to allow state authorities to more easily gather evidence located outside their jurisdictions, and need to assess whether we have adequate tools at the federal level to effectively investigate cyber crime. Finally, we need to work in partnership with industry to address cyber crime and security, where we can discuss challenges and develop effective solutions that do not pose a threat to individual privacy.

It is the role of government to protect all of these forms of speech, as well as interstate commerce that over the Internet. Consequently, we must send a clear message to those who would attempt to interfere with the free speech and mobility of citizens and industry through the Internet—Americans take this very seriously. Cyber criminals will be dealt with along with other criminals.

I look forward to your comments.

Chairman **BOEHLERT.** But I think we should go right to the Panel because you are the resources. You have been waiting a half hour and we are anxious to hear from you and learn from you and to question you and to have good dialogue.

Our Panel consists of William A. Wulf, President, National Academy of Engineering and Vice Chair of the National Research Council, the principal operating arm of the National Academies of Science and Engineering. He is on leave from the University of Virginia, Charlottesville, where he is the AT&T Professor of Engineering and Applied Sciences and a nationally recognized expert in computer architecture and network security.

Page 41 PREV PAGE TOP OF DOC

We have Dr. Eugene Spafford, Professor of Computer Sciences, Professor of Philosophy, and Director of the Center for Education and Research in Information Assurance and Security at Purdue University, where he is also the Interim Information Systems Security Officer, and that is a challenge and a half.

Ms. Terry Benzel, Vice President of Advance Security Research for Network Associates, Incorporated. As Director of the Network Associates Labs, she is responsible for leading a staff of 100 researchers performing leading-edge research on perceived security issues two to five years in the future.

Finally, Robert Weaver, Assistant Special Agent in Charge, U.S. Secret Service, Special Agent, Director, New York Electronic Crimes Task Force. The New York Electronic Crimes Task Force is a Secret-Service led, 250-member task force, with representatives from 45 law enforcement agencies, prosecutors, academe, and 200 experts from the business world in the areas of cyber security and related fields.

All of you, your entire statements will be put in the record, and we would ask that you try to summarize. Because of the importance of what we are about, we are not going to strictly adhere to the 5-minute rule, but I would appreciate your trying to come as close to that as possible, so that we will have ample time for questions. And, as you can see, there is a great deal of interest in this important subject. And so we are here to learn from you and we will start. Dr. Wulf, you are first.

STATEMENT OF DR. WILLIAM A. WULF, Ph.D., PRESIDENT, NATIONAL ACADEMY OF ENGINEERING; VICE CHAIR, THE NATIONAL RESEARCH COUNCIL; AT&T PROFESSOR OF ENGINEERING AND APPLIED SCIENCE, UNIVERSITY OF VIRGINIA

Page 42 PREV PAGE TOP OF DOC

Dr. **WULF.** Thank you, Mr. Chairman. I deeply appreciate the opportunity to be here. There are lots of risks. The news media seems to be in the business of trying to scare us. I rebel at doing that, so I am not going to talk about the kinds of risks that face us in concrete terms.

I would note, however, that three years ago the Presidential Commission on Critical Infrastructure Protection, which had been charged to look at the Nation's vulnerabilities on all of its infrastructures, physical infrastructures, pipelines, but also financial systems and so on, decided that they would focus exclusively on our vulnerabilities in cyber space because that was so overriding that—and affected our ability to protect all of the other infrastructures.

I am worried about a deep problem. That problem is that our research base in computer security and network security is minuscule. There is a very tiny, very conservative group of researchers in universities developing any kind of long-term response to the sorts of threats we are talking about.

The National Academies are, at the moment, mobilizing researchers from the biological community, from the chemical community, and so on, to look at the threats faced by the country. I was terribly struck by the fact that there is almost no one for me to draw on in the cyber security area, by comparison to the tens of thousands of biologists, for example. There are, perhaps, a hundred or two people who work on these kinds of problems.

Let me say a word or two about my background and why I am concerned—why that leads me to be as deeply concerned about this issue as I am. I taught for 13 years in the computer science department at Carnegie Mellon and then I spun out a company and ran that for 10 years. And then I spent a couple of years as an Assistant Director of the National Science Foundation before going back to the computer science department at the University of Virginia.

Page 43 PREV PAGE TOP OF DOC

After I had been there a while, one of my students came to me and said that she would like to do some research in computer security. I had done computer security research previously at Cargenie Mellon, but while I was running my company and at NSF, I had not. So after about 15 years, I came back to a subject that I had previously studied. And, frankly, I was simply appalled. Very, very little progress had been made in that intervening 15 years. The basic model that people were using was the same one that had been developed in the 1960's, a model that, I think, is profoundly flawed, and I detail that in my testimony, and I will say a few more words about it in just a moment.

So I started to ask myself why was that the case? Why—the problems in computer security are absolutely

fascinating ones. Intellectually, they are fascinating problems. Why was it that there was such a small community and so little progress? And my analysis is that there has never been a funding agency that believed that it was its responsibility to develop the community of scholars researching this area. There is a little bit of funding from NSF. There is a little bit of funding from DOD. You can get bits and pieces here and there. But quite unlike every other field, there is no single agency which believes that this is its responsibility.

As a consequence, because the resources are so scarce, the community gets very conservative. In a context in which there isn't a guarantee of long-term funding, proposals don't think out of the box. They make small incremental additions to what is already known. Out-of-the-box thinking in an environment of scarce resources doesn't get funded. It seems to me that we need to think in terms of a response to this situation which encourages out-of-the-box thinking. It very explicitly encourages out-of-the-box thinking.

Page 44 PREV PAGE TOP OF DOC

I said earlier that the basic model on which most contemporary computer research is based is flawed. I call it the maginot line model. It is a perimeter defense model. I am sure you have heard the word firewall used in the context of computer and network security. It is a notion that there is bad stuff out there and good stuff in here and we want to protect what is in here against the bad guys out there. That model doesn't work.

First of all, it is fragile. If anybody does penetrate the perimeter, as the Germans did in France, you can run absolutely amuck. There is nothing which is protected. Second, many of the flaws that have been discovered in computer systems are designed in. That is, they are not errors. They are not mistakes that somebody made.

In a report released by the Naval Research Laboratory several years ago, some 50 security violations were analyzed. Twenty-two of those were the result of properties specified as correct behavior of the system. Now, I am not saying that that is the right ratio. The particular incidents studied were not selected to be a perfectly random sample. So I don't know if that is anything close to the right ratio. But the point is, it is not the case that all—get it out of your mind that somehow security flaws are the result of mistakes. That is not always the case.

Third, the maginot line doesn't protect against insiders, and some of the greatest vulnerability are against insiders. It is not always necessary to penetrate a system. I am sure you—many of you have heard of so-called distributed denial of service attacks. There was a military exercise a few years ago, four years ago Spaff tells me, called Eligible Receiver, in which a small group of hackers essentially shut down a major joint exercise between the Army, the Navy, and the Air Force, largely by using relatively unsophisticated denial of service attacks.

Page 45 PREV PAGE TOP OF DOC

And, finally, the maginot line has never worked. We have not, in the roughly 40 years that we have thought about computer security, built a secure system. Every one of them has been penetrated.

I think we need to think, therefore, out-of-the-box in a number of different ways. For one thing, I think that any kind of centralized system is not going to work. We have got to think about distributed security.

We need to think about active defense. Everything we have done so far is passive. We have tried to protect something from being attacked. You are going to have to think, I think, in terms of ways of hitting back.

And, finally, computer security research is only very loosely tied to the legal system. We need to think very deeply. And, in fact, there are impediments in the current legal system to fostering good computer security.

I have tried to think also about what is the appropriate response in the current situation. I think we desperately need to do something. First and foremost, unfortunately, we need money. Academics always seem to sit on this side of the table and ask for more money for research, but I think this is really different. And, first and foremost, I don't think it is an issue of a lot of money. What it is, is a guarantee of some kind of long-term money. Academics will not enter a research area if they can't expect to have a career in that area.

I think we need to respond fairly quickly, and so we need an agile mechanism. I have trouble mapping what I think of as the requirements for the response on to any of the existing funding agencies, as much as I love all of them. And I think, therefore, we may need to think about a different approach. Thank you.

Page 46 PREV PAGE TOP OF DOC

[The prepared statement of Dr. Wulf follows:]

PREPARED STATEMENT OF WILLIAM A. WULF

Cyber Security: Beyond the Maginot Line

Good morning, Mr. Chairman and Members of the Committee. I am Wm. A. Wulf, President of the National Academy of Engineering and AT&T Professor of Engineering and Applied Science in the Department of Computer Science at the University of Virginia. I appreciate the opportunity to testify today on cyber security.

A few words about my background will provide a context for my remarks. I was a professor at Carnegie Mellon University (CMU) for 13 years (from 1968 to 1980); and during that time computer security was one of the areas of my research. I left CMU in 1980 to found and run a software company and subsequently served as an Assistant Director of the National Science Foundation (NSF). In 1991, I returned to academia at the University of Virginia, where after a time I resumed my research on computer security. The gap of more than 15 years between my first and second exposures to the state of the art in computer security gave me a different perspective than I would have had if I had stayed in the field.

In a report by the National Research Council,(see footnote 2) a committee of experts concluded that the immediate vulnerabilities of government computer systems could be ameliorated by rigorous

implementation of industrial "best practices." I agree with that assessment.

Page 47 PREV PAGE TOP OF DOC

I am troubled, however, by a deeper problem. We have virtually no research base on which to build truly secure systems and only a *tiny* cadre of academic, long-term, basic researchers who are thinking deeply about these problems. The immediate problems of cyber systems can be patched by implementing "best practices," but not the *fundamental* problems. Well funded, long-term basic research on computer security is crucial to our national security.

For historical reasons, no federal funding agency has assumed responsibility for supporting basic research in this area—not the Defense Advanced Research Projects Agency (DARPA), not the NSF, not the Department of Energy (DOE), not the National Security Agency (NSA). Because no funding agency feels it "owns" this problem, relatively small, sporadic research projects have been funded, but no one has questioned the underlying assumptions on cyber security that were established in the 1960s mainframe environment.

In my view, the little research that is being done is focused on answering the wrong question! When funds are scarce, researchers become very conservative, and bold challenges to the conventional wisdom are not likely to pass peer review. As a result, incrementalism has become the norm. Unfortunately, in this context, the right answer to the wrong question is worse than useless because it leads to counterproductive efforts and a false sense of security.

I should point out that researchers in this area might disagree with my assessment of the problem. As I said, the research community in this area is very small and very conservative—and some will surely not like my implicit challenge to their life's work. However, I believe it is imperative that we reassess our approach to this urgent problem.

Page 48 PREV PAGE TOP OF DOC

My analysis can be broken down into four areas:

1. The need for a new "model" of the threat to replace the "Maginot Line" model.

2. The need for a new definition of cyber security.

3. The need for "active defense."

4. The need for coordination with the legal and regulatory systems.

The Maginot Line Model

Most research on cyber security is based on the assumption that the "thing" we need to protect is "inside" the system. Therefore, we have tried to develop "firewalls" and other mechanisms to keep outside attackers

from penetrating our defenses and gaining access or taking control of it. This model of computer security—I call it the Maginot Line model—has been used since the first mainframe operating systems were built in the 1960s. Unfortunately, it is dangerously flawed.

First, like the Maginot Line, it is fragile. In WWII, France fell in 35 days because of its reliance on this model. No matter how formidable the defenses, the attacker can make an end run around them, and once inside, the entire system is compromised. The Maginot Line model is especially inappropriate in a networked environment, which does not have an "inside" or "outside" defined by the hardware. Many attempts have been made to simulate a networked environment, especially through various cryptographic techniques, but so far none of these has worked.

Page 49 PREV PAGE TOP OF DOC

Second, the Maginot Line model fails to recognize that many security flaws are "designed in." In other words, a system may fail by performing *exactly* as specified. Flaws are not always "bugs" or errors—they can also result when a system behaves as designed, but in ways the designers did not anticipate. In 1993, the Naval Research Laboratory did an analysis of some 50 security flaws and found that nearly half of them (22) were part of the requirements or specifications. It is impossible to defend or provide a firewall against security flaws that were conceived of as perfectly legitimate—that were, in fact, considered *requirements* of correct system behavior!

In the 1990s, I did research on cryptographic protocols—very short pieces (10 to 20 lines) of code that use cryptographic techniques to perform certain functions, such as establishing the identity of participants in a network transaction. These protocols are the principal techniques of creating software simulations of networked systems based on the "inside" vs. "outside" paradigm of the Maginot Line model. Even when these protocols have been mathematically proven to be correct, they can be, and have been, compromised by the clever manipulation of a feature critical to its "correct" operation. If we cannot recognize the flawed specification of a 10-line program, it is highly unlikely we will be able to recognize flaws of a program with millions of lines of code.

Third, the Maginot Line cannot protect against insider attacks. No one has ever compromised the CIA by mounting a frontal assault on its external fence in Virginia. But security breaches have been made by employees inside the fence. The analogy to computer systems is clear. If we only direct our defenses outward, we ignore our greatest vulnerability, the legitimate insider.

Page 50 PREV PAGE TOP OF DOC

Fourth, one need not "penetrate" a system to do major damage. This was demonstrated by the distributed denial-of-service attacks on Yahoo and others last year, which showed that expected behavior can be disrupted or prevented without any form of penetration. Simply by flooding a system with false requests for service, it became impossible to respond to legitimate requests. We can be grateful that so far these denial-of-service attacks have been against Internet sites and not against 911 services in major cities.

Finally, the Maginot Line model has never *worked!* Every system built to protect a Maginot Line-type system has been compromised—including the systems I built in the 1970s. After 40 years of trying to develop a foolproof system, it's time we realized that we are not likely to succeed. It's time to change the flawed inside-outside model of security.

This is not the place to espouse alternatives, but I'll mention a few just to show that alternatives exist. DARPA has a program to investigate models based on biological immune responses. Other models could distribute the responsibility for defining and enforcing security to every object in the system so that the compromise of one object would be just that—a compromise of one object and not a compromise of the whole system. The point is that there are much more robust models on which we might build the architecture of a secure cyber space.

Definition of Security

The military definition of security emphasizes protecting access to sensitive information. This is the basis of the compartmentalized, layered (confidential, secret, top secret) classification of information. The slightly broader definition of security used in the research community includes two other notions: integrity and denial of service.

Page 51 PREV PAGE TOP OF DOC

Integrity implies that information in the system cannot be modified by an attacker. In some cases, medical records for instance, integrity is much more important than secrecy. We may not *like* other people seeing our medical records, but we may die if someone alters our allergy profile.

Denial of service is just what it says—the attacker does not necessarily access or modify information in a system but does deny its users a service provided by that system. In the case of logistical operations, for instance, the ability to flood a communication channel with traffic can cripple an operation. Several years ago, for example, the Joint Chiefs of Staff asked a small team to see whether they could disrupt a major multi-service military exercise called Eligible Receiver. In fact the team caused the exercise to be canceled, in part by using denial of service techniques. This relatively unsophisticated form of attack could also be used against phone systems (military base exchanges, 911, etc.), financial systems, and, of course, Internet hosts.

A *practical* definition of security must be more complex than privacy, integrity, and denial of service. A proper definition will differ for each kind of object—credit card medical record, tank, aircraft flight plan, student examination, and so forth. The notion of restricting access to a credit card to individuals with, say, *secret* clearance is nonsensical. Other factors, such as the timing, or at least the temporal order, of operations, correlative operations on related objects, and so on, are essential to the security of real-world information. (An example often cited is that the best way to anticipate major U.S. military operations is to count the pizza deliveries to the Pentagon.)

Page 52 PREV PAGE TOP OF DOC

The military concept of sensitive but unclassified information has a counterpart *in spades* in the cyber world. Indeed, the line between sensitive and nonsensitive information is often blurred in cyber space. In principle, one must consider how *any* piece of information might be combined with innumerable other pieces of information and used in some way to compromise our interests. The vast amount of information available on the Internet and the speed of modern computers make it impossible to anticipate how information will be combined or what inferences will be drawn from such combinations.

A simple model of "penetration" does not reflect *any* of these dimensions of realistic security concerns. Hence, an analysis of the vulnerability of a system in terms of how it can be "attacked" in terms of the inside-outside Maginot Line model—is unlikely to reveal its true vulnerabilities.

Active Defense

Based on my experience over the past 30 years, passive defense alone will not work, especially if one holds to the Maginot Line model. Effective cyber security must include some kind of active response, some threat, some cost higher than the attacker is willing to pay, to complement passive defense. Our current computer security is primarily passive (although there are a few laws against crimes using a computer).

Our ability to identify and respond to an attack, in the cyber world *or* the physical world, can be improved substantially, but these approaches are not being aggressively pursued. Much better models of passive defense are possible—especially models like the immune system response that distribute the responsibility for protection and defense rather than concentrating it at the Maginot Line.

Page 53 PREV PAGE TOP OF DOC

Developing an active defense will not be easy. The practical and legal implications of active defense have not been determined, and the opportunities for mistakes are legion. The international implications are especially troublesome. It is difficult, sometimes impossible, to pinpoint the physical location of an attacker. If the attacker is in another country, could a countermeasure by a U.S. government computer be considered an act of war? Resolving this issue and related issues will require a thoughtful approach and careful international diplomacy. Precisely because these issues have not been thought about in depth, we desperately need long-term basic scholarship in this area.

Coordination with the Legal and Regulatory System

Any plan of action must begin with a dialogue on legal issues. I am not a legal expert, but there are two kinds of issues I think should be addressed soon: (1) issues raised in cyber space that do not have counterparts in the physical world; and (2) issues raised by place-based assumptions in current law. The first category includes everything from new forms of intellectual property (databases, for example) to new forms of crime (spamming, for example). Issues of particular interest to this discussion are right(s) and limitation (s) on active countermeasures to intrusions (indeed, what constitutes an intrusion). Issues raised by place-based assumptions in current law include many basic questions. How does the concept of jurisdiction apply in cyber space? For tax purposes (sales taxes in the United States and value-added taxes in Europe), where does a cyber space transaction take place? Where do you draw the line between national security and law enforcement? How do you apply the principle of *posse comitatis?*

Page 54 PREV PAGE TOP OF DOC

Not all of these issues are immediately and obviously related to cyber space protection. But cyber space protection is a "wedge" issue that can force us to rethink some fundamental questions about the role of government, the relationship between the public and private sectors, the balance between privacy and public safety, and the definition of security.

Addressing the Problem

In 1998, the Presidential Commission on Critical Infrastructure Protection released a report focused on vulnerabilities to cyber attack in the military, law enforcement, commerce, indeed virtually every aspect of life in the United States. I was hopeful that the report would lead to the creation of a serious, long-term research program. Unfortunately, it hasn't.

In our typical fashion, research since then has focused on solving short-term problems. NSA, for example, has recently established a number of (unfunded) centers of excellence and earmarked an institute for information infrastructure protection at Dartmouth. All of these are focused on near-term problems.

Although industrial best practices will plug the most obvious holes in any computing system, in the long run we must develop a conceptual foundation that includes a strong research base and a cadre of committed researchers to address these issues. This will require that a single agency, with enough resources to fund a long-term, stable research program, be assigned responsibility for coordinating the development of a fundamental science base and a community of researchers.

Page 55 PREV PAGE TOP OF DOC

As a former Assistant Director of NSF, I have been both the source and the target of requests for research funds. I hope my remarks today will not be interpreted as "more of the same." I believe the United States is extremely vulnerable to cyber terrorism. Unlike the situation in the 1940s when the country was attacked, we have no pool of scientists and engineers today to fill the breach. We must do everything we can to create that pool as quickly as possible—and, unfortunately, it may not be quickly enough.

I believe that ensuring stable, long-term funding, at whatever level will be most effective, is the most important change we can make immediately. Academics build their careers by establishing their reputations among their colleagues over a long period of time. Attracting the brightest minds to this critical field will require reasonable assurances that they can continue to work in the field.

Thank you for the opportunity to testify on this critical matter.

Chairman **BOEHLERT.** Thank you very much, Dr. Wulf. Dr. Spafford.

STATEMENT OF DR. EUGENE H. SPAFFORD, PROFESSOR OF COMPUTER SCIENCE, PROFESSOR OF PHILOSOPHY, AND DIRECTOR OF PURDUE UNIVERSITY'S CENTER FOR EDUCATION AND RESEARCH IN INFORMATION AND ASSURANCE AND SECURITY (CERIAS); INTERIM INFORMATION SECURITY OFFICER, PURDUE UNIVERSITY

Dr. **SPAFFORD.** Thank you, Chairman Boehlert, and, Ranking Member Hall, for the opportunity to testify at this very important hearing. I would like to thank all of you for turning your attention to the vital issues that are involved in this area, not only for the current threat, but for the long-term health and safety of the Nation. These are issues that are not going to be solved immediately and they are not going to go away. They are part of a long-term series of concerns that need to be addressed.

Page 56 PREV PAGE TOP OF DOC

I am going to focus my testimony on the important role that university researchers bring to information security and assurance, and, in particular, to some of the challenges that we have been facing that hopefully you can help us address.

As the Chairman noted, I am a Professor of Computer Sciences at Purdue University and the Director for the Center for Education and Research and Information Assurance and Security. CERIAS, as we call it, is the largest academic research center in the country, possibly the world, devoted to areas of information assurance and security. We also have a very active affiliate program with other universities that don't have quite the resources and faculty that we do, or that have other specialized talents and educational resources. So we are also working with universities in Illinois, Iowa, North Carolina, the District of Columbia, Ohio, Virginia, and New York State. So we have an ongoing program to try and bring other educators into the fold.

Despite that background, my statement today really is to represent the USACM, which is the Association for Computing Machinery's Committee on U.S. Public Policy. For those of you who are not familiar with ACM, it is a nonprofit educational and scientific computing society of about 75,000 members who are committed to open interchange of information concerning computing and related disciplines.

My statement also has been approved by the Computing Research Association. This is an association of more than 180 North American academic departments of computer science and computer engineering, industry and academic laboratories, and affiliated professional societies.

Page 57 PREV PAGE TOP OF DOC

The USACM and the CRA believe it is important to present a strong and unified message to Congress that investing in computer security education and research is vital to securing the information infrastructure of our Nation. We cannot hope to manage our security needs without a sustained commitment to the conduct of research, both basic and applied, and to the development of new experts.

So in the remainder of my remarks, I am going to briefly mention challenges in five critical areas that we have identified affecting current university research. An expanded version of these remarks has been submitted as the written testimony. And through my comments and through reading my written remarks, you may gain some insight as to why the academic community has not been better able to address some of the concerns that Dr. Wulf mentioned in his testimony.

The first area is that of support. I conducted a survey of my peers at leading institutions over the last week

to find out what some of the factors are affecting their work, and the common consensus is there is not enough long-term support for their research. In recent years, cost-cutting measures have driven many Federal funding agencies to focus almost exclusively on short-term research instead of basic research. This is particularly true of defense-related agencies.

Thus, instead of finding new ways for us to design systems that are resistant to attack or that can recover from attack, we find most of our research being directed at how to apply new patches to the same old, buggy systems. Instead of finding new ways to build the infrastructure in a safe manner, we are finding ways to correct the same old mistakes that continue to be made.

Page 58 PREV PAGE TOP OF DOC

Experience has also shown that industry is concerned with information security, certainly, and is willing to provide some funding for our research in this area, but it is usually tied to short-term deliverables and often has restrictions on publications of results, primarily because of information proprietary concerns. And, as a result, our faculty have not been particularly interested in pursuing funding of that nature because it hinders their ability to progress in academia.

Neither of the approaches that are currently put forth by government or industry serve to fix long-term problems, nor do they help build the capacity of our educational institutions to do further research and to build up more experts.

The second area is infrastructure. Few institutions have the resources necessary to continuously support and evolve the infrastructure needed for current research, especially when they are already stretched to provide resources to surging needs in the general computer science population.

The Federal Government has no ongoing programs to support the range of needs at recognized centers of excellence. This limits the nature and scope of the research we can undertake and the number of students we can support. In some cases, there is a real concern that some of the research centers pieced together over the last few years may wither away from a lack of support to update themselves. We have built up a fair amount of momentum and are afraid of losing it.

The third area of concern is in real-world data. The nature of much of the research being undertaken in information security is such that it requires considerable real-time data for analysis and validation. Unfortunately, we are often unable to see that data. Companies and government agencies are unwilling, or unable, by statute, to provide access because they consider the data sensitive or proprietary. They are especially uninterested in us using it in research that would be published, which, again, hurts our research agenda. It is not possible to construct valid models or solutions unless we can properly analyze the actual problems and have access to real large-scale systems.

Page 59 PREV PAGE TOP OF DOC

Third, personnel. Currently, there is a large unmet need for computer scientists and computer engineers.

Information security specialists are an even scarcer commodity. The situation is especially acute when it comes to qualified faculty. There are only a few dozen faculty in the United States who have significant background in security research and they are graduating only a few Ph.D.s per year to add to their ranks.

Based on figures I have collected over the last week, I surveyed 24 of the largest and best-known graduate programs in the country who work in information security. They report that they have graduated a total of 23 Ph.D.s in security over the last three years. That is all. And only a fraction of those have decided to go into academic positions to help increase the supply. This isn't enough to keep up our current rate of production, let alone create new centers or departments.

And then, last of all, I want to mention legal impediments. In recent years, owners and creators of intellectual property have sought greater protections for that property. Unfortunately, the evolution of law has led to unintended consequences for those of us working in security. I have had several reported instances where research into new and novel forms of information security have had to be curtailed or stopped because the researchers have been threatened by the patent holders. University faculty do not have the resources to fight such threats, whether they are justified or not. Therefore, those avenues of research have been abandoned.

More recently, provisions of the Digital Millennium Copyright Act have led to faculty being threatened with lawsuits for publishing their security research, and some faculty, myself included, have had to stop our research in security forensics because of the potential for us to be arrested or sued because of our research. This affects people such as Mr. Weaver, who would like to use our tools, perhaps, in investigating computer crime. We are no longer able to do that research.

Page 60 PREV PAGE TOP OF DOC

Legislation that is scheduled to be introduced into the Senate, the Security Systems Standards and Certification Act, may further restrict what research is conducted and what software we are able to use.

On behalf of the USACM and the CRA, I would like to point out that legislation against the technology hurts us in other ways. The legislation should be against the behavior, particularly the infringing behavior, and we urge you to consider this as future legislation is considered.

Finally, I would like to say that the USACM and the CRA will be delighted to help you in any way we can by providing our expertise in science and research in addressing these very formidable challenges. And I thank you for the time.

[The prepared statement of Dr. Spafford follows:]

PREPARED STATEMENT OF EUGENE H. SPAFFORD

Thank you Chairman Boehlert for the opportunity to testify at this timely and important hearing. I want to commend you, the Science Committee members, and your staff for turning the attention of Congress to the vital issue of securing our nation's information infrastructure. My testimony focuses on the important role of university research in information security, and in particular on some of the challenges research faculty face.

By way of introduction, I am a professor of Computer Sciences at Purdue University, a professor of Philosophy, and the Director of the Center for Education and Research in Information Assurance and Security. CERIAS is a campus-wide multidisciplinary Center, with a mission to explore important issues related to protecting information and information resources. We conduct research, educate students at every level, and have an active community outreach program. CERIAS is the largest such center in the United States, and we have a series of affiliate university programs working with us in Illinois, Iowa, North Carolina, the District of Columbia, Ohio, and New York State. In addition to my role as an academic faculty member, I also serve on several commercial boards of advisors, including those of Tripwire, Guardent, and Open Channel Software; and I act as an advisor to Federal law enforcement and defense agencies, including the FBI, the Air Force and the NSA.

Page 61 PREV PAGE TOP OF DOC

My statement today represents the USACM, the Association for Computing Machinery's Committee on U. S. Public Policy. ACM is a non-profit educational and scientific computing society of about 75,000 computer scientists, educators, and other computer professionals committed to the open interchange of information concerning computing and related disciplines. USACM, of which I serve as the Co-chair, acts as the focal point for ACM's interaction with the U.S. Congress and government organizations. USACM seeks to educate and assist policy-makers on legislative and regulatory matters of concern to the computing community.

To underscore the significance of today's hearing, my statement has also been approved by the Computing Research Association—an association of more than 180 North American academic departments of computer science and computer engineering, industry and academic laboratories, and affiliated professional societies. The CRA is particularly interested in issues that affect the conduct of computing research in the USA.

The USACM and CRA believe it is important to present a strong and unified message to Congress that investing in computer security education and research is vital to securing the information infrastructure of our Nation. I know you are aware of the continuing, substantial growth in malicious software, system attacks, and cyber crime and I will not speak to those numbers. I will note that the figures available to me show growth rates of more than doubling each year in the number of incidents, and current estimates of losses in the tens of billions of dollars per year.

We cannot hope to protect our information infrastructure without a sustained commitment to the conduct of research—both basic and applied—and the development of new experts. The incredible growth of our society's deployment of computing has too often been conducted with concerns for speed or lowest cost rather than with concern for issues of safety, security, and reliability. Security cannot be easily or adequately added on after-the-fact and this greatly complicates our overall mission. The software and hardware being deployed today has been designed by individuals with little or no security training, using unsafe methods, and then poorly tested. This is being added to the fault-ridden infrastructure already in place and operated by personnel with insufficient awareness of the risks. Therefore, none of us should be surprised if we continue to see a rise in break-ins, defacements, and viruses in the years to come.

Page 62 PREV PAGE TOP OF DOC

There are a great many problems that need to be addressed to help secure our infrastructure. Some of these problems have known solutions that are infrequently applied—perhaps because of cost or availability. Other problems will require long-term basic research and development of new technologies. Some of these solutions are potentially within easy reach of current scientists performing short-term research, while others will require training at least a new generation of research scientists with sound foundations in information assurance.

I use the term "information assurance" here because those of us working in the field have learned that the issues are really larger than simply computer security. Information assurance covers issues of building safe and reliable information systems that are able to weather untoward events no matter what the cause—whether natural disaster or caused by a malicious individual. Whether critical data in a financial institution or defense agency is affected by a hardware failure, a power outage, a computer virus or a hacker doesn't matter in at least one sense: unless the system is resistant to the damage and built for assured operation, the data is gone. We seek to protect those data and systems from a wide range of threats.

I would also like to clarify a point that is not always obvious: information security is not cryptography. Cryptography is simply one component branch of information security, in the same way that carpentry and plumbing are components in building a house. Information assurance also involves issues of physical security, malicious software, privacy, authentication technologies, software engineering, database security, network security, computer forensics, intrusion detection, and a number of other fields.

Another point that I should make is in response to a myth that is often repeated, namely that industry will find incentives to solve our security problems. To the contrary, it is largely because of industry practices that we currently face such security problems! Industry is concerned with getting products to market as quickly as possible, at the lowest cost. The result is often software with extraneous, poorly designed and poorly tested features. To spend extra time or money on better security is to put the companies at a disadvantage in the marketplace. Instead, many software companies have disclaimed all liability in their licenses, and sought to insulate themselves from adverse reactions and scrutiny of their software via laws such as the UCITA (at the state level), and the DMCA (at the Federal level). In the current market that does not offer consumers significant choices, and where there is no liability for faulty products, there is little likelihood that industry players will invest in fundamental research to improve products.

Page 63 PREV PAGE TOP OF DOC

In the remainder of my remarks, I will briefly discuss issues in five aspects of current university operations as being of the highest concern to those of us conducting research and advanced education in information security. Those areas are: support for research, development of infrastructure, access to real-world data, personnel shortages, and legal impediments.

Support

For research to be conducted, investigators need financial support. The support is needed to hire graduate student assistants, purchase hardware and software, travel to conferences, subscribe to necessary journals, and other expenses. There are two general sources for funding of the sort needed by information assurance researchers in academia: from industrial sources, and from the government.

Experience by my peers has shown that many companies are concerned with information security and are willing to provide some funding to research in this area. However, this funding is generally quite limited, both in quantity and in the number of researchers supported. Furthermore, this funding is almost always tied to short-term deliverables and with restrictions on publication of results. A common practice within industry is to terminate university-based projects after delivery of prototypes—evaluation and validation of design is not always supported, and may actually be damaging to marketing plans. The results of this kind of support may be of short-term value for a few students and the companies involved, but it does little to advance to state of the art. Funding from corporate America that has fewer "strings attached" is more difficult to come by, and is particularly susceptible to fluctuations in the overall economy, as has happened recently. As such, few researchers depend on corporate support for their work.

Page 64 PREV PAGE TOP OF DOC

Funding from government is the major source of support for most academic faculty. Traditional sources of this funding are the National Science Foundation, NIST, DARPA, the military labs, the Department of Energy, national laboratories, and the National Security Agency. Each of these agencies funds some research, often under specific and narrowly defined initiatives. However, my colleagues have indicated that they have found that few (if any) of these sources have provided long-term, on-going funding for information assurance research. Several of my colleagues have reported that they have begun to gain understanding of a fundamental problem after several years of research, only to find that the program under which they did their work was discontinued and no further funding was available. Others report an inability to find any funding to try new and novel approaches, especially if those approaches require multiple years of funding for an involved, systems-based investigation.

Similar to industry support, much of the Federal funding that is available is focused on near-term, deployable results. In some cases, this research produces no new publishable results, and is thus of little academic benefit to the faculty or students involved. Of more concern, in recent years cost-cutting measures have driven funding agencies (particularly Department of Defense agencies) to focus more on short-term research than on basic research; instead of finding ways to design new systems resistant to attack, we thus find most of the research being directed to how to apply newer patches to the same old buggy code. This does not serve to fix the long-term problems, nor does it serve to help build the capacity of educational institutions to do further research.

Most of the funding reported by my colleagues seems to be from within a larger program at the indicated agencies. I have heard from a number of frustrated faculty colleagues that their applications for information security research were competing for limited dollars against proposals for research in delivery of multimedia, improved computer science education, and new WWW applications, Only a few information security-specific programs have been available in recent years, and these have generally been underfunded.

For example, NIST announced allocation of $5 million in research awards under their 2001 Critical Infrastructure Grants program. They received 133 submissions and were only able to fund nine, and the continuation of the program in fiscal year 2002 has been zeroed out in the Senate. This means some projects begun under this year's program won't be funded to completion. This is typical of many of the programs established to fund security. Instead of cutting this program, serious thought should be given to expanding it. The new NSF program in Trusted Computing that has recently been announced also shows promise as an important mechanism to fund research in this area.

A survey of my colleagues at 23 major universities (see the Appendix) reveals that with the exception of two universities with large project grants, the information security faculty at these institutions are averaging $105,000 per year per faculty member. This is enough to support some modest equipment, travel and a few graduate students. It is not enough to fund long-term projects to advance the state of the art.

Let me also note that it is extremely frustrating for researchers to see competitive, merit-based programs reduced or eliminated at the same time directed funding is being provided to institutions without any clear history of excellence in the area or capacity to use that funding. Such actions can actually serve to be destructive in the community rather than constructive.

Infrastructure

To perform relevant research and education requires that we have an up-to-date infrastructure. This includes modern hardware and software, adequate space to house that equipment, and personnel to configure and maintain it. However, because of the nature of the field and the speed of its evolution, few institutions have the resources necessary to continuously support and evolve the infrastructure needed for current infosec research, especially when they are already stretched to provide resources to surging needs in general computer science.

Most of the programs in information security in the USA have strong ties to computer science and computer engineering departments. The surge in undergraduate enrollments in many of these programs mean that those departments are critically short of space for offices, laboratories, and academic needs. Many of these universities are public institutions with limited funds, and thus there is little hope for new space in the coming years. Information security, as a relatively new (and underfunded) specialty has little priority for what little space is available. Those of us in the community regularly exchange stories about how we have commandeered storage closets and regularly violate fire codes to house our equipment and students.

Industry has not been forthcoming about providing significant contributions of current products to more than a few select programs without tying such support to onerous intellectual property agreements. Often, donations are made without support included, and without needed options, thus creating an additional burden on cash-strapped programs (few grants allow inclusion of support costs). And the Federal Government has no on-going programs to support the range of needs at recognized centers of excellence.

This significant lack of infrastructure limits the nature and scope of the research we can undertake, and the number of students we can support. In some cases, there is a real concern that some of the research centers pieced together over the last few years may wither from lack of support to update themselves.

Real-world Data

The nature of much of the research being undertaken in information security is such that it requires considerable real-world data for analysis and validation. Unfortunately, we are often unable to see that data. Companies and government agencies are unwilling or unable to provide access because they consider the data sensitive or proprietary. (Note: I have heard from personnel in companies and government agencies that they often won't even share with each other!) It is not possible to construct valid models or solutions unless we can properly analyze the actual problems.

Page 67 PREV PAGE TOP OF DOC

Consider, for instance, the problem of correlating data to identify attacks in wide-scale networks. To properly test theories, identify data markers, and validate designs, researchers need millions of audit records representing "normal" and "abnormal" traffic patterns; artificially-generated records cannot be used because we have not yet been able to construct valid models. Then, after the data has been analyzed, we need to instrument and test a real network. There are serious concerns about doing this data collection and testing on a real network because of the potential for adverse effects. Yet, no experimental testbed of this size and complexity exists for researchers to use. There are many other examples that can be cited, in different subfields of information security.

Personnel

Currently, there is a large unmet need for computer scientists and computer engineers in the USA. Information security specialists are an even scarcer commodity. The situation is especially acute when it comes to qualified faculty: there are only a few dozen faculty in the U.S. who have significant background in security research, and they are graduating only a few Ph.D.s per year to add to the ranks. The 23 institutions reported in the Appendix graduated a total of 20 Ph.D.s in security in the last three years—an average of less than seven per year. These are some of the largest and best-known programs in the country in information security! Of those graduates, only a fraction have been interested in faculty positions. This results in intense competition for the few new faculty available, new programs cannot get started with domain-experienced faculty, and few existing programs are able to grow in this area.

Page 68 PREV PAGE TOP OF DOC

Based on figures I obtained from the 23 universities, it appears that the active programs in the area average 3 or 4 CS faculty working in security at each institution. Many of them report that their time is often spent teaching basic, non-security CS courses to support their departments, so they are not able to devote their full attention to security research or teaching. It is also the case that there are not enough good students applying for the best graduate programs, for a variety of reasons. Without sufficient numbers of students or faculty, our ability to conduct research is severely limited.

The National Science Foundation's Scholarship for Service program, and NIST's Computer Science Fellowship program are both examples of programs to help build personnel. However, they only address a very small portion of the need, and neither addresses the critical shortage of Ph.D.s in the field.

Legal Impediments

As more content has been developed for use with computers and networks, there has been a greater concern for protecting intellectual property. Content owners have stridently lobbied for greater and greater protections for their on-line property. Unfortunately, the evolution of the law has led to unintended consequences for those of us working in security. In particular, I know of several instances where research into novel forms of information security has been curtailed because patent holders have threatened researchers. University faculty members do not have the resources to fight such threats.

More recently, provisions of the Digital Millennium Copyright Act (DMCA) have led to faculty being threatened with lawsuits for publishing their security research, and some faculty (myself included) have had to curtail or stop our research in security forensics because of the potential for us to be arrested or sued. Legislation that is scheduled to be introduced into the Senate, the Security Systems Standards and Certification Act (SSSCA), may further restrict what research is conducted in information security. Legislation against technology instead of against infringing behavior can only hurt our progress in securing the infrastructure.

Page 69 PREV PAGE TOP OF DOC

I will be happy to expand on any of these points, now or in the future.

Thank you again for the opportunity to testify.

Appendix—Information Sources

Academic colleagues at the following institutions contributed comments and data for this testimony. This testimony is more complete for their contribution, but is not in any way suggested as representing their individual views.

Florida State University
George Mason University (VA)
George Washington University (DC)
Georgetown University (DC)
Georgia Institute of Technology
Iowa State University
Mississippi State University
Naval Postgraduate School (CA)
North Carolina State University
Purdue University (IN)
Syracuse University (NY)

University of California, Davis
University of Idaho
University of Maryland, Baltimore County

Page 70 PREV PAGE TOP OF DOC

University of Maryland, College Park
University of Nebraska
University of New Mexico
University of North Carolina-Charlotte
University of Virginia
University of West Virginia
University of Wisconsin-Madison
U.S. Military Academy (West Point, NY)
Yale University (CT)

BIOGRAPHY FOR EUGENE H. SPAFFORD

Eugene H. Spafford is a professor of Computer Sciences at Purdue University, a professor of Philosophy, the university's Information Systems Security Officer, and is Director of the Center for Education Research Information Assurance and Security. CERIAS is a campus-wide multidisciplinary Center, with a broadly-focused mission to explore issues related to protecting information and information resources. Spaf has written extensively about information security, software engineering, and professional ethics. He has published over 100 articles and reports on his research, has written or contributed to over a dozen books, and he serves on the editorial boards of most major infosec-related journals.

Almost every major award and honor in information security has been bestowed on Professor Spafford. He is a Fellow of the ACM, Fellow of the AAAS, Fellow of the IEEE, and is a charter recipient of the Computer Society's Golden Core award. In 2000, he was named as a CISSP, *honoris causa*. He was the year 2000 recipient of the NIST/NCSC National Computer Systems Security Award, generally regarded as the field's most significant honor in information security research. In 2001, he was named as one of the recipients of the "Charles B. Murphy" awards, Purdue University's highest award for outstanding undergraduate teaching. In 2001, he was elected to the ISSA Hall of Fame, and he was awarded the William Hugh Murray medal of the NCISSE for his contributions to research and education in infosec. Among his many activities, he is Co-chair of the ACM's U.S. Public Policy Committee, is a member of the Board of Directors of the Computing Research Association, and is a member of the U.S. Air Force Scientific Advisory Board.

Page 71 PREV PAGE TOP OF DOC

More information may be found at:

<*http://www.cerias.purdue.edu/homes/spaf/narrate.html*>

Chairman **BOEHLERT.** Thank you very much, Dr. Spafford. Ms. Benzel.

STATEMENT OF MS. TERRY C. VICKERS BENZEL, VICE PRESIDENT OF ADVANCED SECURITY RESEARCH, NETWORK ASSOCIATES, INCORPORATED

Ms. **BENZEL.** Chairman Boehlert, Ranking Member Hall, and, members of the Committee, thank you for inviting me to testify today on the role and importance of research and development in the protection of our Nation's computer networks from cyber attacks. My name is Terry Vickers Benzel and I am the Vice President of Research for Network Associates.

For those of you who may not be familiar with Network Associates, you probably know us by our leading brand names, McAfee Anti-Virus software, Sniffer Technologies, PGP Security, and Magic Solutions. Within Network Associates I further serve as the Director of NAI Labs.

And NAI Labs is an industry-leading, multi-disciplined research organization with over 100 researchers addressing the issue of information security. We do this through largely government-sponsored research grants from DARPA, NSA, NIST, Army, Air Force, Navy, and other DOD agencies, as well as several commercial vendors.

Page 72 PREV PAGE TOP OF DOC

We are in a somewhat unique position and are pleased to be here today because we do government research and have been involved in long-term research under government sponsorship while, at the same time, we find ourselves as part of a leading vendor of information security technology.

In addition to my work with Network Associates, I am also here today to share with you my perspective in working with two collaborative partnerships. That is, the Security Research Alliance and the Partnership for Critical Infrastructure Security.

In 1999, Network Associates spearheaded the formation of the Security Research Alliance. The Research Alliance is a true alliance of the research laboratories of major vendors, including Cisco, Sun, Lucent, Entrust, and BBN Technologies.

The Partnership for Critical Infrastructure Security is a leading industry/government research organization in response to PDD-63. Within the PCIS, I co-chair the R&D Working Group.

Now, let me turn my attention to some of the questions before the Committee. I have prepared a detailed written testimony that I have provided for the record. Today, I will briefly summarize some key points and I will confine my remarks first to the first three questions and leave discussion of education and training to my colleagues from academia.

What are some of the current potential threats to cyber security? When we look at threats to computer systems and networks, as part of our critical infrastructures, that is, energy, financial services, transportation, communication, and information services, and vital human services, the threats are extensive and serious. These systems are extremely vulnerable. A cyber threat taken in conjunction with a physical threat of

terrorism, as we have witnessed, is beyond frightening.

Page 73 PREV PAGE TOP OF DOC

For example, if we were to look at an issue of a cyber attack on the control systems of a water purification plant, at the same time as a biochemical attack on the water itself, then we would have no way of understanding and knowing the threats which would exist there. In this context, that is, the context of traditional information security, along with physical threats, I believe it is evident we don't really know how vulnerable we are.

These are serious challenges which are going to require Federal funding and new changes in our policies and our ways of thinking. Critical infrastructure vulnerabilities need to be assessed. First and foremost, we need to perform an in-depth vulnerability analysis of our cyber threats in the critical infrastructure arena. In fact, it is good to note that some of the remarks that have been made to Governor Ridge relative to the new Homeland Office of Security is that he, too, needs to look at performing a thorough threat analysis and vulnerability assessment in the broad picture.

We need to have a more complete understanding of the threats and vulnerabilities so that we can construct an R&D map. It is difficult for us to be able to point to what are the correct R&D gaps that exist without fully understanding the context and the background in which we need to perform this research.

Nonetheless, through the work we have done in the Partnership for Critical Infrastructure Security and the Security Research Alliance, we have identified three key areas which we believe will be fruitful for investigation, and we urge urgent and quick investment in these areas. They are interdependencies, converged networks, and control systems. And my written testimony provides more in-depth detail on each of those areas.

Page 74 PREV PAGE TOP OF DOC

In order to make progress in these areas, Federal funding and policy changes are required to address the significant challenges. We need to look for new approaches to information sharing. It is difficult to know what is currently being done, what has been done, and what is proposed, in order to construct the new road maps.

We need to share beyond the small community that my colleagues have already mentioned and into cross-sector communities. But as I envision a need for some of the excellent researchers which I believe must exist in operations and research for power plants, nuclear systems, energy, transportation, to work together with the community of researchers in information security, we need to put our heads together to address these problems, cross-sector, cross-government, and cross-academia.

This leads to the question of how we can work more effectively in these different communities. We need to increase our collaboration and partnerships. Over the past few years, there have been some increases in collaboration and partnerships with good results. Having said that, however, let me indicate emphatically, it

is nowhere near enough. Having the small community of the several hundred researchers in computer security talk to each other is not going to address the problems in front of us.

As I said, my written testimony describes some of the work that we are doing in the PCIS, in the Security Research Alliance, and also in the Army Research Labs Collaborative Technologies Alliance. I urge you to look at these as examples of ways we can build new alliances across industry, government, and academia.

Page 75 PREV PAGE TOP OF DOC

It is imperative for all R&D stakeholders to embrace this unprecedented form of new collaboration. We need to have Congress help mandate and fund the incentives to require research alliances and leveraging of other research. All R&D stakeholders should participate in an urgent and ongoing effort to catalog our efforts and how they relate to the critical infrastructure vulnerabilities facing us today.

In summary, I have five recommendations for Congressional action. One, ensure that cyber security is part of homeland security. Two, authorize a study of our Nation's critical infrastructure cyber vulnerabilities. Three, authorize dramatic increases in funds for R&D leading—in leading departments and agencies. Four, reach out to continue coordination among government-funded R&D projects and industry and academia. And, five, develop a new collaborative research mechanism.

Mr. Chairman, the opportunity to have a real impact on the cyber security of our Nation's critical infrastructures is tremendous. This requires a strong commitment to research and development. I urge you to take immediate action, and I pledge my company's support. Thank you for the opportunity to testify. I look forward to answering your questions.

[The prepared statement of Ms. Benzel follows:]

PREPARED STATEMENT OF TERRY C. VICKERS BENZEL

1. Introduction

Chairman Boehlert, Ranking Member Hall and Members of the Committee, thank you for inviting me to testify today on the role and importance of research and development in the protection of our Nation's computer networks from cyber attacks. My name is Terry Benzel, and I am the Vice President of Advanced Security Research at Network Associates, Inc. I am honored to have the opportunity to be here today to discuss the action needed to protect our Nation's computer networks from attack and how this Committee can help advance the research that is required to ensure that effective protection measures can be put in place.

Page 76 PREV PAGE TOP OF DOC

From our Chairman, CEO and President, George Samenuk, and the more than 3,540 employees of Network Associates, I share with you and the American family our thoughts and prayers for all those affected by the tragic events of September 11th. And now, as the American response begins, we extend those thoughts to our men and women serving in the armed forces and to their families at home, including

the employees of our company who have been called to active duty through the military reserve.

With headquarters in Santa Clara, Calif., Network Associates, Inc. is a leading supplier of network security and availability solutions for e-businesses. Our four product lines—McAfee, PGP Security, Sniffer Technologies, and Magic Solutions—deliver a complete range of security solutions, including anti-virus protection, firewalls, intrusion detection, encryption, network and application management.

Network Associates is committed to working with industry and government to ensure the protection of our critical infrastructures, and our employees actively participate in a number of collaborative efforts to share our knowledge with others. In addition, we take part in numerous industry-led activities, including those of such leading associations as the Business Software Alliance (BSA) and the Information Technology Association of America (ITAA).

I am here today to share with you my perspectives on the importance of cyber security research and development to the protection of our infrastructures. Within Network Associates, I serve as the Director of NAI Labs, an industry leading security research and development organization with 120 dedicated staff in four research facilities throughout the United States. We were formally Trusted Information Systems (or TIS), and have been contributing to network and information systems security since 1983. NAI Labs is a multidiscipline research organization with world-renowned expertise in the areas of network security, applied cryptographic technologies, secure execution environments, security infrastructure, adaptive network defenses, distributed systems security, and information assurance. Our research is supported by ongoing projects funded through the U.S. Defense Advanced Research Projects Agency (or DARPA), Air Force, Navy, Army, National Security Agency, and other Department of Defense and government agencies. In addition to our prominent role in the security research community, all unclassified network and information systems research is shared with Network Associates' product development and support organizations in an effort to transfer research results to consumers.

Page 77 PREV PAGE TOP OF DOC

In addition to my work with Network Associates, I come here today to share with you my experience working with two other collaborative organizations: the Security Research Alliance (SRA) and the Partnership for Critical Infrastructure Security (PCIS). Launched in 1999, the SRA is a vendor neutral alliance of industry leaders focussed on bringing security issues to industry at large from a purely research-driven perspective. Network Associates is joined in the SRA by Cisco Systems, Sun Microsystems, Lucent Technologies Bell Labs, BBN Technologies, Entrust Technologies, and GTE Government Systems. The Partnership for Critical Infrastructure Security is a collaborative effort of industry and Government to address risks and assure the delivery of essential services over the Nation's critical infrastructures. I co-chair the PCIS Research and Development Working Group, tasked with identifying an R&D roadmap for critical infrastructure security.

Mr. Chairman, I'd like to commend you and the Members of this Committee for your leadership in holding today's hearing. While the attacks of September 11th were physical in nature, I believe they serve to underscore how important it is to understand the potential impact of a coordinated physical and cyber attack on the delivery of critical services to our citizens, and to help prepare the United States in advance.

The "What-Ifs?" of a physical and cyber attack are many. "What if" the terrorists were also able to impact our communications system, thus hampering the rescue and recovery efforts? "What if" the attackers were able to compromise systems monitoring the water supply for Manhattan? "What if" power to parts of the northeast corridor could have been brought down through a cyber attack on key systems? We must prepare now to prevent this from happening and ensure that technologies, plans and procedures are in place to prevent and respond to any future attack.

Page 78 PREV PAGE TOP OF DOC

As the Nation begins to regain its footing after the attacks on the World Trade Center, the Pentagon, and in Pennsylvania, we are poised to leverage a heightened awareness of our vulnerabilities into ongoing efforts to ensure continuous operation of our national critical infrastructures—Energy, Financial Services, Transportation, Communications & Information Services and Vital Human Services.(see footnote 3)

Stable and continuing operation of these interdependent sectors is vital to maintaining safety, public order, vital human services as well economic stability.

Fundamentally, we are facing the same R&D challenges as before the September attacks—the vulnerabilities both cyber and physical are the same, but our collective awareness of the reality of malicious intent towards the United States has changed, as has awareness of potentially immense consequence of a relatively small act. While concern is warranted and action is critical, it is certainly possible to compound our terror by overstating our vulnerabilities before we have a clear picture of our situation.

Our success will depend on unprecedented cooperation between and among the private, quasi-private and public sector entities and an unrelenting focus on building our polices, assessments, strategies and actions on a powerful, flexible and comprehensive foundation of information security R&D. To understand how best to protect American computer networks from attack, therefore, we must dramatically increase our understanding of what kinds of attack we are vulnerable to, what systems are available and working and, what is missing.

Page 79 PREV PAGE TOP OF DOC

2. How big is this issue and what are the priorities in information security R&D?

2.1 We know that we are vulnerable, but not how vulnerable.

A notable, but often overlooked, gap in our understanding is the extent of our computer network vulnerabilities. We know that we are vulnerable, but not how vulnerable.

Worse yet, by failing to understand the extent of the vulnerabilities and the reality of the interdependencies, we compound our risk—not only are networks vulnerable as such, but critical systems may be accessible through less critical systems and the relatively small vulnerabilities can be exploited to conduct simultaneous electronic and physical attacks. Have we overstated the threat or understated it? We just don't know.

Our R&D proposals will necessarily include developing appropriate assessment strategies and criteria, including identifying areas where good policies have been developed, but are not yet in practice. This understanding can keep us from diverting R&D energy and resources from explorations of crucial outstanding areas. For example, as you have heard in recent GAO testimony on Aviation Security,(see footnote 4) some security breaches result from an incomplete application of existing knowledge—for example, incomplete deployment of existing technology or a lapse in following procedures. In these cases, we don't need to know anything new, we need to do something with what we already know.

Generally, our expertise in information technology and networking has out paced our understanding of its effect on the integrity of our systems and of our understanding of how to prevent, contain or mitigate the damage from malicious cyber attacks and potentially devastating user errors and failures. We will not only need to "catch-up" we will need to "keep-up" with developments in information technology. There is much to explore.

Page 80 PREV PAGE TOP OF DOC

2.2 Much Research, But Too Many Unknowns

There is a broad range of information security R&D being done and being considered to help protect our cyber systems from attack. But there are especially urgent areas for study that we have barely begun to investigate—as a result, we can only guess at the extent of our vulnerability. *Terrorists are motivated to understand and study our vulnerabilities, we should be too.* As we are now painfully aware, there are people in the world who are sufficiently motivated to look for our security vulnerabilities. Are we sufficiently motivated to do the same?

2.2.1 Focus this morning on highest priority types of attacks

This morning, I'd like to focus on what I see as the highest priority targets of attack, and most significant threats. There are many kinds of threats and many kinds of systems at risk, but none are more critical than the computer systems and networks that control our Nation's critical infrastructure (CI). And, as we shall see, most significant threat to these CI systems is cyber terrorism.

To this we need to look both forward and backwards. Look backwards at practices, interdependencies and technologies—we need to know what is being done well, what is failing and what is not being done at all. And look forward at what can be improved and—even more critically—how to develop a shared understanding of assessing the vulnerabilities. To complete the challenge, all of this must be done across and among the five industry sectors with an as yet uncounted number of private, public and quasi-public entities connected in as yet unknown number of networks with a range of practices, interdependencies and technologies.

Page 81 PREV PAGE TOP OF DOC

2.2.2 Not just funding—Congressional leadership is needed

We ask for your help in setting the agenda, dispersing funding and championing an unprecedented kind of collaboration within the CI industry, across sectors and including government agencies of all types. This will require a transformation that is quite like what the intelligence community is currently undergoing—sharing information across decades old—and sometimes centuries old—organizational barriers. For this to be accomplished the leadership needs to come from the very top, just as the pressure for results is coming from your constituencies.

2.3 CI Systems and Cyber Terrorism

CI systems are called critical just because of what happens if they are crippled by cyber attacks, physical attacks or a combination of both.

2.3.1 Attack on CI systems devastating

If CI systems are successfully attacked, people will die, the Nation's economy will be crippled and protective services systems will be weakened—fire, health, police, minimum essential services—all of the systems vital to public safety, domestic order and economic stability.

2.3.2 Critical infrastructure protection and cyber protection are interwoven

Page 82 PREV PAGE TOP OF DOC

We cannot protect ourselves from cyber terrorism without protecting these CI's, just as we cannot protect these CI's without protecting ourselves from Cyber Terrorism.

Always interrelated, the operations of our critical infrastructures are increasingly interdependent and operations within each entity are increasingly dependent on their information technology and they are increasingly connected to one another over private networks and the public Internet.

Because of this vast interconnectedness, we know that the potential damage to our critical infrastructures—in the form of multiple, simultaneous, and cascading disruptions on a regional, national or international scale—is high.

Correspondingly high is the need to assess that potential by engaging in operational research of critical infrastructure provider's technical operations—not only of their control systems, but also of their other technical operations, at least far enough to determine the extent of their interdependence and the security requirements of their interfaces. We also know that sharing such sensitive information within and among the critical information sectors will pose a unique challenge.

What are critical infrastructure assets?

Critical Infrastructure assets are defined as assets essential to the functioning of the Energy, Financial Services, Transportation, Communications & Information Services and Vital Human Services sectors(see footnote 5)—i.e., the assets of those systems vital to maintaining safety, public order, vital human services as

well economic stability.

Page 83 PREV PAGE TOP OF DOC

Which systems are critical infrastructure systems?

In brief, CI systems are the control systems and *any* connected system that can modify control systems. Control systems are those that directly manage the assets or implement the services on a moment-to-moment basis; as well as any system that the control systems depend on, or which can modify the operation of control systems, or have an indirect effect upon them. In some cases, CI systems may even include ordinary, Internet-connected workstations on the corporate LANs of infrastructure provider companies—all that is necessary is that the CI system has the ability to alter any of the control systems of a critical infrastructure IS.

Greatest national exposure to cyber terrorism is a homeland attack, distinct from more ordinary cyber vandals, hackers and thieves.

The most alarming scenario—and the one most likely to be the cause of multiple, simultaneous, and cascading disruptions on a regional, national or international scale—is a combination physical and cyber attack made by adversaries with the same motivation and ruthlessness of those committing the attacks this September.

This form of attack is a direct attack on the U.S. homeland, and is distinct from the activities of ordinary vandals, thieves, "hacktivists," and other types of people who exploit information security vulnerabilities of many kinds on many types of systems.

2.4 What is at Stake?

Page 84 PREV PAGE TOP OF DOC

The most pressing protection issue for information security today is preparing for the ability of cyber terrorists to work in conjunction with physical terrorists. As an industry and a Nation, we understand and are pursuing information security issues that will help us prevent, protect and mitigate damage to our critical infrastructures.

Here is an overview of the risk scenario as we understand it today.

Terrorism can be more devastating.

Threats to CI are more extensive.

The fallout from cyber-assisted terror is far greater than well-known examples of cyber attack.

The addition of cyber attacks to a standard terrorist scenario could increase the effectiveness and success rate of physical assaults and increase instability, physical damage and casualties. As our systems are more

complex and interdependent and as our systems—both electronic and operational—increase in complexity and geographic reach the risk of cascading damage and the vulnerability to attacks, increases. The threat is more extensive. Each computer connected to the Internet can increase the risk, and it just keeps growing.

It is relatively easy to imagine a terrorist developing a scenario that combined the September 11 attack with a cyber attack on the computers and networks of air traffic control radar, reducing our ability to track off-course airplanes and increasing the danger for other planes in the sky at the same time. Another combination-risk scenario would combine a cyber attack on water supply control systems with chemical weapons attack. This attack on the control systems of the water supply could mask effects of chemical or biological agents. It is worth noting that the fallout would be greater than that from viruses and worms that overload enterprise networks, or distributed denial of service attacks that cripple web sites.

Page 85 PREV PAGE TOP OF DOC

While cyber vandalism threats are significant and deserve attention including R&D, we know much about their damage potential and vulnerabilities. But are the vulnerabilities of CI systems sufficiently addressed? It is unlikely. We need to dramatically increase the magnitude and scope of R&D to include both the risks of "traditional" information security and to begin to address the investigation of the vulnerabilities of CI systems as a whole and the understanding of the real risk to our national security.

2.5 Urgent Challenges

I am concerned about four urgent challenges to InfoSec research and critical infrastructure. This committee can help in each case.

1. Critical lnfrastructure Vulnerabilities

We need to assess the vulnerabilities of Nation's critical infrastructure systems. We lack a specific, accurate, complete understanding of the *vulnerabilities* of CI systems. One type of R&D not being performed now is the *operations research* needed for this assessment. Operations research should focus on a range of representative CI systems—real world systems in operation today—to determine how current InfoSec technology and practices fit with those vulnerabilities, by answering these questions:

How can current InfoSec be better used for remediation of vulnerabilities, to make our CI systems more resistant to attacks today?

Page 86 PREV PAGE TOP OF DOC

How can we define "standard" approaches to apply current InfoSec to CI systems?

What are the limits of current InfoSec with respect to existing vulnerabilities and threats?

What are the technical R&D efforts needed to address the gaps?

2. Difficult R&D Problems

There are some hard R&D problems that urgently need attention in order to understand what these gaps may be, and how to effectively address them once we've defined them.

Interdependencies—Our Nation's networking and systems—including but not limited to CI systems—have grown increasingly dependent on one another for correct operation. Within CI, it is not only the systems that are interdependent, but each infrastructure area's delivery capability is logistically dependent on others.

Converged Networks—We have a new threat environment, with cascading effects on multiple information domains, potential for widespread outages impacting what are traditionally seen as redundant, fault tolerant sources.

Control Systems—There is an alarming dearth of information security technology for the embedded control systems that are used pervasively from manufacturing to power plants, throughout our CI systems and beyond.

3. R&D information sharing

Page 87 PREV PAGE TOP OF DOC

Today's world of InfoSec R&D is sufficiently fragmented and uncoordinated that it is not feasible to do more than a partial and cursory attempt to catalog efforts, assess relevance to CI-related InfoSec needs, and determine priorities. Indeed, the whole notion of setting new priorities is beset with difficulties based in the organizational structure of current government funding of InfoSec research—as well as government-performed R&D and the largely unconnected world of corporate funded and executed InfoSec R&D. Consequently, there is a real need for R&D information sharing and collaboration on a new level.

4. CI information sharing

Similarly, there is a need for information sharing and collaboration within the world of CI operators. The required vulnerability assessment, much less actually securing our networked infrastructure from cyber attack (or even from accidents causing cascading damage), *requires an unprecedented type of information sharing and collaboration* with the CI industry, and between industry and government. Put simply, the CI industry has never before had a reason to share information and collaborate on security. Government may have a critical role in ensuring that effective collaboration develops in a timely manner.

3. Challenges

I'd like to elaborate on each of these challenging areas, and then make some suggestions about what this committee can do to help.

3.1 Hard Problems, Urgent Needs for New Research

Page 88 PREV PAGE TOP OF DOC

Through Network Associates' work with the Partnership for Critical Infrastructure Security (PCIS), three challenge areas have been identified. These are: interdependency, converged networks, and control systems. These were identified as leading problem areas early on because of their criticality due to the scale of potential consequences of even partially successful attacks.

Control systems are at the heart of CI operations. While being the most significant asset (in terms of impact and cost of successful attack), control systems may also be highly dependent on other systems, as described above. And given the dearth of InfoSec R&D relevant to them, we really don't have an adequate understanding of either the applicability of current InfoSec to control systems, or the relevance of current R&D to gaps pertinent to control systems. Likewise, given the increasing trend to converged a networks, interdependencies and cascading attacks are a growing concern. Convergence ranges form data/telephony network convergence to multi-company shared e-business computing to CI providers' networks and computers interoperating with those of other CI providers.

All of these concerns come together because of various types of interdependencies. First, each infrastructure company has its own needs for infrastructure provided by other sectors, so failure in one sector can cascade effects to other infrastructure sectors. For example, water supply companies depend on chemical supplies that are delivered by transportation systems that, if disrupted by attack, can lead to supply shortages, degraded service, and increased risk. A second type of interdependency results from the fact that some infrastructure company's computer systems regularly interact with computing systems of others. As a result, each infrastructure company's computing systems are dependent on (regularly interact with, are vulnerable to) the computing systems of other companies, both other infrastructure providers and other companies in supply chain or partner roles. All of these interfaces create multiple entry points for cyber attack, so that a cyber attack on one company's systems can create opportunities for cascading cyber attack on others.

Page 89 PREV PAGE TOP OF DOC

These interdependency issues cut across physical operations (delivery of infrastructure services), information sharing, and protection and response technology. In each aspect of interdependency there are exacerbating factors that make the R&D issues even more critical:

Most existing InfoSec R&D may not be directly relevant to CI. The majority of traditional InfoSec research has been done in context of TCP/IP networks only, and standard commercial operating systems and software. Because control systems do not entirely share this technology base, current InfoSec may not be relevant to control systems specifically, CI systems and networks generally.

Most current R&D is oriented to technology and practices that are common in commercial world, and/or military/government's use of the same COTS technology for different purposes.

Existing InfoSec technology was developed with a single-owner/operator model. In practice, interdependent CI systems have dependencies and trust issues that span multiple operators' systems. Although these situations exist to some extent in more typical commercial computing, they are often not treated as technical issues but rather business issues. In CI computing however, the risk of one system to abuse from another is

simply a risk that cannot be accepted. Although there is some limited "inter-enterprise security" research in extranets and e-commerce applications which focus on extending security perimeters in controlled ways, current InfoSec R&D is not targeted towards developing solutions to these interdependency issues.

In summary, if we are to address critical infrastructure protection, then we need to examine technology and research solutions to address security threats that arise from the inter-dependency of multiple owners, operators, sectors and technology.

Page 90 PREV PAGE TOP OF DOC

3.1.1 CI-Oriented InfoSec R&D

Although we are not yet in a position to identify all of the R&D needs of CI (due the lack of vulnerability knowledge discussed above), there are some areas of InfoSec R&D that the R&D working group of the PCIS has identified as very likely to be relevant to CI needs.

Inter-enterprise security. R&D is needed to overcome the single owner/operator model mentioned above. Only very recently have we started doing technical R&D on security for this type of complex inter-enterprise computing. Commercial practice of linking systems, sharing e-business infrastructure, supply chain management—has outstripped commercially available security technology and current research. There is plenty of room for technical R&D here.

Anomaly-based security monitoring is a needed complement to current intrusion detection systems (IDS). Current IDS techniques are based on a technique familiar to users of anti-virus software: maintain and update a database of known attacks, and look for occurrences of a match with any of the items in the database. In the case of IDS, network traffic is monitored for a match with any of the known attack signatures. Anomaly-based monitoring, by contrast, is based on the notion of an existing policy, or set of rules, about what kinds of network traffic are permitted. Anything that is not specifically permitted is flagged as a potential security error or breach. Self-learning systems are an important capability, so that security systems can infer policies, and can modify policies when anomalies are deemed to be new behavior that is allowed. Inter-enterprise computing generally, and perhaps CI computing specifically, includes a more complex set of applications and data flows than the Internet connections that are typically protected by IDS. As a consequence, policy-based anomaly detection is needed to build up and evolve the set of rules about what it permitted; the simple lack of a match of IDS signatures would not, alone, ensure that an inter-enterprise security policy is in force.

Page 91 PREV PAGE TOP OF DOC

Situation-specific security mechanisms are needed for *real-time sharing of information on vulnerability and potential incidents.* These needs would derive from current efforts to build ISACs. An ISAC is an organization whose members are infrastructure operator companies in a CI sector, who are willing to share information about possible attacks, or sector-specific vulnerabilities for which countermeasures are available. Unlike public alert forums such as CERT, ISACs handle extremely sensitive information, both

because of the sensitivity attached to the information by member companies, and because of the information being of significant value to an attacker. Consequently, there are complex need to know issues, authorization requirements, and the need to use them to control inter-enterprise data flows to and through an ISAC. There are similar issues for ISAC-to-ISAC sharing, across CI sectors, as well as ISAC collaboration with public alert forums and cyber components of homeland defense organizations. Consequently, there is a need to develop both new technology and new standards and schemas for security usage to enable this type of information sharing. Also, without both basic and applied R&D on these issues, infrastructure provider companies may have significant security and privacy concerns that could be an impediment to otherwise desirable information sharing and collaboration (see Section 2.4).

Data mining techniques for ex post facto audit and reduction of large amounts of security log data. Currently, large amounts of log data go unregarded because of the lack of tools to analyze them. However, if such tools were developed, an effective security posture would include audit log reduction and security analysis to check for discovering well-camouflaged attacks in progress or lying dormant. In current commercial practice, many security incidents are discovered some time after the initial break-in occurs. While undesirable, this situation is acceptable in business computing because of the consequences of attacks do not often include a fundamental breakdown of the enterprise's ability to perform its mission. With CI systems, this is not the case. Furthermore, the current and typically costly and time-consuming approach to incident response is not likely to be workable for CI systems when an attack has been discovered. Again, much more effective data mining techniques will be required for analysis of an attack and determination of effective responses.

Page 92 PREV PAGE TOP OF DOC

Another part of incident response is recovery, including reconstitution of systems to a secure initial state, followed by backup/restore operations. Again a very costly part of current incident response, these operations could be greatly enhanced by *large-scale system-level checkpoint/rollback transaction technology* for entire system states for rapid post-attack reconstitution. Such rapid reconstitution will be extremely important for CI systems, as an alternative to going back to square one and rebuilding entire systems from scratch.

Analytic tools for modeling Cl interdependencies are need to first model systems and dependencies, and then plan logistical improvements to mitigate scope of cascading effects of attack. While such tools can be very important for infrastructure operators to mitigate risks, there would also be substantial sector-wide and national-level benefit. Eventually we would need to model the entirety of Nation's CI systems of note, to identify nodes of interdependency and/or shared risk that create greatest possibility for cascades. Such nodes represent the highest "degree of return" for an attacker efforts—physical or cyber terrorism or both.

These R&D areas are in addition to needed operations research (described in Section 2.2 below) that will better define R&D needs as well near-term priorities for vulnerability remediation.

3.2 Critical Infrastructure Vulnerabilities

There is a pressing need for operations research to fill large and critical gaps in the information security communities understanding of the logistical and technological aspects of infrastructure operators'

operations. The "facts on the ground today" are critical for assessing the vulnerability of our critical infrastructure to cyber terrorism. At present, information about these vulnerabilities exists only as closely held information of those infrastructure operators that have performed any security assessment. And no one understands the vulnerabilities that are shared across companies and sectors. Because our Nation's CI is operated by private CI operator companies, little is known about common vulnerabilities, or shortcomings of existing InfoSec technology and practice. This is just one glaring example of the types of collaboration that is needed; Collaboration between researchers in infrastructure operations and researchers in information security.

Page 93 PREV PAGE TOP OF DOC

Some practical results of collaborative operations research would be:

More precisely understand vulnerabilities.

Determine effective near-term remediation with existing InfoSec technologies, products, practices, and procedures.

Develop shared guidelines and standards for applying current InfoSec to CI systems.

Develop shared criteria for assessing the adherence of CI systems to guidelines and standards.

Define needs of CI security that are not met by current InfoSec technology and practices.

Assess these unmet needs in terms of current R&D, and define the gaps in current R&D.

Note that these "standards" (guidelines for applying current InfoSec technology, recommended policy/ procedures, assessment criteria, remediation guidelines, etc.) would be standard within a CI sector, or across CI providers generally.

However, without these "standards," individual CI companies will be very challenged to assess vulnerability, remediate, and identify tech gaps and practices gaps to be filled by R&D.

Page 94 PREV PAGE TOP OF DOC

Public policy issues include questions about how to go about meeting these goals. How much effort is needed and appropriate to devote to achieving these goals? What is the government's role in articulating them and achieving them? What role does government have in creating motivation for acceptance and application of "standards" and R&D goals? How should infrastructure operators be held accountable for security?

3.3 R&D Information Sharing and Collaboration

The problems in addressing cyber security are too big for any one community to tackle. The challenges here go far beyond those that can be addressed through forms of traditional government sponsored R&D

(both DOD and Civilian), privately funded industry R&D, and University R&D. The threats are real and imminent. We cannot afford to engage in politics and territorial disputes over R&D arenas. Furthermore, the magnitude of R&D required to even begin to address this area dictates that we must work together to collaboratively develop solutions and to identify synergies between various communities of R&D.

3.3.1 Solutions to Cyber Security R&D: Opportunities Through Partnerships

We are not proposing incremental approaches, rather we believe that it is imperative for all R&D stakeholders to embrace a completely unprecedented collaboration both in and across CI sectors to assess vulnerabilities today, establish standards, define gaps, and define R&D needs. Furthermore, this unprecedented level of collaboration must continue once research agendas are underway and throughout the full life cycle of R&D. We cannot afford to be less than vigilant in our steps towards understanding and addressing the ever-evolving set of threats in information security. This means that the critical infrastructure research community must become an integral part of steering and tracking information security R&D, in order to ensure that critical infrastructure needs are being articulated and addressed.

Page 95 PREV PAGE TOP OF DOC

At this stage we see three stakeholders that must embrace a radically different approach to R&D and new forms of cooperation, collaboration, and information sharing:

Federally funded R&D—both across agencies in terms of funding of contracted efforts and between agencies for internally funded and executed R&D.

Privately funded R&D by Industry—Because most privately funded R&D is focused on next generation products, we should expect to encounter barriers to info sharing and collaboration as corporations strive to protect their intellectual property. We encourage you to explore policy issues and develop new incentives for industry to share information and jointly pursue longer term, less product-oriented R&D. We must be innovative and find ways for corporations to dedicate some of the Nation's top brainpower towards solving problems for the greater good. Approaches might include corporate participation in consortia or through temporary assignment of key staff to a virtual think tank addressing these problems.

University R&D—This group presents a mixed bag of government funded R&D (both state and Federal) and industry and university funded R&D. Here the challenge is not so much sharing of research (the many academic conferences and journals make the research available) but how to capitalize in a timely manner on these research results.

Over the past several years, NAI Labs has been a leader in developing new forms of collaboration and partnerships in critical infrastructure protection research. Many of these are fledgling efforts, but they can serve as examples and we should seek opportunities to enhance and duplicate these efforts.

Page 96 PREV PAGE TOP OF DOC

3.3.2 Three Examples of Collaborative Partnerships

Partnership for Critical Infrastructure Security

The Partnership is a collaborative effort of industry and Government to address risks to the Nation's critical infrastructures and assures the delivery of essential services over the Nation's critical infrastructures. These infrastructures, identified in PDD–63, include:

Energy

Financial Services

Transportation

Communications and Information Services

Vital Human Services, including Health, Safety, and Water

Federal Lead Agencies are currently building partnerships with individual infrastructure sectors in industry. The Partnership will serve as a forum in which to draw these individual efforts together to facilitate a dialogue on cross-sector interdependencies, explore common approaches and experiences, and engage other key professional and business communities that have an interest in infrastructure assurance. By doing so, the Partnership can raise awareness and understanding of, and to serve, when appropriate, as a catalyst for action among the owners and operators of critical infrastructures, risk management and investment communities, and other members of the business community and state and local governments. The mission of the Partnership is to work with the Federal Government to promote the critical infrastructure security of the United States by focusing on cross-industry sector issues.

Page 97 PREV PAGE TOP OF DOC

The PCIS has five working groups:

Interdependency Vulnerability Assessment

Information Sharing, Awareness and Education

Legislative and Public Policy Objectives

R&D and Workforce Development

Organization Issues/Public Private Cooperation

Many people from industry and government have worked long and hard to bring the Partnership into existence and each of the working groups is actively engaged in addressing requirements, plans and developing road maps. The Partnership is a leading example of the collaboration across a wide range of organizations. However, funding for the partnership is small and the majority of participants do so in a "volunteer" role in addition to their regular responsibilities within their organizations. In order for the

Partnership to make substantial progress towards its ambitious goals in this challenging arena, new forms of funding and staffing need to be explored so that dedicated staff and funded projects can support the objectives of the organization.

Security Research Alliance (SRA)

Page 98 PREV PAGE TOP OF DOC

The SRA is a professional scientific alliance pursuing advanced research efforts bearing on the future of network security and related technology.

Network Associates formed the Security Research Alliance in 1999. It is a vendor-neutral organization of commercial information security vendors, each of whom have significant investments in the area of advanced security research. Charter members of the Alliance are BBN Technologies, Cisco Systems, Entrust Technologies, GTE, Lucent Technologies, Network Associates, and Sun Microsystems.

This group organized to form a true alliance between research laboratories of major information security vendors. Each organization is actively engaged in forward-looking research that explores information security technologies and issues 2–5 years out. Unlike product-focused R&D efforts, advanced security research projects take a broader look at security technologies and looks for better ways to overcome current limitations.

The group's primary objectives are threefold:

1. Better Communication of Research Findings to IT Community

2. Increase Likelihood of Transferring Research Findings into Commercial Solutions

3. Enhance Research Efforts through Collaborative Research and Peer Review

The Alliance seeks to improve communication of advanced security research findings to the IT community in order to provide the IT consumer with a longer-term view of technology. By doing so it is believed that we can move the state of practice from a reactive stance to a more proactive stance. This objective is synergistic with the Alliance's second objective of increasing opportunities for technology transfer. Better-educated consumers will demand increasingly sophisticated solutions. All research suffers to some degree from challenges of technology transfer. Through collaboration, on research projects, the Alliance aims to increase the likelihood that successful research findings will be transferred into commercial products. Alliance membership facilitates this process by sharing research findings, where appropriate. Ultimately, the Alliance believes these efforts will help to improve the overall quality of security products and technologies available to customers worldwide. Finally, the Alliance seeks to bring scientific discipline to the investigation of information security. Many researchers have backgrounds in mathematics and the hard sciences and well understand the value of peer review. However, due to the very early stages of information security research, little in the way of scientific discipline has yet evolved. The Alliance engages in peer review as a means of moving information security from art to a science.

Page 99 PREV PAGE TOP OF DOC

Army Research Labs, Collaborative Technology Alliance:

The Army Research Laboratory (ARL) is in the second phase of its innovative Collaborative Technology Alliance program. In its first phase, ARL created a new paradigm for Army research—a "federated laboratory." This new paradigm spanned the combination of government in-house, industry, and academic components striving together for excellence. ARL expanded and improved this concept with the creation of *Collaborative Technology Alliances.* These new alliances include five new programs focused on those technologies critical to transforming the Army, including aspects of information security and critical infrastructure research. The Army Research Laboratory's strategy is to continue exploiting commercial technology and expertise where it exists through the issuance of cooperative agreements and task order contracts.

The ARL CTA's are a set of programs covering 5 different technology areas: Advanced Sensors, Advanced Decision Architectures, Communications & Networks (C&N), Robotics, and Power & Energy.

NAI Labs is a member of the Communications & Networks (C&N) consortium led by Telcordia with industry teammates BAE Systems, Motorola, Network Associates, and BBN, and academic members University of Maryland, University of Delaware, Princeton University, the City College of New York, the Johns Hopkins University APL, Georgia Tech, Morgan State, and Clark Atlanta. NAI Labs has a lead role in developing efficient security services, including encryption and intrusion detection technologies, for these networks. Despite the military focus, the technology has great potential for transfer to the civilian world. The terms of the alliance recognize this and provide liberal intellectual property rights for consortium members encouraging rapid commercialization of research results.

Page 100 PREV PAGE TOP OF DOC

3.3.3 Future Directions for Enhanced Partnership and Collaboration

Each of these demonstrates a different approach to partnership and collaboration: the PCIS, a true partnership of industry sectors and civilian government agencies; the SRA, an alliance of leading information technology vendors; and the ARL CTA, an alliance of government, industry and academia. Each still faces many challenges, among them funding, dedicated staff, and concerns around intellectual property. However, we believe that these can serve as first case worked examples for R&D information sharing (as opposed to vulnerability and incident information sharing as in the ISACs), partnerships and collaboration. It is vital to recognize though, that as beneficial as these organizations are, they do not go far enough. They are a necessary, but not sufficient, first step towards addressing the national level coordination and collaboration that is required to ensure adequate R&D today, tomorrow, and into the future to protect our critical infrastructure resources.

We specifically recommend that congress develop new mandates and funding for unprecedented levels of collaboration. Such mandates must be motivated and encouraged through incentives that encourages new kinds of collaboration. All R&D research in the critical infrastructure protection arena should include requirements for developing research alliances and leveraging other research community R&D. All

researchers should be directed to take a participatory approach to R&D. Furthermore, we recommend that all information security R&D funding organizations (public and private) and researchers participate in an ongoing national effort to catalog and track their efforts applicable to the critical infrastructure threat. In order to accomplish this, the Federal government must create incentives for broad public/private participation, between and among government agencies and through private collaboration consortia like the Security Research Alliance. This will require direct action to promote the urgent need for new collaboration and new approaches to policy in order to identify and eliminate barriers to collaboration within government and between government and private industry.

Page 101 PREV PAGE TOP OF DOC

3.4 CI Information Sharing and Collaboration

The need for CI information sharing and collaboration is unprecedented but required in order to address the CI vulnerability issues described in Section 2.2, and to define effective R&D goals to drive the R&D collaboration described in Section 2.3. The need is for security collaboration both within the CI industry and between industry and government.

Just as the intelligence and law enforcement communities, after September 11, realized the inadequacy of current approaches to collaboration, CI players are realizing that neither comprehensive improvement in security nor creating an effective preparedness/response capability is possible without collaboration. Yet unlike intelligence and law enforcement, CI players have never had any significant motivation for collaboration—and indeed in many cases are competitors in a field of private for-profit delivery of CI services.

The PCIS has started to build some collaborative structures, but is still in the early days of the work. Some degree of R&D gap analysis has been done (as described in Section 2.1.2), but clearly done without any but the most general understanding of the InfoSec needs of actual CI systems as they are operated today. Work on those needs has been primarily focused on gaining a better understanding of the interdependency problems, and considering how working groups can research the needs to address those problems—within the constraints of PCIS operation as public/private consortium.

However, a much greater degree of collaboration is needed, as indicated by the following goals of the working group.

Page 102 PREV PAGE TOP OF DOC

Within and across sectors in the CI industry, perform pilot vulnerability assessments of representative systems.

Share the results, work to define the specific needs for addressing CI vulnerabilities.

Determine the extent to which current InfoSec can address those needs, and how to codify recommendations for doing so.

Determine the extent to which current InfoSec is insufficient, define the specific technical and procedural InfoSec gaps.

Define R&D needs

Work honestly to flag unknowns, keep flexible and collaborative, yet strive to define "standards" that useful tools for CI providers to improve security and identify R&D needs.

The CI community must become integral part of steering and tracking InfoSec R&D, ensure that CI needs are being articulated and addressed in R&D, as defined in Section 2.3 above.

The CI community must work with homeland defense, to collaborate on requirements for detection, response, and recovery from attacks. This is a broad area with many issues relevant to formation of ISACs, information sharing ISACs and with homeland defense.

Public Policy Issues: For many of these goals, there are important public policy issues, ranging from anti-trust concerns to concerns over development of new, unfunded mandates (similar to the decision that commercial airlines should not be compelled to operate heightened security measures without assistance and guidance).

Page 103 PREV PAGE TOP OF DOC

4. What Can This Committee Do To Help?

Our call for congressional action falls into two areas in which this Committee's efforts can begin to be effective in the short term.

Foster highest-impact R&D—spending and set direction

Promote focus on CI protection—spending and set direction

4.1 Foster Highest-Impact R&D

This Committee can take immediate steps to ensure that R&D spending is focused on efforts of the highest impact in both the near- and long-term. High-impact R&D does not mean only near-term; rather impact should be sought through innovative approaches towards bringing together distinct research teams to focus on common problems and understanding. Some suggested steps that the committee can do to start to help are:

Work towards mandate and funding for unprecedented collaboration

i. Including *all* InfoSec R&D fenders/researchers to catalog and track efforts applicable to CI. Create incentives for broad public/private participation: government agencies and private collaboration consortia like SRA.

ii. Promote urgent need for new collaboration.

Page 104 PREV PAGE TOP OF DOC

iii. Identify and eliminate barriers to collaboration within government and between government and private.

Help accelerate work of public and private organizations including public/private partnerships like PCIS, with groups working on R&D, interdependency, and public policy.

4.2 Focus on CI Protection

This Committee can foster a focus on CI protection by developing public policies that support CI protection:

Promote Congressional action on public policy issues—both in creating new public policy and in eliminating public policy barriers (e.g., antitrust relief for collaboration with CI sectors).

Create new agenda for CI InfoSec research, starting with operations research needed for vulnerability assessment and R&D gaps.

Feed new R&D results into public policy evaluations.

Use this evaluation information to set R&D priorities, redirect efforts, begin to set assessment criteria, best practices and priorities for future research. This must be an ongoing effort, as we work to fill the gaps in our knowledge about Cl vulnerabilities and InfoSec technology gaps.

Page 105 PREV PAGE TOP OF DOC

Fostering sharing of information between government/industry/university R&D work—while honoring and protecting legitimate competitive concerns. (Private IP rights important to maintain benefits to customer, rights to developer, and preserve private incentive for R&D.)

4.2.1 New Mandate

Perhaps the most basic goal is *funding* and *mandate* to accelerate CI vulnerability assessments, resulting R&D gap analysis, and subsequent R&D to fill the gaps. The resulting "standards" are needed for an improved security posture, while the R&D gap information is required to better direct R&D. Both are needed to overcome limits and gaps in current InfoSec, for guidance of government-funded research, and for aid in public/private advocacy of private R&D that is both infrastructure-critical and potentially strategic to company funding the research.

Continuing the information security R&D that is currently underway is necessary but not sufficient. Current efforts provide a technology and knowledge base to draw on once a more complete picture of CI vulnerabilities is in process. Thus, more research money (via NSF, NIST, NSA, DARPA, etc., for technical

R&D in InfoSec) would be beneficial, but in parallel with this, we *must* work to assess CI vulnerability to determine needs.

5. Recommendations for Congressional Action

In light of the challenges I have just outlined, I respectfully offer to the Committee suggestions on five steps that this Committee and Congress can take in the area of cyber security research and development.

Page 106 PREV PAGE TOP OF DOC

1. Ensure cyber security is part of Homeland Security

As the new Office of Homeland Security begins to take shape and as the new Cabinet Secretary begins his role, I ask Congress to ensure that cyber security is a part of our Nation's approach to Homeland Security. While the events of September 11th were physical in nature, we must remember that protecting our doors but leaving open a cyberwindow makes the American house vulnerable.

2. Authorize a study of our Nation's critical infrastructure vulnerabilities

As I have conveyed throughout this testimony, before we expand our R&D agenda, we must fully understand our critical infrastructure vulnerabilities. I ask this Committee to authorize and Congress to fund a rapid but thorough analysis of our vulnerabilities The study should focus on bringing together the many analyses that already exist, while identifying needs for further study.

3. Authorize increases in funds for technical R&D to leading departments and agencies

Currently, many departments and agencies throughout the Federal Government are engaged in extensive R&D projects. I ask Congress to provide these agencies, such as NIST, DARPA, NSA, NSF and others, with expanded resources to conduct research to meet their own cyber security needs.

Page 107 PREV PAGE TOP OF DOC

4. Improve coordination among government-funded R&D projects

While each Federal department and agency certainly needs to pursue projects for its own needs, Congress should work with them to ensure that plans and results are shared widely to avoid duplicative work and fully leverage the knowledge gained. From its oversight role, Congress can ensure that continued coordination takes place.

5. Develop a new collaborative research mechanism

Within government, industry and academia, a tremendous amount of research is taking place. Yet, much of the results go unshared. I ask Congress to develop a collaborative mechanism to catalog and track efforts applicable to critical infrastructure and to create incentives for broad public/private participation.

6. Conclusion

Mr. Chairman, the opportunity to have a real impact on the cyber security of our Nation's critical infrastructures is tremendous. But doing so will require a strong commitment to research and development, for we cannot rely on today's solutions for tomorrow's challenges. We urge your Committee and Congress to continue putting energy into the R&D issues I have outlined. In return, I pledge to you our company's support to continue to work with government to identify our Nation's R&D needs and conduct the research essential to ensure our Nation's cyber security.

I thank you again for the opportunity to testify here today, and I look forward to answering any questions the Committee may have.

Page 108 PREV PAGE TOP OF DOC

BIOGRAPHY FOR TERRY C. VICKERS BENZEL

Ms. Benzel is Vice President of Advanced Security Research for Network Associates, Inc. (NAI), and Director of NAI Labs.

As Director of NAI Labs, she is responsible for leading the nation's premier advanced security research laboratory, with a staff of 100 researchers performing leading-edge research on perceived security issues two to five years in the future. NAI Labs works on a wide range of security topics under contract to DARPA, other DOD agencies, and commercial programs.

Ms. Benzel proactively seeks to foster new partnerships between industry and government. She is a member of the security panel of the President's Council of Advisors on Science and Technology; Chair of the R&D working group of the Partnership for Critical Infrastructure Security; and Founder of the Security Research Alliance.

In addition to her duties in government-sponsored research, she participates on Network Associates' engineering review board and product strategy teams, including leading technology transfer projects.

Ms. Benzel comes to Network Associates through its acquisition of Trusted Information Systems (TIS) in early 1998. At TIS, Ms. Benzel spent ten years directing DARPA-sponsored research and providing security products consulting to major security vendor organizations. Prior to joining TIS, Ms. Benzel was a group manager at the MITRE Corporation in Bedford, Massachusetts. She holds an advanced degree in mathematics from Boston University and an Executive MBA from University of California, Los Angeles.

Page 109 PREV PAGE TOP OF DOC

Chairman **BOEHLERT.** Thank you much—very much, Ms. Benzel. I really appreciate it. I would like to ask all of the Committee join me in welcoming our next presenter, Mr. Robert Weaver, of the New York Electronic Crimes Task Force from the Secret Service, whose offices were Number Seven World Trade Center. You are doing magnificent work for the country, and our prayers have been answered—you are all

safe from your unit. So, we welcome. You may proceed.

STATEMENT OF ROBERT WEAVER, ASSISTANT SPECIAL AGENT IN CHARGE, U.S. SECRET SERVICE; DIRECTOR, NEW YORK ELECTRONIC CRIMES TASK FORCE, NEW YORK FIELD OFFICE

Mr. **WEAVER.** Mr. Chairman, Mr. Hall, members of the Committee, thank you for the opportunity to address the Committee regarding computer security and how we can protect American computer networks from attack. I want to especially thank you, Mr. Chairman, for your unwavering support and advocacy on behalf of all the members of the Task Force. After the dark day of September 11, your commitment and dedication to our rebuilding efforts has been, and remains, inspiration to all of us who are committed to public service. You were the first to call and we appreciate that.

As you know, Mr. Chairman, on September 11, the Secret Service lost one of its largest field offices in the attack on the World Trade Center. Our New York Field Office and New York Electronic Crimes Task Force were housed on the 9th and 10th floor of Seven World Trade Center, the third building to collapse on that tragic day.

Page 110 PREV PAGE TOP OF DOC

While we lost equipment, vehicles, and records, we were largely shielded from the tragic loss of life that was endured by our partners in law enforcement and emergency services communities. Despite this tremendous blow, the New York Electronic Crimes Task Force is today not only fully functional, but actively involved in the financial and telecommunications investigations surrounding the suspected terrorists. Our ability to detect and prevent computer-based attacks against our critical infrastructure has not diminished in any form, and our resolve has been immeasurably strengthened.

The Secret Service fights cyber crime as part of our core mission to protect the integrity of this Nation's financial payment systems. There is no question that our critical infrastructure and financial payment systems are highly vulnerable to potential attacks from hackers, criminal organizations, and terrorists alike. The New York Secret Service, Electronic Crimes Task Force, had developed a highly effective formula for combating high-tech crime.

While the Secret Service leads this innovative effort, we do not control it, dominate the participants, or even the investigative agenda of the Task Force. Rather, the Task Force impacts the community by providing a productive framework and collaborative crime/fighting environment in which the resources of its participants can be combined to effectively and efficiently make a significant impact on electronic crimes.

Within this New York model, which we established in 1995, there is a wealth of experience, expertise, and resources that reside on the Task Force. Coupled with unprecedented information sharing, we yield a highly mobile and responsive machine. These investigations encompass a wide range of computer-based criminal activity involving e-commerce frauds, intellectual property, telecommunication fraud, a wide variety of computer intrusion crimes. Since we started in 1995, we have charged over 800 individuals with electronic crimes valued at $525 million in losses.

Page 111 PREV PAGE TOP OF DOC

We have trained, in addition, 13,000 law enforcement personnel, prosecutors and private industry representatives, in the criminal abuses of technology and how to prevent them. This systemic approach and business model of the Task Force is based on the principal of prevention, education, training and awareness, pre-incident response and risk management, investigations, and prosecutions.

But what I believe truly separates this Task Force from all others, which gives us our unique brand that has generated so much success, is our commitment to builded trusted partnerships and relationships in placing the highest priority on that which is in the best interest of the community.

Mr. Chairman, the greatest strength of the Task Force in New York is our commitment and contribution to the community. Our core mission has been always very simple: to make a difference, to have an impact on the community, to respond to the needs of the consumer, private industry, and our law enforcement partners. The community has always been our focus. Little did we know that one fateful day after the destruction of our office and all of our investigative tools and resources and records, that this community would stand by our side and help us to rebuild. Despite losing our building and our equipment, we still had our most precious resource—each other.

I cannot tell you how proud I am, not only of the young men and women of the Secret Service who work tirelessly, night and day, but also of the assistance and support the Task Force partners have given us. I cannot quantify that to you. Because of this support, I can tell you that after the complete destruction of the New York Field Office, the now battle-tested Task Force was operational within 48 hours and fighting back.

Page 112 PREV PAGE TOP OF DOC

Mr. Chairman, I would like to close with one last point about partnerships. They are a very popular term in government and private industry these days and everyone agrees that is a great approach. Unfortunately, partnerships cannot be legislated, regulated, or stipulated, nor can they be purchased, traded, or incorporated. They are built between people and organizations who recognize the value and the joint collaboration toward a common end. They are fragile institutions which need to be established and maintained by all participants upon a foundation of trust. Everyone knows the Secret Service protects and serves. Now, in the information age, our mission is also to protect servers.

In today's high-tech criminal environment, the challenge to Federal law enforcement and government alike is to identify existing repositories of expertise and provide a framework for inclusion and productive collaboration amongst the many government agencies and the respective industry and academic counterparts. We are convinced, the Secret Service is, that building trusted partnerships with the private sector and local and state law enforcement is the model for combating electronic crimes in the information age.

Mr. Chairman, and, Mr. Hall, the Committee, this concludes my presentation and my prepared remarks, and I would be happy to answer questions you my have.

[The prepared statement of Mr. Weaver follows:]

PREPARED STATEMENT OF MR. ROBERT WEAVER

Mr. Chairman, Members of the Committee, thank you for the opportunity to address the committee regarding computer security and how we can protect American computer networks from attack. Mr. Chairman, I want to especially thank you, Mr. Chairman, for your unwavering support and advocacy on behalf of all of the members of our task force. After the dark day of September 11, 2001, your commitment and dedication to our rebuilding efforts has been and remains inspirational to all of us who are committed to public service.

Page 113 PREV PAGE TOP OF DOC

The Secret Service fights cyber crime as part of our core mission to protect the integrity of this nation's financial payment systems. This role has evolved from our initial mandate to suppress the counterfeiting of currency upon our creation in 1865. Since this time, modes and methods of payment have evolved and so has our mission. Computers and other "chip" devices are now the facilitators of criminal activity or the target of such. The perpetrators involved in the exploitation of such technology range from traditional fraud artists to violent criminals—all of whom recognize new opportunities and anonymous methods to expand and diversify their criminal portfolio.

In this era of change, one constant that remains is our close working relationship with the banking and finance sector and the telecommunications industry. Our history of cooperation with these industries is a result of our unique responsibilities and status as an agency of the Department of the Treasury. We believe that protection of the banking and financial infrastructure and telecommunications is our "core competency" area. As an agency, we seek to manage and apply our unique investigative resources in the most efficient manner possible for the benefit of our telecommunications financial institution customers.

Mr. Chairman, there is no shortage of information, testimony, or anecdotal evidence regarding the nature and variety of cyber-based threats to our telecommunications and banking and financial infrastructures and the need to create effective solutions. There is, however, a scarcity of information regarding successful models to combat such crime in today's high tech environment. That is where the Secret Service can make a significant contribution to todays and future discussions of successful law enforcement efforts to combat cyber crime.

Page 114 PREV PAGE TOP OF DOC

The Secret Service has found a highly-effective formula for combating high tech crime—a formula that has been successfully developed by our New York Electronic Crimes Task Force. While the Secret Service leads this innovative effort, we do not control or dominate the participants and the investigative agenda of the task force. Rather, the task force impacts the community by providing a productive framework and collaborative crime-fighting environment in which the resources of its participants can be combined to effectively and efficiently make a significant impact on electronic crimes. Other law enforcement agencies bring additional criminal enforcement jurisdiction and resources to the task force while representatives from

private industry, such as telecommunications providers, for instance, bring a wealth of technical expertise.

Within this New York model, established in 1995, there are 50 different federal, state and local law enforcement agencies represented as well as prosecutors, academic leaders and over 150 different private sector corporations. The wealth of expertise and resources that reside in this task force coupled with unprecedented information sharing yields a highly mobile and responsive machine. In task force investigations, local law enforcement officers hold supervisory positions and representatives from other agencies regularly assume the lead investigator status. These investigations encompass a wide range of computer-based criminal activity, involving e-commerce frauds, intellectual property violations, telecommunications fraud, and a wide variety of computer intrusion crimes.

Since 1995, the task force has charged over 800 individuals with electronic crimes valued at more than $525 million. It has trained over 13,000 law enforcement personnel, prosecutors, and private industry representatives in the criminal abuses of technology and how to prevent them. We view the New York Electronic Crimes Task Force as the model for the partnership approach that we hope to employ in additional venues around the country in the very near future. The systemic approach and business model of the task force is based on the principles of prevention, education, training and awareness, pre-incident response risk management, investigations and prosecution. But what I believe separates this task force from all others, what truly gives us our unique brand that has generated so much success, is our commitment to building trusted partnerships and lacing the highest priority on that which is in the best interests of the community.

Page 115 PREV PAGE TOP OF DOC

Mr. Chairman, the greatest strength of the New York task force is our commitment and contribution to the community. Our core mission has always been simple—to make a difference, to have an impact on the community, and to respond to the needs of our law enforcement partners, consumers, and private industry. The community has always been our focus. Little did we know, that one fateful day after the destruction of our office and all of our investigative tools and records, that this community would stand by our side and help to rebuild us. Despite losing our building and our equipment, we still had our most precious resource, each other. I cannot tell you how proud I am of not only the men and women of the Secret Service who work tirelessly on the task force day and night, but also the assistance and support of our task force partners that cannot be quantified.

Because of this support, I can tell you that within 48 hours of the complete destruction of our New York Field Office, the now battle-tested task force model was operational within 48 hours and fighting back.

An important component in our investigative response to cyber crime is the Electronic Crimes Special Agent Program (ECSAP). This program is comprised of approximately 175 special agents who have received extensive training in the forensic identification, preservation, and retrieval of electronically stored evidence. Special Agents entering the program receive specialized training in all areas of electronic crimes, with particular emphasis on computer intrusions and forensics. ECSAP agents are computer investigative specialists, qualified to conduct examinations on all types of electronic evidence, including computers, personal data assistants, telecommunications devices, electronic organizers, scanners and other electronic

paraphernalia.

Page 116 PREV PAGE TOP OF DOC

The Secret Service ECSAP program relies on the 4 year-old, Treasury-wide Computer Investigative Specialist (CIS) initiative. All four Treasury law enforcement bureaus—the Internal Revenue Service, Bureau of Alcohol, Tobacco and Firearms, U.S. Customs Service and the U.S. Secret Service—participate and receive training and equipment under this program. Recently, this has been expanded to include state and local law enforcement.

All four Treasury bureaus also jointly participate in curriculum development and review, equipment design and distribution of training assets. As a result, financial savings by all Treasury bureaus are realized due to economies of scale. Additionally, agents from different bureaus can work together in the field in an operational capacity due to the compatibility of the equipment and training. In the end, the criminal element suffers and the taxpayer benefits.

Because of the recognized expertise of those in ECSAP, other law enforcement agencies regularly request training from the Secret Service or advice concerning their own computer forensics programs. These requests have come from agencies all across the country, as well as foreign countries such as Italy and Thailand. The Secret Service recognizes the need to promote international cooperation and remains proactive in the dissemination of information to law enforcement agencies, both domestically and internationally, regarding program initiatives and current financial and electronic crimes trends.

Mr. Chairman, we are committed to working closely with our law enforcement counterparts worldwide in response to cyber crime threats to commerce and financial payment systems. We currently have 18 offices in foreign countries and a permanent assignment at Interpol, as well as several overseas initiatives. Our foreign presence increases our ability to become involved in foreign investigations that are of significant strategic interest.

Page 117 PREV PAGE TOP OF DOC

In addition to providing law enforcement with the necessary technical training and resources, a great deal more can be accomplished in fighting cyber crime if we are able to harness additional resources that exist outside government in the private sector and academia. The Secret Service believes there is value in exploring new methods within the legal framework with both those in the private sector and academia who are devoting substantial resources to protecting their networks and researching new solutions.

Finally, law enforcement in general is not sufficiently equipped to train the masses nor can it compete with academic institutions of higher learning in the area of research and development. However, our partnerships with industry and academia have demonstrated that this should be an integral part of the solution.

Partnerships are a very popular term in both government and the private industry these days and everyone

agrees that there is great benefit in such an approach. Unfortunately, however, partnerships cannot be legislated, regulated, or stipulated. Nor can partnerships be purchased, traded or incorporated. Partnerships are built between people and organizations who recognize the value in joint collaboration toward a common end. They are fragile entities which need to be established and maintained by all participants and built upon a foundation of trust.

The Secret Service, by virtue of the protective mission for which we are so well known, has always emphasized discretion and trust in executing our protective duties. We learned long ago that our agency needed the full support and confidence of local law enforcement and certain key elements of the private sector to create and maintain a successful and comprehensive security plan. Furthermore, we are also keenly aware that we need to maintain a trusted relationship with our protectees so that we can work with them and their staffs to maintain the delicate balance between security and personal privacy. Everyone knows the Secret Service "protects and serves;" now, in the Information Age, our mission is to also "protect servers."

Page 118 PREV PAGE TOP OF DOC

Our predisposition towards discretion and trust naturally permeates our investigative mission where we enjoy quiet successes with our private sector partners. We have successfully investigated many significant cases with the help of our private sector partners such as network intrusions and compromises of critical information or operating systems. In such cases, even though we have technical expertise that is second to none, we still rely on our private sector counterparts to collaborate with us in identifying and preserving critical evidence to solve the case and bring the perpetrator to justice. Equally important in such cases is conducting the investigation in a manner that avoids unnecessary disruption or adverse consequences to the victim or business. With the variety of operating platforms and proprietary operating systems in the private sector, we could not accomplish these objectives without the direct support of our private sector partners.

In fact, in one recently completed complex investigation involving the compromise of a wireless communications carrier's network, our case agent actually specified in the affidavit of the federal search warrant that representatives of the victim business be allowed to accompany federal agents in the search of the target residence to provide technical assistance. This is unprecedented in the law enforcement arena and underscores the level of trust we enjoy with those we have built relationships with in the private sector. It is also indicative of the complexity of many of these investigations and serves to highlight the fact that we in law enforcement *must* work with private industry to be an effective crime fighting force. In approving this search warrant, the court recognized that in certain cases involving extraordinarily complex systems and networks, such additional technical expertise can be a critical, and sometimes imperative, component of our investigative efforts.

Page 119 PREV PAGE TOP OF DOC

Recently concluded investigations demonstrate the breadth of cases the Secret Service is working, and provide concrete evidence of the continuing success of ECSAP. Examples of such cases include an intrusion into a telecommunication provider's network and an attack on a private investment company's trading network.

The first case was initiated on February 20, 2001, a case with obvious critical infrastructure implications, when two major wireless telecommunications service providers notified the New York Electronic Crimes Task Force that they had identified two hackers in different remote sites who were attacking their systems. These hackers were manipulating the systems to obtain free long distance service, re-route numbers, add calling features, forward telephone numbers, and install software that would ensure their continued unauthorized access.

The level of access obtained by the hackers was virtually unlimited, and had they chosen to do so, they could have shut down telephone service over a large geographic area, including "911" systems, as well as service to government installations and other critical infrastructure components.

On March 20, 2001, the Secret Service simultaneously executed search warrants in New York City and Phoenix and computer equipment was seized at both locations. One suspect was arrested on federal computer fraud charges, while the other suspect is pending indictment for computer tampering under Arizona state statute. The partnership and teamwork with the telecommunications service providers made all the difference in the successful and final outcome. They were included from start to finish in the investigative and prosecutorial strategies to better protect their information and operational effectiveness.

Page 120 PREV PAGE TOP OF DOC

The second case occurred from March 9, 2000, through March 14, 2000, when a company located in New York, NY, received several Internet-based "denial of service" attacks on its servers. A "denial of service" attack occurs when a perpetrator launches malicious programs, information, codes, or commands to a target or victim computer which causes a degradation of service or shutdown, thereby denying access by legitimate customers to those computers. In this instance, the company was a prominent provider of electronic trading services on Wall Street.

While the attacks were still occurring, the company's CEO contacted the New York Electronic Crimes Task Force. The CEO identified a former employee as a suspect, based upon the fact that the attacks preyed on vulnerabilities which would only be known to the former employee. These attacks continued through March 13, 2000, when ECSAP agents and task force members identified the attacking computer and arrested the former employee for violating Title 18, USC, Section 1030 (Computer Fraud). In a post-arrest statement, the suspect admitted that he was responsible for the denial of service attacks. As a result of the attacks, the company and its customers lost access to trading systems. Approximately $3.5 million was identified in lost trading fees, commissions, and liability as a result of the customers' inability to conduct any trading.

Let me relate the Secret Service's mission in fighting cyber crime to the bigger picture of critical infrastructure protection. As previously stated, we target cyber crime as it may affect the integrity of our nation's financial payment and banking systems. As we all know, the banking and finance sector comprises a very critical infrastructure sector and one which we have historically protected and will continue to protect. In this context, our efforts to combat cyber assaults which target information and communication systems which support the financial sector are part of the larger and more comprehensive critical infrastructure protection scheme. The whole notion of infrastructure protection embodies an assurance and confidence in the delivery of critical functions and services that in today's world are increasingly

interdependent and interconnected. To put this all in perspective, the public's confidence is lost if such delivery systems and services are unreliable or unpredictable regardless of the cause of the problem.

Page 121 PREV PAGE TOP OF DOC

We also recognize that our unique protective responsibilities, including our duties as the lead federal agency for coordinating security at National Special Security Events, demand heightened electronic security awareness and preparation. A well-placed cyber attack against a weak technology or support infrastructure system can render an otherwise sound physical security plan vulnerable and inadequate.

Mr. Chairman, it should also be noted that all deliberate infrastructure attacks, before they rise to such a threshold, are also cyber crimes and are likely to be dealt with initially by law enforcement personnel, both federal and local, in the course of routine business. In fact, I don't believe there is universal agreement as to when a "hack" or network intrusion rises to the threshold of an infrastructure attack and corresponding national security event but we would all probably recognize one when it reached catastrophic proportions.

Given this continuum and interplay between computer-based crimes and national security issues, the Secret Service recognizes that its role in investigating computer-based attacks against the financial sector can be significant in the larger plan for the protection of our Nation's critical infrastructures. When we arrest a criminal who has breached and disrupted a sensitive communications network and are able to restore the normal operation of the host—be it a bank, telecommunications carrier, or medical service provider—we believe we have made a significant contribution towards assuring the reliability of the critical systems that the public relies upon on a daily basis.

As a footnote, the task force meets regularly with representatives from Wall Street and the Financial Services Information Sharing and Analysis Center (FS/ISAC) that was created pursuant to Presidential Decision Directive (PDD) 63. The directive mandated the Department of the Treasury to work with members of the banking and finance sector to enhance the security of the sector's information systems and other infrastructures, a responsibility managed by Treasury's Assistant Secretary of Financial Institutions. The role of the FS/ISAC is to devise a way to share information within the financial services industry relating to cyber threats and vulnerabilities. The Secret Service feels that it can make a significant contribution to the work of the FS/ISAC and is exploring common areas of interest with the FS/ISAC, to include information sharing, information technology, and expertise in technical, physical security and administrative areas of concern.

Page 122 PREV PAGE TOP OF DOC

The Secret Service is also continuing to receive requests from local law enforcement agencies and others for assistance, and we welcome those requests. On an alarmingly increasing basis, our local field offices and the Financial Crimes Division of the Secret Service receive desperate pleas from local police departments for physical assistance, training and equipment in the area of computer forensics and electronic crimes so that they can continue to provide a professional level of service and protection for their citizens. In short, the Secret Service has become another option for local law enforcement, the private sector and others to turn to

when confronted with network intrusions and other sophisticated electronic crimes.

Over the past 3 years, Secret Service ECSAP agents completed 2,122 examinations on computer and telecommunications equipment. Although the Secret Service did not track the number of exams done for other law enforcement agencies during this period, it is estimated that some 10 to 15 percent of these examinations fell in this category. Many of the examinations were conducted in support of other agencies' investigations such as those involving child pornography or homicide cases simply because the requesting agency did not have the resources to complete the examination itself.

In spite of our limited resources, we do provide physical assistance on a regular basis to other departments, often sending ECSAP agents overnight to the requesting venue to perform computer related analyses or technical consultation. In fact, so critical was the need for even basic training in this regard that the Secret Service joined forces with the International Association of Chiefs of Police and the National Institute for Justice to create the "Best Practices Guide to Searching and Seizing Electronic Evidence" which is designed for the line officer and detective alike.

Page 123 PREV PAGE TOP OF DOC

We have also worked with this group to produce the interactive, computer-based training program known as "Forward Edge" which takes the next step in training officers to conduct electronic crime investigations. Forward Edge incorporates virtual reality features as it presents three different investigative scenarios to the trainee. It also provides investigative options and technical support to develop the case. Copies of state computer crime laws for each of the fifty states as well as corresponding sample affidavits are also part of the two-CD training program and are immediately accessible for instant implementation.

Thus far we have dispensed over 220,000 "Best Practices Guides" to local and federal law enforcement officers and we are preparing to distribute, free of charge, over 20,000 Forward Edge training CDs.

In an additional effort to further enhance information sharing between the law enforcement community and the financial industry, the Secret Service recently created the "E Library" Internet website which serves as a mechanism for all members to post specific information, images and alerts relating to fictitious financial instruments, counterfeit checks, and credit card skimming devices. This website is accessible free of charge to all members of the law enforcement and banking communities and is the only such tool of its kind.

In today's high tech criminal environment, the challenge to federal law enforcement and government is to identify existing repositories of expertise and provide a framework for inclusion and productive collaboration amongst the many government agencies and their respective industry and academic counterparts. The Secret Service is convinced that building trusted partnerships with the private sector and local law enforcement is the model for combating electronic crimes in the Information Age.

Page 124 PREV PAGE TOP OF DOC

Mr. Chairman, that concludes my prepared statement, and I would be happy to answer any questions that

you or other Members of the Subcommittee may have.

BIOGRAPHY FOR ROBERT WEAVER

Bob Weaver has served in the Secret Service for nearly 20 years. He currently holds the position of Assistant Special Agent in Charge of the New York Field Office, and also serves as the head of the New York Electronic Crimes Task Force. As part of his duties, he is responsible for coordinating and supporting a wide range of financial crime investigations—including credit card fraud, identity theft and telecommunications fraud—as well as training our law enforcement and private industry partners in the criminal abuses of technology and how to prevent them.

Bob began his career with the Secret Service in 1982 as a Special Agent assigned to the Washington Field Office, and since that time has served in a variety of positions, including Team Leader of the Secret Service's Counter Assault Team and a tour of duty with the Vice Presidential Protective Division.

Prior to joining the Secret Service, Bob earned his undergraduate degree from Central Connecticut State University and subsequently served with the Federal Bureau of Investigation and as an assistant to Supreme Court Justice Warren Burger. After joining the Secret Service, he earned a Masters of Forensic Science degree from George Washington University. Today, as head of the New York Electronic Crimes Task Force, he supervises a dedicated staff of high tech crime fighters and criminal investigators who are respected throughout law enforcement, the private sector and academia.

Page 125 PREV PAGE TOP OF DOC

Discussion

Chairman **BOEHLERT.** Thank you very much for excellent testimony. Thank all of you for excellent testimony. Wish it were possible to have this hearing retroactively and to initiate action retroactively. It is very apparent to me from your testimony that we don't know what we don't know. But there are some things we do know. And to coin the phrase, or to borrow a phrase from Ms. Benzel, it is beyond frightening.

We know there is no real focal point or computer security matters in the Federal Government. We know—and even the Administration can't tell us there are no exacts as to how much is being spent by which agencies on computer security. We know there are too few experts in the field. We know that we don't have an active minor league system with young people coming up. We know that the thinking is short-term versus long-term.

We know, in many instances, we have been too conservative. This is not philosophic—political philosophy, but too conservative in our thinking. We haven't thought out-of-the-box, so to speak. You know, I love the National Science Foundation. It is one of my favorite agencies in the whole wide world and I put the people there on a pedestal, but I am very mindful that they operate under peer-review, which is very important, but peer-review doesn't allow, in this instance, particularly, for the innovative sort of a somewhat different thinker.

So we have got our work cut out for us. And let me start by asking a very basic question. If we all agree

that there is no focal point—and I think we can all agree there should be some focal point—have we given some thought to where that focal point should be? Should it be the new Office of Homeland Security under Governor Ridge? Should it be our—should it be NSF? Should it be something new that we create? But, obviously, when we have got so many unanswered questions, we need to start at the beginning by having a center of gravity and have things work out from there.

Page 126 PREV PAGE TOP OF DOC

So the focal point. And then, if you can be a little more specific on some of the dollar amount. And while you are thinking of the answer, I just have a quick question. Dr. Spafford, you mentioned that 23 Ph.D.s in computer security in the last three years. Do we know the country of origin of those 23 Ph.D.s?

Dr. **SPAFFORD.** Well, those 23 were from—as I said, from those 24 institutions. There may be more nationally. The numbers I have indicate that somewhere between g and b are U.S. citizens.

Chairman **BOEHLERT.** Which means the other——

Dr. **SPAFFORD.** The other——

Chairman **BOEHLERT.**—h or b are not. The point is that there are some people suggesting, I think, unwisely, that we cut off all student visas and we close our universities to so-called outsiders. And, boy, that would really be biting off our nose to spite our face and deny us of some very, very important valuable resources. No one questions, I certainly don't, the need for the INS to tighten up and to get the people who shouldn't be here and to make sure the people who overextend their stay are sent back from whence they came. But to close our doors in the university community, to foreign-born nationals, would just deny us of something that is very important.

Dr. **SPAFFORD.** Sir——

Page 127 PREV PAGE TOP OF DOC

Chairman **BOEHLERT.** Yes.

Dr. **SPAFFORD** [continuing]. If I may——

Chairman **BOEHLERT.** Go ahead.

Dr. **SPAFFORD** [continuing]. In computer science, in general, and computer security, specifically, a very large percentage of the contributors at the faculty level and at the senior graduate student level are not U.S. citizens. But as a result of our educational system and the freedoms we offer here and the opportunity, they stay and become a very important as part of our scientific enterprise.

Chairman **BOEHLERT.** And major contributors.

Dr. **SPAFFORD.** Very much so.

Chairman **BOEHLERT.** Well, then let us go to the focal point and dollar. And I will go right down the Panel. Dr. Wulf.

Dr. **WULF.** Because the community is so small, it seems to me that we don't need a lot of dollars at the moment. I would like to see us build another ten centers, maybe operating at $10 million a piece. But if you gave us $100 million today, I am not sure we could spend it. What is really important is that this support build up over time and there would be some kind of guarantee that it is going to be there. That is what it takes to attract people into a research area.

Page 128 PREV PAGE TOP OF DOC

I think, at the moment, because of the sense of the country, we could get some people who are doing research in other areas, some very fine minds who are doing research in other areas, to focus on the subject so we could move some over. We could, perhaps, build up a little bit faster than you might otherwise think. But——

Chairman **BOEHLERT.** The focal point part of the question.

Dr. **WULF.** You mean, where?

Chairman **BOEHLERT.** Yeah. Where. I mean——

Dr. **WULF.** Yeah. I—let us see——

Chairman **BOEHLERT.** When everybody is in charge, nobody is in charge.

Dr. **WULF.** Well, that is what is wrong with PDD–63, in fact. I said in my oral testimony that I thought about this and I tried to map what we need onto the existing agencies, and I don't find the match. And so the notion, for example, of giving it to the new Homeland Security Office, I find quite attractive.

Chairman **BOEHLERT.** Dr. Spafford.

Dr. **SPAFFORD.** I am not certain that a single focal point is going to be the best approach for two reasons. First of all, information assurance, information security, isn't well-defined as to what that encompasses. It includes not only computer science research, but communications research, criminology, psychology, issues of ethics, management, economics, and a number of other issues. It is not clear that any existing agency has the breadth of view that is going to address all of those.

Page 129 PREV PAGE TOP OF DOC

It is also the case that we have both short-term and long-term research interests, and the nature of agencies supervising funding in those areas tends to be rather different.

I will say that, again, talking to my colleagues, the agencies that they have found the most responsive, in terms of funding for what they want to do, have primarily been NSF, NIST, and the National Security Agency, with NASA being a fourth agency. Each has a slightly different focus and has been supportive of what has been done. As to what we should do from here, perhaps a coordinating body to make sure that the research that is spent by these agencies is directed in the right places, but I am not sure I would advocate a single focal point.

Ms. **BENZEL.** Yes. I certainly agree we need a focal point. In terms of where it should be located, I believe we really need to look at having some sort of a new organization. And this further may require changes in legislation and law so that we can create a new organization which can benefit from some of the best and the brightest minds in industry, academia, and government. We need to have a true partnership so that the minds can come together and really focus on creating an agenda.

I think coordination is extremely important. As you have indicated, it is difficult to know just exactly what the extent of information security research is that is going on in the country today. Doing this type of coordination and setting an agenda and a road map, which can cover both near, mid, and long-term research, will require a significant investment. So while Dr. Wulf has indicated that it may not be a large increase in funding directly to the research community, I think we need to look at some significant investment in creating coordination, cooperation, and partnerships. I hope that has answered the question.

Page 130 PREV PAGE TOP OF DOC

Chairman **BOEHLERT.** Thank you. Mr. Weaver, do you have any thoughts on that?

Mr. **WEAVER.** I am struck by the proverb that is on the back wall, there is no vision—well, if there is no vision, then people perish. Just as I think where this Committee is going to step forward in the future and take a more prominent role in science and technology, you need that vision. That vision comes from research and development and new technology. I see this as a bigger role for you.

Our focal point, with the Treasury, within the Treasury and the White House, is Dick Clark, very streamlined, very fast-track, and we know exactly what we need to do. That is where we go to.

Chairman **BOEHLERT.** Thank you very much. Mr. Hall.

Mr. **HALL.** I would note that the lack of vision is behind the Republicans part of in this. And we quote Tennyson.

Chairman **BOEHLERT.** No. It is a matter of—it is not party affiliation. It is a matter of positioning. It is on the left.

Mr. **HALL.** There you go. But I thank you for your testimony. It has been great. And I look forward to this. As I have done the President's message after the attack, that I have reread and read his speech and, while he delivered it very well, rereading that speech is really an inspiration. And for those of you who don't have a copy of it, I suggest you get it, because, as a Texan, I have never really been much of a New Yorker, but I am a New Yorker now. And I think his speech brought us all together.

Page 131 PREV PAGE TOP OF DOC

I think, Ms. Benzel, you pointed out that we don't fully understand the vulnerabilities. And that, of course, is a good statement. And, Dr. Wulf, you talked about the Maginot Line and I never did know if they built that because the Germans had a Siegfried Line or which one came first, but neither one of them did the job they were set out to do.

Would it have been possible 30 years ago to have built a maginot line that—and how would we have done it? And we can look back for a minute, but I want to ask you a follow-up question in a minute—what can we do from this point forward to set up some type of defense?

Dr. **WULF.** Back before computers were networked with each other, it is, I think, conceivable that you could have protected the information with a single computer with a perimeter defense.

Mr. **HALL.** Would the successes have been slower and surer or would it have been an easy thing to have done at that time in the initial thrust?

Dr. **WULF.** Well, clearly it wasn't an easy thing, no. It was not an easy thing to do. We, in fact, tried to do it. People tried to build systems that were completely secure and we have never managed to do it.

Mr. **HALL.** You know, businesses try——

Dr. **WULF.** But, now that we have got networks, the whole concept is just bankrupt.

Page 132 PREV PAGE TOP OF DOC

Mr. **HALL.** Then I think, Ms. Benzel, I would like to know—we need to get right down to how much money it is going to cost because that is going to be, in the final analysis, a major factor that we put in the computer. And I doubt that you all have had an opportunity to make that study. It is not your duty to. It is your duty to tell us what is needed and what is needed, if we provide it, what it will do for us.

But do any of you have any idea of the amount? You are talking about R&D, Ms. Benzel, and R&D and cooperation. And Bob Weaver been a living example of that type of cooperative thrust. Can you put a price tag on it?

Ms. **BENZEL.** Well, I am not prepared to actually put a number on it, but I would say that I believe it needs to be in order of magnitude above what it currently is.

Mr. **HALL.** And would it be cost attractive—well, like water, we do a water deal. We think we get back seven bucks every time we build a lake. The Chairman doesn't help me build lakes anymore, but he would if it was needed.

Ms. **BENZEL.** Well, you know, cost always needs to be weighed against what the risks are. We are proposing long-term R&D. And so long-term R&D means there needs to be some failures in there. And so

the payoff certainly would not be on the level of the water systems. I tend to, in my research laboratory, try and strive for a 30 percent success rate in terms of doing technology transfer from the research into technology.

Page 133 PREV PAGE TOP OF DOC

Mr. **HALL.** Is that a reasonable rate?

Ms. **BENZEL.** It is a difficult and ambitious number, to be honest. And so it may be even lower than that.

Mr. **HALL.** Who should carry out the work? If if we decide on what level of resources we do need, who or what entity should carry out the work? The Chairman asked that question and I don't think he got an answer to it.

Ms. **BENZEL.** Well, I would actually advocate that perhaps we need to have a new form of an organization which can have a board or a steering committee made up of industry, academia, and government. I, Dr. Spafford, and several of us have been involved in the discussions in the previous Administration and the OSTP about creating a new institute for information protection. Clearly, that did not come to fruition, but there were many ideas in that exercise that we may want to go back and look at.

Mr. **HALL.** And my final question to Dr. Spafford, you mentioned the legal impediments, and I think that is certainly an important aspect here. We face that, you know, in trying to solve health problems and things like that. Threats from patent holders; what is the answer to that? And, if you would, I don't ask you to tell me who the Senate sponsor is, but just tell me the number of the bill. I would like to know what it says and what it does that is restricting our use and restricting encouraging men and women of your pursuit to be protected from that legal threat that hangs over you on almost everything today.

Dr. **SPAFFORD.** Well, sir, as far as patents go, that is a complex issue and I am——

Page 134 PREV PAGE TOP OF DOC

Mr. **HALL.** Yeah.

Dr. **SPAFFORD** [continuing]. Not certain I can give you an answer right away. I don't know how frequent this is going to be, but the idea of patenting software and algorithms is a contentious one within the computing community, some who are very much in favor and many who are very much opposed, some who question whether it is even consistent with the intent of the Constitution.

What is happening is, as we do research that may make use of algorithms of concepts in computing, we find that we may stray into territory where patent has been asserted. And we don't have the resources or the time to attempt to contest those. I don't know a good solution, but that is the origin of the problem.

Your second question about the legislation, there are two that are very obvious to us. One is the Digital Millennium Copyright Act, which was passed several years ago——

Mr. **HALL.** Uh-huh.

Dr. **SPAFFORD** [continuing]. And the provisions of that that make it against the law for us to do any research that might be used to circumvent a copyright protection. Well, those are security mechanisms. And if we are going to understand how they work or how to build better ones, we need to do that research. But it gives a right to commercial entities to bring lawsuits against us and some researchers have been threatened with that. Others have been arrested. That is going to be an ongoing problem.

Page 135 PREV PAGE TOP OF DOC

The new legislation has not yet been introduced, but a draft bill has been circulated. It is to be introduced into the Senate Commerce Committee. The USACM has written a letter on this. We will be happy to share it with you. And——

Mr. **HALL.** I would like to have it and like to make it a part of this record, Mr. Chairman.

Chairman **BOEHLERT.** Without objection.

Mr. **HALL.** And my time, Dr. Spafford, has expired and I thank you.

Dr. **SPAFFORD.** Okay. Thank you.

Mr. **HALL.** And I think what you are saying is the same thing Ms. Benzel is saying. R&D—you know, companies have forever cranked their depreciation back into R&D and that has been enough. But it is not enough in a day like this and a thrust like yours. I thank you and I yield back my time.

Chairman **BOEHLERT.** Thank you. Chairman Smith.

Mr. **SMITH.** Given the critical importance of cyber security to the private sector, why isn't there a greater effort on the part of the private companies and agencies to invest more and be more active in this area?

Page 136 PREV PAGE TOP OF DOC

Ms. **BENZEL.** Is that——

Mr. **SMITH.** Yeah.

Ms. **BENZEL.** The question from industry's perspective—consumer industry has been very slow to adapt security. What sells continues to be ease of use and performance. And so it is difficult to get people to take the security seriously. So I would have to bring that up.

Secondly, when we are really talking about these critical infrastructure issues, it is not clear who is going to buy it, you know. As a software vendor, I need to create something that I can sell to someone. But the critical infrastructure really falls into that area that is in between. It is those interdependencies that are in

between. And most of our consumer technology and information security is really aimed at a single owner/operator. I can sell it to an insurance company, to State Farm. I know how they will use it. But when we really talk about the insurance company trying to work with the financial systems and with the Health and Human Services systems, that is where it is hard to understand where to put it. And so the investment really isn't there because of the consumer market.

Mr. **SMITH.** Dr. Wulf.

Dr. **WULF.** I think you need to make a distinction between industries like the banking industry where, in fact, a substantial amount of effort has gone into securing their own transactions versus the shrink-wrap software industry, which Ms. Benzel was talking about. Frankly, it is cheaper for the shrink-wrap industry to write a contract with the purchaser which absolves the company of any responsibility for bugs, whether they be security bugs or other kinds, than it is to do the research and implementation to make quality software.

Page 137 PREV PAGE TOP OF DOC

Mr. **SMITH.** So I am trying to think of the balance there. And I appreciate Ms. Benzel who says let us bring everybody in the private sector, industry, government. Should some of this information be classified that we develop in terms of developing better ways to protect ourselves from cyber terrorism? Dr. Spafford.

Dr. **SPAFFORD.** That brings us back to the point that we need the data and the access to be able to do the research. And with a significant proportion of non-nationals involved in our programs and the need to publish to be able to move academia along, classifying information is very problematic, which gets back to the Chairman's original question about the focal areas for funding. There are different kinds of research necessary.

Mr. **SMITH.** Does the development of the exceptional software that works best and then having a whole industry, such as the way we keep track of and move electricity around the country—and so there tends to be a selection of software to do that across the country—does that make us more vulnerable or in any other areas where we tend to depend on similar software, even our home computers? It would seem would make us more vulnerable.

Dr. **SPAFFORD.** We have pretty much standardized now, and the same software that people are using at home to browse the web and keep their recipes are also being used to run the weapon systems on new aircraft carriers and protect our nuclear secrets. And those are the same ones that you keep seeing a blue screen and getting viruses on. So having a monoculture is a great problem when we standardize on the same underlying technology throughout, and that is based on cost rather than on its performance and function.

Page 138 PREV PAGE TOP OF DOC

We need to be much better at deciding that security has a cost margin that we can apply and acquisition and be willing to invest, in some arenas, in more secure software. And we haven't been doing that to date.

Mr. **SMITH.** As I mentioned down there, I am a farmer, and if our electricity goes out, we have got a

generator ready to hook up. And if our generator goes out, then we milk the cows by hand. But how about backup systems? When you talk about being creative in terms of looking at this problem, is there such a thing as a backup system, Dr. Wulf?

Dr. **WULF.** You will notice that—I think it was Shearson who was on the 35th Floor of the World Trade Center and managed to get all but six of their 3,500 people out. And on Monday, when the stock market opened, they were up and running again. It is an odd thing that the preparation for Y2K probably saved a lot of the companies in the New York area from a severe downturn.

That said, there isn't really a backup for the broader system, the kinds of infrastructure that might be taken down by a cyber attack. And there is no——

Mr. **SMITH.** Mr. Chairman——

Dr. **SPAFFORD.** There is no company which profits from that.

Mr. **SMITH.** Terry, did you have a——

Ms. **BENZEL.** Sir, I just had one brief comment, which is, putting in backup systems may, in themselves, introduce new vulnerabilities. So I think what——

Page 139 PREV PAGE TOP OF DOC

Mr. **SMITH.** Yeah.

Ms. **BENZEL** [continuing]. Dr. Wulf was referring to, a backup to the Internet itself and fault redundancy there would actually, perhaps, create new vulnerabilities that could make it worse.

Chairman **BOEHLERT.** The Chair——

Mr. **SMITH.** Mr. Chairman, just let me finish up by saying it seems to me that over the short run we don't want to cut off these foreign students that are adding so much to our research and knowledge effort, but in the long run, we have got to do a better job of encouraging more American students to get interested in and to pursue this endeavor. Thank you.

Chairman **BOEHLERT.** Without objection, so ordered. There is unanimous consent. That is something we can all agree on. Just before I recognize Ms. Rivers, just let me ask you, Ms. Benzel, you are in business to sell a product that people are going to buy. Prior to September 11, I think featuring security as one of the selling points drew a muffled yawn. They just wanted to know how fast you could go and how cheap they could get it. Wouldn't you suggest that maybe the climate has changed now, which would serve as an inducement for the private sector to invest more in R&D to make systems more secure?

Ms. **BENZEL.** Well, I certainly do believe the climate has changed. And, in fact, our stock is one of the few that has closed up consistently since the market reopened. We are thrilled to see that. But on a more serious note, we have to balance that with the economic realities that have occurred prior to September 11 and since September 11. And so our investment dollars are smaller today, but we do see that the mood has

changed. And, as you say, our technologies have been some of the most secure technologies, but we have lost out, in fact, in everywhere except for the DOD to an Israeli company that sells a faster, higher-performing technology. And——

Page 140 PREV PAGE TOP OF DOC

Chairman **BOEHLERT.** The Chair recognizes Ms. Rivers for five minutes.

Ms. **RIVERS.** Thank you, Mr. Chair. I have so many questions that I am going to have to widdle down here. I don't know if we are going to have a second round. Probably not. But I may offer some in writing. Just to follow up on something the Chairman just said—that after September 11 there was a trend toward greater security. I think that is true when one looks at governmental infrastructure. But I have also heard the opposite, a trend away from the ability of individuals, private citizens, to use techniques like cryptography, stenography, other kinds of ways to keep their transactions private.

And I am interested in knowing if the consumer sector is removed, whether that helps or hinders research. In other words, if we limit development of new techniques only to government use, are we going to see this —I have a university community and I have a fairly large security—computer security program. Their students are working on all kinds of things, not just limited to services toward the government. It seems to me that if we were to step away from private usage or private kinds of programming, that a lot of the research would fall by the wayside. Dr. Spafford, and, Dr. Wulf?

Dr. **SPAFFORD.** The problems that are faced, there is a broad array that go from the individuals who need to protect their banking information on their home machines, to universities protecting proprietary information and all kinds of business needs. So that is a very large market and one that we need to build into the commodity products that those people use on a regular basis, because the majority of them don't understand security. And so we have to find ways to get it into their product domain.

Page 141 PREV PAGE TOP OF DOC

Ms. **RIVERS.** And make it easier.

Dr. **SPAFFORD.** Yes. And make it easier, seamless, and not observable. That is critical for what we do. So we really can't remove them from the equation because they are part of the network. They are part of the overall fabric of what we do.

Ms. **RIVERS.** But the Attorney General right now has been making noises about eliminating private use of cryptography, though I don't think anyone has produced any evidence of it being used in the attacks that we just experienced. Do you have a comment on that?

Dr. **SPAFFORD.** The short answer to that is it is not technically feasible at this point without perhaps destroying the online economy and much of what we do with our computers. It simply has not been shown that there is a technology to do what has been suggested. And furthermore, it is not clear that that would have made any difference in the events that we have seen. So the official position of the USACM on this is

that it is not feasible. We have another letter that we will introduce as part of the written testimony.

Ms. **RIVERS.** Dr. Wulf, do you want to follow up?

Dr. **WULF.** Let us see, I would just say ditto to what Spaff just said. I would only add to that that as we think through these issues, there are going to be many who call for reduced civil liberties in one way or another, particularly with respect to privacy. And I think one of the directions we must look is technologies which increase security without giving up civil liberties. It is just like a metal detector is less intrusive than a pat-down search and probably more effective as well. I think there are technologies we should look for that have exactly that property.

Page 142 PREV PAGE TOP OF DOC

Ms. **RIVERS.** Ms. Benzel, one of the things that comes up periodically when we talk about security systems is the need for the government to have a back door, a way to crack the security system, so in the event of some sort of criminal act, there is a way to get to the information. How does your company feel about that and how do your customers feel about that?

Ms. **BENZEL.** Well, the customer answer is quite easy to answer. The customers are emphatically against that. We work very hard to comply with all U.S. regulations in terms of export and use of cryptography. We are able to work with the government authorities under proper circumstances. We have engaged actively in this debate, both in my former company, Entrusted Information Systems, and as part of PGP Security. And I really echo the comments of Dr. Wulf and Dr. Spafford. We need to move away from that debate in terms of limiting civil liberties for the customer's space.

Ms. **RIVERS.** I want to go back to legal impediments, in particular, the DMCA, which many of us don't realize. I think that was passed out of the House twice on voice votes and was never really fully debated or on a rollcall vote. Dr. Spafford, can you talk about why, well, how do I want to put this, why, how this provides an impediment or why this represents an impediment? What is happening to people? And I think I would point to the two researchers from Princeton and one from Europe that couldn't present their materials at the Naval Research Lab, Skylerov from Russia, who was arrested even though his work was not done in the United States and broke no law. Can you help people understand why this is a real problem?

Dr. **SPAFFORD.** The problem is primarily one of new technology. A number of firms produce intellectual property, whether it is music, video, pictures, books, and they want to provide these over the network to consumers. That is good. However, this is very new. Commercial use of the Internet itself is only seven years old. And so we haven't quite developed the economic models yet, the understanding of how best to do this. Those firms are very concerned about their information being taken and so they put in very primitive protection mechanisms that are easily circumvented. So to address that the DMCA creates legislative remedy so that if someone attempts to circumvent that protection or develops methods that can be used to circumvent those protection methods, they can be either charged with a Federal felony or they can be sued by the holders of the technology.

Page 143 PREV PAGE TOP OF DOC

Ms. **RIVERS.** Even if this is part of what would normally be a fair use optimization or as——

Dr. **SPAFFORD.** For any reason.

Ms. **RIVERS** [continuing]. Part of research——

Dr. **SPAFFORD.** For any reason.

Chairman **BOEHLERT.** The gentlelady's time has expired.

Ms. **RIVERS.** Thank you.

Chairman **BOEHLERT.** We have good attendance, so I want to give everyone a chance. So thank you very much, Ms. Rivers. Just one quick question. Is this CERIAS—is that the way you pronounce it?

Dr. **SPAFFORD.** Yes, sir.

Chairman **BOEHLERT.** I love that. It is great.

Dr. **SPAFFORD.** We are serious about security.

Chairman **BOEHLERT.** Which New York State program are you talking about?

Page 144 PREV PAGE TOP OF DOC

Dr. **SPAFFORD.** The Center for Assurance at Syracuse University.

Chairman **BOEHLERT.** All right. Thank you. That is what I thought. The Chair is pleased to recognize Chairman Bartlett. I just wanted to get a plug in.

Mr. **BARTLETT.** Thank you very much. In thinking about a focal point for this activity, I might suggest looking at our weapons labs shrouded in secrecy and two of the three are isolated in a New Mexico desert and mountains. But I know from a recent visit that they have an enormous capability, and I know that they are very aggressively pursuing hiring the best of the best computer people that come out of our schools. And I would suggest that this kind of a mission is something which fits with their overall mission. That is, protecting us.

I would just like to ask you what, in your judgment, is the weakest link in the overall system? That is, what places are most vulnerable and would be most damaging to society if disrupted? We have been talking generically about our vulnerabilities. I would just like to get your estimate as to what is the weakest link, that is, the place that, if disrupted, would hurt us most?

And, secondly, a companion question. To your knowledge, has any evidence turned up during investigation of recent events which would indicate that there are threats to us in these areas being contemplated?

Dr. **WULF.** Well, let me take a hack at the—excuse me, that is a computer term—at the first of those questions. And I will just warn you, I am not going to answer the question because, to the best of my knowledge, there does not exist a well-developed methodology for answering that question. It is—in fact, the first thing that I did at the National Academy of Engineering, after the 11th, was to begin to put together a panel to try and develop such a methodology.

Page 145 PREV PAGE TOP OF DOC

The notion of risk, as I am sure you realize, takes into account both the probability of something happening and the consequences of it happening. And to apply that systematically to all of the kinds of things that could potentially happen, simply hasn't been done. My understanding is that the FBI has been—was charged five years ago with doing that, but according to the most GAO report that came out just a few weeks ago, that has not—either it has not been done at all, or at least it hasn't been published.

Mr. **SMITH.** For instance, I was thinking, though, is it our power grid, is it our communications, is it our financial market? What, in your judgment is the most vulnerable? Yes, sir. Dr. Spafford.

Dr. **SPAFFORD.** Well, sir, I would say that they are all vulnerable. It depends on how they are attacked as to what the effect might be. But, as Dr. Wulf said, we don't really have a good evaluation there to be able to say how weak it is or what kinds of attacks might occur. And this actually leads to an answer to your second question about knowing about the existence of a threat. There very certainly is one. It is not necessarily an organized threat from a nation state. We have an ongoing and increasing level of malicious behavior by criminals, vandals, idealogs, and others, who are attacking our systems on an ongoing basis as background noise. And that is continuing to grow, doubling—more than doubling every year.

Ms. **BENZEL.** Well, again, I mean, the first question is very difficult to answer without understanding what kinds of threats we are talking about. I could say somewhat flippantly, you know, our weakest link is anywhere that a control system computer is connected to the wide Internet. And so any control system control computer, which controls a critical infrastructure, be it power, water, finance, health, human services—if it has somehow connection to the Internet, then that is a weak link. But that is a difficult question.

Page 146 PREV PAGE TOP OF DOC

In terms of investigation in current threats, I would defer to Mr. Weaver.

Mr. **WEAVER.** The areas that have been previously identified by Presidential Decision Directive 63, as highlighted by everybody here on the Panel, are the areas of concern. To probe deeper into that may be more suitable, at your convenience, in a more sensitive setting, to specifically highlight a great gray area of concern. But as I see it from the New York angle, there is two areas that this is breaking down into—the IT area and the physical security area. And they are both going to come together now. Everything from dumpster diving to hacking an intrusion or physical disruption of the actual location itself. These two areas are going to—you are going to see more merging together. And that is a highlight that I could point to your

attention.

Mr. **BARTLETT.** Thank you. Mr. Chairman, unless we are careful, I think that our greatest strength could become our greatest weakness because we are so dependent on computers and the net, which is one of the reasons we have been so effective. Because we are so dependent on it means that we are, of all the nations of the world, most vulnerable to this kind of warfare.

Chairman **BOEHLERT.** You are exactly right.

Mr. **BARTLETT.** And I think that the kind of focus that you are emphasizing here is way past due. Thank you.

Chairman **BOEHLERT.** Thank you very much. And Dr. Wulf mentioned in his testimony the Joint Chiefs of Staff military exercise, Eligible Receiver. Those exercises were conducted a couple of years ago, and they had a team to see if they could disrupt it. They had to cancel the exercise. It was disrupted just like that. And so this is serious business we are about. And I am pleased to now recognize someone who can add to the dimension of the issue, the distinguished gentleman from North Carolina, Mr. Etheridge.

Page 147 PREV PAGE TOP OF DOC

Mr. **ETHERIDGE.** Thank you, Mr. Chairman. And I want to follow that line of questioning also because I think we are onto an issue that is so critical and so focused when you think in terms of the Internet interlinks. And I thank the Chairman for having this meeting and for the witnesses that we have. You have been sharing some very insightful information to us about our computers' infrastructure.

But when we think about the Internet, it has become such a powerful tool that I don't think any of us ever recognized seven years ago or so when we started, it would be as powerful as it is today in interconnecting so many things, from commerce to all kinds of technologies. And most of us in this room carry some kind of gadget around with us that hooks us into the Internet. And so we are dependent on it in a lot of ways.

That being said, as we use the Internet to collaborate, interact all around the world. Not just here, but literally around the world, the power of the Internet lies not only in our ability to communicate, but also our ability to link so many systems together as you have been talking about already. That being said, as we talk about linking all those systems, many of them, as has already been indicated today, are critical systems. They can be linked in remote areas, for that matter, if you have a wireless system.

My first question to you is, what are the current and potential threats as we look at this cyber security? And I know I am following on some ground that has already been covered, but I think it is important. How equipped are we to deal with it? And, secondly, how can universities, industry, the Federal and state governments, work more effectively together to deal with network securities beyond—you know, we talk about the homeland securities, but I think that is the critical patch of how do we do the seamless link to help deal with this issue?

Page 148 PREV PAGE TOP OF DOC

Dr. **WULF.** We held a meeting at the Academy on the 26th of September and invited a large number of very senior scientists and engineers and current and former government officials. And one of the points that was repeatedly made, as we talked about what we should be doing, was that the goal of terrorists is to terrorize. And in many ways, exposing the range of vulnerabilities that we have is perhaps one of their greatest weapons. So if you—when you ask this question of where are we most vulnerable, the answer is, I think, that we are vulnerable in so many places, and that is so powerful in terms of terrorizing. I think our greatest vulnerability is in our psyches in some sense.

Dr. **SPAFFORD.** I would say, to your second question, that one of the things we need to do is to make all of the potential stakeholders aware that it isn't their problem. It is all our problems. So when we have government agencies who won't talk about their systems or their data or otherwise because it is theirs, they are depriving the others of being able to address some of those issues.

The same way when industry won't talk about things because it might destroy their market, they are preventing others from finding ways of interacting to solve problems. So we need to find ways to break down those barriers and all of us take ownership of this as a joint problem area.

Ms. **BENZEL.** I very much echo Dr. Spafford's remarks. I think that we really need to find innovative ways in working together. And some of the specifics is, we need to have new approaches to intellectual property so that we do feel comfortable sharing this information. We need relief from certain regulations so that industry can serve in an advisory role to government. We need to find a way to create a true board of industry, academia, and government, which can set the research agenda. And, perhaps, we should look at some sort of a third party clearinghouse or virtual think tank which could collect all of this information and animize it or cleanse it up enough so that we don't have to be worried about the direct sharing.

Page 149 PREV PAGE TOP OF DOC

Mr. **WEAVER.** Certainly, this is like an advertisement for the Task Force. I would promote and suggest and recommend that the model that we have in New York is truly a model that responds to the needs of the community. It moves at the speed of corporate. It meets their needs. It gets them what they need. It is a more a systemic approach that addresses the underlying issues. It is not—it is more in the prevention mode, proactive mode, education and training, the risk management part of corporate world, getting in there ahead of time, trying to prevent or ward off these things. If you need help, call us. We will be happy to help you, but we prefer not to operate in a crisis response mode. You don't make money. It is too stressful for all of us. Let us try and head these things off ahead of time.

The network that we have established, I think, is a good model, a good model maybe for the Nation. Certainly, with the leadership of this Committee paying particular focus to it, and with the support of this Committee, I think our finest hour is ahead.

Mr. **ETHERIDGE.** Thank you, Mr. Chairman.

Mr. **BARTLETT** [presiding]. Thank you very much. We are recognizing members in the order of their appearance, and that means Mr. Grucci is next.

Mr. **GRUCCI.** Thank you, Mr. Chairman. Dr. Wulf, you had mentioned earlier that you were appalled at the lack of commitment there was to cyber terrorism as compared to other terrorists' activities and the amount of commitment that was made to them. Have you seen any change in that since the fateful day of September 11?

Page 150 PREV PAGE TOP OF DOC

Dr. **WULF.** It has been too soon. I have not seen anything.

Mr. **GRUCCI.** What recommendations would you make to help us understand what we need to do to assist in that area?

Dr. **WULF.** For one thing, as you know, the National Academies operate under a charter from the U.S. Congress to provide advice to you. We are pulling together a committee, as I speak, to try and prioritize R&D areas that would be appropriate to address the full spectrum of threats to the Nation, not just cyber, but including cyber. We will, of course, make that available to you as soon as we can.

We have also written a letter to the President, to Governor Ridge, and to the Congressional leadership, including of this Committee, offering our services in any way that we can be of help. And as you know, and as your staff knows, we have typically operated under some rules and regulations—self-imposed rules and regulations on what we would do. We have said those are off the table. Whatever you want us to do, we will do.

Chairman **BOEHLERT** [presiding]. Let me, Mr. Grucci, interrupt just 1 second. We didn't have to initiate the draft. You enlisted, and we really appreciate that.

Mr. **GRUCCI.** Thank you, Mr. Chairman. Dr. Spafford, you—I think it might have been you that suggested in your testimony or said in your testimony that there are some kinds of programs that are on my laptop computer that these little chubby fingers are pecking away at a keyboard on is the same kinds of programs that pilot and man our mightiest warships and run our defense systems and probably our water supply systems, etcetera, etcetera. Is that a good thing to have that—to have no separation between them two?

Page 151 PREV PAGE TOP OF DOC

Dr. **SPAFFORD.** I don't believe that it is for several reasons. The first is that that software was not developed for those applications. And, in fact, on the license it explicitly disclaims any liability for fitness for that kind of use. That software has been developed generally for business and home use and includes many features for that lowest common denominator of use to be able to sell it.

The second reason that I don't think it is particularly good to use in those environments is because it is the same software that is available everywhere. And one vulnerability discovered in a university lab or in a small company can then spread throughout government systems and be damaging.

Mr. **GRUCCI.** I tell you that testimony has given me a great deal of respect for these two fingers, I will tell you that. I have a company in my district by the name of Simple Technologies. The founder of it, Jerry Schwartz, was the founder and inventor of the bar coding system. He had talked to me shortly after the tragedy has happened and said that there is great technology out there, not only that his company has, but many others that are working on it. And you have got to forgive me because I am not as computer literate as I would love to be.

But he used the term "pdf" files where they can imprint pictures on things like airline tickets so that when you put an airline ticket through a scanning machine, you would identify the actual holder of the ticket to be the actual person that is boarding the airplane. He also suggested that that kind of technology exists in doing things like getting into records and files in very sensitive areas of computers. I assume that you are familiar with those things. And if you are, can you elaborate on where that technology is and is this a good avenue for us to pursue?

Page 152 PREV PAGE TOP OF DOC

Dr. **SPAFFORD.** There are a number of technologies. I believe you are referring to an area known as biometrics, which includes being able to identify people by physical characteristics—picture, fingerprint, and otherwise. These are technologies that do work and they are useful in some environments. In others, they require a great deal of background information to work properly. They have, in some cases, a failure rate, generating false replies, false positives, for individuals. They are not ideal in every circumstance, but they are being examined to be used more in high-security applications.

Mr. **GRUCCI.** Thank you. My last question, if I may, Mr. Weaver—and if this is information that you choose not to share in this environment, I would truly understand. But the events of September 11 and what it has done to your operation, has it weakened your ability to be able to respond? And, if so, what would you suggest we do for you immediately to help you get back to the level of response that you ought to be at?

Mr. **WEAVER.** I would say because we were virtual, our most important asset was our personal resources. The equipment was replaceable. We did so through the help of our corporate partners and our government partners, the National Institute of Justice, ROME Labs, right there on top of it. We are twice as strong now because people are paying attention to this issue. But there is much work to do. But we were not based on a building and the equipment in the building. And this virtual concept gives great flexibility and that is important. And it also makes you redundant and robust and survivable. That is what you need. You need to be open for business tomorrow, and that is what we did.

Mr. **GRUCCI.** Thank you for your answer. Thank you, Mr. Chairman.

Page 153 PREV PAGE TOP OF DOC

Chairman **BOEHLERT.** Thank you very much. And one of the things, Mr. Grucci, I intend to do is, as soon as we can work it out with Mr. Weaver and his team, is to have this Committee to have an opportunity to visit with the New York Electronic Crimes Task Force and to hear the presentation that I was privileged

to hear. And it is exciting and the work you are doing is extremely important. And, as you indicated, there is a heightened sense of awareness of the importance of your work. So keep up the good work. The Chair is pleased to recognize the distinguished lady from Texas, Ms. Jackson Lee.

Ms. **JACKSON LEE.** I thank the Chairman very much. Let me applaud the Chairman and the Ranking Member for this hearing. A few days ago I was talking to constituents in Houston and speaking to them about the importance of the Science Committee and its impact in the energy legislation that we passed, I guess, a couple of weeks ago. Your leadership, Mr. Chairman, and the Ranking Member now have put us squarely, if you will, in the midst of another very important topic that I believe will maybe be our finest hour.

I would hope this hearing would cause us to look at the bipartisan legislation, I think, that has been simmering in this Committee for a period of time, and hopefully we will have the opportunity to look at it closely and, again, put our mark on a very important challenge of this Nation.

Might I just for a moment speak to the H1B issue because I wore that hat as the Ranking Member on the Immigration and Claims Committee. And I don't want to say I told you so, but I think Chairman Smith—I know he is not here—one of the amendments that I had was to increase the training opportunities for Americans. I am not, in any way, disregarding the importance of our international talent, as it regarded writing software and providing the opportunities for our population to be engaged at the very highest levels of technology. And so I hope maybe as we look at these visas or our future we will include that responsibility.

Page 154 PREV PAGE TOP OF DOC

Let me also say just a few days ago we worked on the anti-terrorism bill in the Judiciary Committee again. And I would like to say to those of you who are concerned about civil liberties, we were very careful to try to distinguish the issue of content versus the identification of the email holder. And I hope that pleased you and I hope that as the bill is moving to the House, the good bipartisan work of a very unique Judiciary Committee that voted 36 to 0 on this bill, will not be upset.

But, Dr. Wulf, I have a very important question for you, very important. You are on leave from what university?

Dr. **WULF.** Oh. From the University of Virginia. And I know that you are a graduate of that.

Ms. **JACKSON LEE.** I was. I thought that would add to the hearing and I wanted to make sure you made that very clear.

Chairman **BOEHLERT.** So pleased the gentlelady brought that to our attention.

Ms. **JACKSON LEE.** Let me—and I know the time is going—let me ask this question. Dr. Wulf, I think you mentioned it as I was coming in. I am sorry I was delayed with other business. But we mentioned Y2K. And I believe the enormous experience that we had with Y2K, I think we should note that we were shocked ourselves at how we managed to move into the next century. And what I would like to know is what do you

think private industry learned from that? And would you also answer the question with respect to the Homeland Security Cabinet position that has just been appointed—what will we need to add to the responsibilities of Governor Ridge and, of course, the new terrorist czar that has come in from the Defense Department, retiree, to put us on track for these important responsibilities?

Page 155 PREV PAGE TOP OF DOC

Dr. **WULF.** Let us see—several things about the Y2K. First of all, it provided the opportunity for most companies to critically examine their software in a number of ways. They didn't just look for the date calculations. Second, they—many of them got very much more serious about backing up their data and providing backup systems in remote locations so that they could resume business if something did go down.

I must say, as a computer scientist, I was a little bit—I wish that Y2K had bit us just a little bit. I think we would have been much more sensitized and done a great deal more a lot sooner. One of the things that we absolutely do not know is what the interdependencies are between these various systems. When people ask me about what are we vulnerable on, we can talk about water supplies. We can talk about building ventilation systems and lots of things.

The trouble—the thing that bothers me more than any of those individual things is the interdependencies between the systems because we have no idea what those are. And so what will be the overall impact of a particular attack is just totally unknown. If we had had a little bit of a bite in Y2K, we might have seen some of the ripple effect and might have understood that a little better.

Ms. **JACKSON LEE.** Well, clearly, with the Homeland Security Office, the interdependency research or component or how we are interrelated is very important.

Dr. **WULF.** That is right.

Page 156 PREV PAGE TOP OF DOC

Ms. **JACKSON LEE.** Let me quickly—I know that the light is on—ask a combined question, and I would appreciate the other members answering it, if I am indulged to ask the question. And that is the interrelatedness and the infrastructure question.

Particularly, I go back to September 11 and I use the FAA in particular, though I know that there are many things that we may see in the future. The infrastructure question and whether or not there was enough connectedness with respect to notification, computer notification, connectedness through the FAA infrastructure. Would anyone want to be able to just comment on how we could have done a better job in that enormous tragedy—how the infrastructure technology system could have helped us in that very terrible tragedy?

Ms. **BENZEL.** I guess I will take a cut at that.

Ms. **JACKSON LEE.** Thank you.

Ms. **BENZEL.** You know, the infrastructure and connectedness is both the positive and the negative. It also introduces the vulnerabilities. And, you know, in my testimony, I called for us to do a critical vulnerability analysis of our infrastructures. And what we need to look at is some of the near-term sort of operational models to make sure that that connectedness is there and the right information is flowing in the right time and across agencies that are involved. And, you know, my vision is that as we do this analysis from an operational model, we also bring in some of the experts in information security so that they can help us identify where the new vulnerabilities are being introduced as we move forward.

Chairman **BOEHLERT.** Dr. Spafford, did you wish to respond?

Page 157 PREV PAGE TOP OF DOC

Dr. **SPAFFORD.** Yes. I—very quickly. A problem with connecting too many systems together is the difference between data and information. We can have a lot of data flowing back and forth, showing air patterns and billing information and passengers, but being able to extract the information we need from that and get it to the right people to act at the right time is a much bigger problem than simply connecting the systems.

Chairman **BOEHLERT.** Thank you very much. It is the Chair's privilege to recognize——

Ms. **JACKSON LEE.** Thank you, Mr. Chairman.

Chairman **BOEHLERT** [continuing]. The distinguished gentleman from Michigan, Dr. Ehlers.

Mr. **EHLERS.** Thank you, Mr. Chairman. This is an incredibly important issue and it is much broader than most people realize. I mean, what has come out, and not all of it has emerged here, but in terms of the critical infrastructure that you referred to, Ms. Benzel, which is, in a sense, mostly hardware, we are vulnerable in the broad sense to a nuclear weapon exploded 130 miles above the earth's surface over central Kansas, let us say, which would cause no deaths, very little physical damage, but wipe out every computer in the country from the electromagnetic pulse. It would just overload the circuits and, boom, every computer other than the hardened military ones would be gone. That would be an incredible devastation for this country.

Page 158 PREV PAGE TOP OF DOC

But that physical damage ranges all the way down to someone with a pair of wire clippers. With 20 terrorists going into 20 switching stations with a pair of wire clippers, you can also shut the country down.

The other danger is what I think we generally think of with security is the—what you might call memory security, packet security, and processor security. And I suspect that is where you mean where you need the research. Right? Dr. Wulf, and, Dr. Spafford. I am interested in a couple of figures. And if you can't answer this, I would appreciate it if you could send them in by mail.

How much do we currently spend on research on security of the type that we have been referring to? How much does our Nation spend? And I am talking about the real basic research that is needed to formulate

solutions. How much are we, as a Nation, currently spending on law enforcement to try to deal with security breaches, security problems? How much are we spending in the Defense Department on military security? And I think you see where I am going here. I am trying to get our priorities in order.

Another question—how much is lost—how much do we lose annually due to the efforts of hackers and/or terrorists—sometimes it is hard to distinguish? But I read a figure last week that just the NIMDA and Code Red problems have cost several billion dollars to the American commerce. I don't even know if there are figures available, but I am curious how much we lose annually.

And what I am really getting at is, if, in fact, we are losing the billions of dollars that we suspect for this, and if we are spending billions of dollars on law enforcement, military defense, shouldn't the research funding be adequate to reduce those numbers? In other words, one—for every dollar spent on research, we may save a hundred thousand dollars in these other areas. I don't know if we will, but it would be interesting to see the numbers.

Page 159 PREV PAGE TOP OF DOC

And if you care, in responding to that, to make a projection of how much you could save in the future for research money spent now, I would certainly appreciate that. So I would be interested in any comments you would have and——

Chairman **BOEHLERT.** That is a tall order. But let me say this, that obviously they will respond immediately as you are able to, but I would like you to reflect upon that because we all would like to have the benefit of your wisdom. But I will tell you, it is a difficult task to pinpoint this.

Mr. **EHLERS.** Yeah. It is——

Chairman **BOEHLERT.** And Dr. Ehlers points out something that is very important. This is a clear example of what we don't know, we don't know.

Mr. **EHLERS.** And order of magnitude is all we need at this point. But a related question is, where would the research money be spent and which agency is best able to handle that?

Dr. **WULF.** Let me just make a comment about the amount lost. That is going to be a particularly hard number to get a hold of. It has been for both reasons of maintaining confidence of the consumer community and also, to some extent, a matter of legally being prohibited from sharing knowledge. That, for example, we don't know what the banking industry loses per year due to people hacking in. We all have heard stories. We have all, perhaps, gotten proprietary information from time to time, but that number is just not known.

Page 160 PREV PAGE TOP OF DOC

Dr. **SPAFFORD.** Some of the numbers depend on how you define research and the information security. There are places that will tell you that they are funding that if you ask them if they are involved and they will say, yes, we are and here is how much we are spending. But then if you say what are the projects? And

the projects that they will come up really don't have bearing on this. So we have some definitional problems.

The amounts that are spent sometimes are bundled into other issues. So in procurement of an overall system, there may be security research that is bundled in with that that is very difficult to separate out. I would conjecture, however, that the amount that is being spent by the government agencies, funding research, basic research that is going on in some of these areas, are likely in the hundreds of millions range and no larger. But without further research for figures that I don't have available, I wouldn't be able to say more than that.

Ms. **BENZEL.** Well, this is a very difficult question. And as a Co-Chair of the R&D Working Group of the Partnership for Critical Infrastructure Security, we attempted, and I must mention, I mean, that is an organization that is government, industry, and academia with the right people with the right government insight, you know, in theory. To even just catalog the technical areas where research is going on in the country, through federally funded programs, and we were not able to do that. And this was one of the reasons why I call for some form of a new, coordinating cooperative body so that we can truly come up with an analysis of what—where the research is.

You know, I believe that in the charter for this hearing there were some numbers that I have seen, or that were provided to me through one of my research assistants, that seemed to imply government funding in the multiple billions of dollars. But my experience would show that it is in the hundreds of millions, and my belief is that it ought to be a ten-fold increase.

Page 161 PREV PAGE TOP OF DOC

Mr. **EHLERS.** Yeah. Okay. Any other comment?

Mr. **WEAVER.** Well, with your permission, we will submit for the record, as soon as possible, what we can for you.

Mr. **EHLERS.** Okay.

Chairman **BOEHLERT.** Thank you very much.

Mr. **EHLERS.** And may I just conclude by saying I—obviously I am a professor. I have asked an impossible question, but I am going to let this be a take-home exam and I would appreciate your answers. Just one last comment.

Chairman **BOEHLERT.** Always the professor.

Mr. **EHLERS.** I own a Macintosh. I got through Y2K with absolutely no—didn't even have to think about it, and I haven't had any virus problems. So there may be a lesson there.

Chairman **BOEHLERT.** Thank you very much, Professor Ehlers. A little bit of a sensitive area, but one of the things that is critically important is for government agencies to build up trust in their various constituencies they are reaching out to. And I know from my experience in examining their work, and Mr.

Weaver and his team, that in some instances there has been a reluctance on the part of the private sector to cooperate with Federal law enforcement officials because the last thing a CEO wants is some subpoena to appear someplace in line with an investigation. And one of the real success stories of Mr. Weaver and his team is they have built up this area of trust with the private sector so information is being shared, and as a result, everyone benefits. The Chair is pleased to recognize Mr. Larson.

Page 162 PREV PAGE TOP OF DOC

Mr. **LARSON.** Thank you, Mr. Chairman. And let me commend you, as well. Let me cut right to the chase here and ask the panelists what role you foresee encryption playing in this discussion and how do we balance the need for security amongst our agencies along with the technological need to market this technology globally?

Dr. **SPAFFORD.** I have some more extensive comments in my written testimony, but I will answer that encryption is a vital component of what we do with system security. If you were to think about building a building, security might very—or encryption might very well be the plumbing that goes into it. It has to be there to enable a lot of the other work to go on. It is also very difficult to get correct. Encryption requires a very deep understanding of mathematical principles and how those are constructed and implemented in a system. We have had systems that have been fielded for decades where there had been vulnerabilities discovered, very subtle ones, that have either been known to government agencies or discovered out in the open.

Putting in a system requires a lot of effort and time to get right. And because it is built in to all of these systems, if we put in the wrong system, if we put in something with a weakness that can be exploited, we endanger all of the other systems that it is built upon. So with that said, we are very much concerned that strong encryption be put into place.

From a law enforcement standpoint, there are other techniques that can be exploited. They haven't been well investigated. This is an area where research could be helpful, is to how to gather evidence and information without having to see inside of those messages.

Page 163 PREV PAGE TOP OF DOC

Mr. **LARSON.** I am on the Armed Services Committee, as well, as this is often times of the give and take that we have on the Committee. We have the various agencies coming saying, you really shouldn't be marketing this technology globally. And, yet, not to market the technology also puts us in an awkward position. Your opinions.

Dr. **WULF.** I think it is about 6 years ago now when the clipper chip proposal was made. Congress asked the National Academies to do a study of what national policy should be with respect to cryptography. And I was fairly close to that study, as a matter of fact. It was conducted partially at very highly classified levels. Members of the Committee included two former assistant secretaries—Assistant Attorney Generals. The Chair was a retired four-star Army general who had spent his life in intelligence. A couple—at least one

former Deputy Director of the National Security Agencies.

I am trying to make the point that the intelligence, defense, and law enforcement agencies were fully represented and important on the committee. The first recommendation that they made was that there should not be any limitation on the use of cryptography within the United States.

Mr. **LARSON.** Thank you very much. Thank you, Mr. Chairman.

Chairman **BOEHLERT.** Thank you, Mr. Larson. Now, the angel of the National Institute of Standards and Technology, the distinguished gentlelady from Maryland, Ms. Morella.

Page 164 PREV PAGE TOP OF DOC

Ms. **MORELLA.** Thank you, Mr. Chairman. He or she who stays to the very end really has a commitment as all of you do. I want to thank you, Mr. Chairman. This is obviously a very important hearing we have. And you have assembled a great group of experts to testify today. And, again, there are so many issues that we could comment on. But I do want to thank Dr. Wulf and Dr. Spafford and Mr. Weaver. And I want to point out to Ms. Benzel, who is the Vice President of Advanced Security Research of Network Associates, that, as she knows, your PGP Security business unit is located in my Congressional district in Montgomery County, Maryland. I am proud of that.

I am also proud, as I looked around, to see a former staffer of mine who is the Director of Internet Network Security Policy for Business Software Alliance, Mario Correa. He is trying to hide back there. But it is a great group and I have been involved with the computer security bill that we hope will come under suspension which will give more authority to the National Institute of Standards and Technology.

I do recognize, as having worked as this Committee did on Y2K over and over again for many years, the validity of having set that groundwork with regard to reviewing our information technology systems and the same problem we now have of trust and interoperability, cooperation, partnership.

But I guess I will direct my question to Ms. Benzel. And that is, I want to congratulate Network Associates for their recent grant on cyber security work that came from NIST. I wondered if you might elaborate a little bit on what that—what you hope to achieve with that grant.

Page 165 PREV PAGE TOP OF DOC

Ms. **BENZEL.** Thank you very much for your support, Ms. Morella, and we are very happy to be part of your district. It is an important presence for us in Rockville, Maryland. We are very happy to be working with NIST. And in our, you know, history as part of Entrusted Information Systems, we have a long history there. And, in fact, my deputy who sits behind me, Dr. Dave Balenson, comes from NIST, works with me very extensively there. We are very happy to have the new grant.

We are working in a university partnership and looking to establish a test bed to test information security in the mobile wireless community. And mobile and wireless have not gotten a lot of discussion in today's debates, but clearly are the leading edge where we need to move forward, and we thank you.

Ms. **MORELLA.** I thank you. Incidentally, I must also compliment NIST for having produced also a Nobel Prize Laureate. I hope you all recognize that too. Let me ask you about education. Mention has been made, and we have known this for years, that we just don't have enough American nationals who are doing graduate work in computer security and related fields.

I am working on legislation, and I wanted to get your feeling on it, that would have a tuition waiver or give scholarships for those students in a—who would do advanced work in computer security. In turn, they would serve the Federal Government in this position for probably two years, if they get two years of assistance. Now, in the computer security bill that we hope will come out on the Floor soon, there are some scholarships within that—you know, a small amount of scholarships. But it seemed to me that if we then got a commitment of those people to go back into Federal Government and work on that, that that might help the business area, the private sector, as well as the public sector.

Page 166 PREV PAGE TOP OF DOC

I guess, Dr. Spafford, you seem to be very much involved with the academic facet, that if you would comment, and then if anyone else has any comments.

Dr. **SPAFFORD.** Well, I would like to comment, first of all, to the fact that there are some programs in place that do similar—the Scholarship for Service Program that is now through the National Science Foundation. We are one of the schools that was a recipient of some of that funding. We have not been able to fill all the positions. The very able students who are interested in research in this area, that we might otherwise attract, are not interested in signing away a couple years of their time afterwards when they can find companies that are willing to hire them.

And that gets to the actual heart of why we don't have as many students going on for the advanced graduate work. When our students observe faculty members, and when we are spending, perhaps, a third of our time doing administrative work and configuration of machines, when we are dealing with out-of-date equipment resources, when we are housing our equipment and students in converted cleaning closets, and we are forced to do short-term research that isn't really part of the intellectual climate of the university, and then they realize that if they only get a master's degree, or sometimes just an undergraduate, they can go out in the industry, work in better surroundings at higher pay with stock options, and state-of-the-art equipment, doing the exact same thing that we are doing and get paid more, they are not interested in staying. So simply covering their tuition is not going to solve that problem.

Ms. **MORELLA.** I want you to think about what the solution would be. I am talking about going into the Federal sector. I know you need them in the faculty also probably. But going into the Federal sector. But if you can come up with something that you think might make it more palatable. It just seems to me national security is also important and recognition——

Page 167 PREV PAGE TOP OF DOC

Ms. **BENZEL.** Ms.——

Ms. **MORELLA.** Yes.

Ms. **BENZEL.** If I may, Ms. Morella, I would like to suggest that in addition to targeting students, that perhaps you want to look at ways for more senior and experienced people in industry to rotate in to do service in the Federal sector. You will benefit from that experience. You won't have the issues that Dr. Spafford talks about, about the young folks that are, you know, urgent to get out there and get their income in. And you also have the maturity and the understanding of the contributions we can make to the Nation.

Ms. **MORELLA.** I would be delighted to work with you on that very issue. Did you want to comment on it?

Dr. **WULF.** Just to point out that although we talk a lot about the fact that we have great difficulty with our K through 12 educational system, it is clear that our educational system at the graduate level is the envy of the world. And a critical piece of that is the fact that we tie research and education together. And so whatever solution you think of, I think should deal in terms of trying to strengthen that relationship as opposed to providing alternate funding which might not couple a student to a faculty member to do that joint research.

Ms. **MORELLA.** My time has expired. I thank you. Thank you, Mr. Chairman.

Page 168 PREV PAGE TOP OF DOC

Chairman **BOEHLERT.** Does the gentlelady require any additional time to get in further plugs for NIST? Let—while we are at plugs, let me just ask Mr. Weaver something, which is near and dear to my heart. Utica College, which is in my Congressional district, and it happens to be my alma mater in beautiful upstate New York, has been developing interdisciplinary programs and economic crime investigation and computer forensics. Can you comment on these programs and how they can be a greater source of talent and expertise for the future?

Mr. **WEAVER.** Well, being on the Board of Directors for Utica College myself, I have a vested interest. And to start out, internship programs are very, very useful. And in addition to the internship programs, the private sector becomes significantly important to their interaction. And I think the combination of both of those programs and the research and development issues that you are bringing forward now, and the new technology is the way to go.

Chairman **BOEHLERT.** Well, thank you very much. And the reason I mention that, and not just to get a plug in for what I think is a great emerging institution, but to demonstrate to all our Panel that we are placing a heavy emphasis on education in this Science Committee, science and math education, in particular. Because to get the people all of you need for the future, we have got to start by creating a more solid foundation.

And we have a bill we reported out to science and math partnership, part of the President's education initiative, $325 million, and we are just beginning to give that area the attention it deserves. And fortunately we have the enthusiastic support of the Administration. We are working in partnership.

Page 169 PREV PAGE TOP OF DOC

Let me conclude the hearing by saying we started out—I started out by saying we don't know what we don't know. But as a result of your expert testimony and the interaction we have had here, we know a little bit more about what we don't know, and we have a clear path charted for us to develop a legislative initiative that will address this issue. And we talked about vulnerability analysis, Ms. Benzel. We are in the process of doing that, not just in this Committee, but every committee in the House right now. I am leaving here to go over to a meeting of the Subcommittee on Water Resources. And we have got a little vulnerability analysis there dealing with the Nation's public water systems.

But I think we are bringing to bear the full talent and commitment and dedication of the entire Congress on a bipartisan basis in this whole area. People were much too casual prior to September 11, and I would suggest much more alert today.

And I want to thank all of you for being such valuable resources, and I would hope that you would be receptive to any further contacts you might have from the Committee to ask you, perhaps, to commit some of your additional thoughts in writing so that we can share it with all of our Committee. And, Dr. Wulf, as I said, you enlisted before you were drafted, and I really do appreciate that. And I appreciate all of what you are doing so well. And, Mr. Weaver, please convey to all of your associates and a magnificent team up there that our hearts and minds and everything else we have are with you. Thank you all very much. This hearing is adjourned.

[Whereupon, at 12:24 p.m., the Committee was adjourned.]

Appendix 1:

Page 170 PREV PAGE TOP OF DOC

Additional Material for the Record

75565c.eps

75565d.eps

(Footnote 1 return)

A Critical Infrastructure is defined as "a network of independent, mostly privately-owned, man-made systems and processes that function collaboratively and synergistically to produce and distribute a continuous flow of essential goods and services." Critical Foundations: Protecting America's Infrastructures, *the report of the President's Commission on Critical Infrastructure Protection (PCCIP) 1997.*

(Footnote 2 return)

Realizing the Potential of c4I: Fundamental Challenges, 1999.

(Footnote 3 return)

As defined by Presidential Decision Directive PDD–633. Or, see, for example, "The National Plan" ver.1, Section 4.A. pp. 22–23.

(Footnote 4 return)

Testimony Before the Committee on Commerce, Science, and Transportation: Aviation Security—Terrorist Acts Demonstrate Urgent Need to Improve Security at the Nation's Airports, September 20, 2001, GAO–O1–1162T. *http://www.senate.gov/commerce/hearings/092001Dillingham.pdf*

(Footnote 5 return)

As defined by Presidential Decision Directive PDD–633. Or, see, for example, "The National Plan" ver.1, Section 4.A. pp. 22–23.

CONTENTS SPEAKERS INSERTS

INSERTS SPEAKERS CONTENTS