AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

CYBER SECURITY RESEARCH AND DEVELOPMENT

HEARING

BEFORE THE

COMMITTEE ON SCIENCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

MAY 14, 2003

Serial No. 108–17

Printed for the use of the Committee on Science

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

U.S. GOVERNMENT PRINTING OFFICE

86–992PS WASHINGTON : 2003

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON SCIENCE

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

LAMAR S. SMITH, Texas
CURT WELDON, Pennsylvania
DANA ROHRABACHER, California
JOE BARTON, Texas
KEN CALVERT, California
NICK SMITH, Michigan
ROSCOE G. BARTLETT, Maryland
VERNON J. EHLERS, Michigan
GIL GUTKNECHT, Minnesota
GEORGE R. NETHERCUTT, JR., Washington
FRANK D. LUCAS, Oklahoma
JUDY BIGGERT, Illinois
WAYNE T. GILCHREST, Maryland
W. TODD AKIN, Missouri
TIMOTHY V. JOHNSON, Illinois
MELISSA A. HART, Pennsylvania
JOHN SULLIVAN, Oklahoma
J. RANDY FORBES, Virginia
PHIL GINGREY, Georgia
ROB BISHOP, Utah
MICHAEL C. BURGESS, Texas
JO BONNER, Alabama
TOM FEENEY, Florida
VACANCY

RALPH M. HALL, Texas
BART GORDON, Tennessee
JERRY F. COSTELLO, Illinois
EDDIE BERNICE JOHNSON, Texas
LYNN C. WOOLSEY, California
NICK LAMPSON, Texas
JOHN B. LARSON, Connecticut
MARK UDALL, Colorado
DAVID WU, Oregon
MICHAEL M. HONDA, California
CHRIS BELL, Texas
BRAD MILLER, North Carolina
LINCOLN DAVIS, Tennessee
SHEILA JACKSON LEE, Texas
ZOE LOFGREN, California
BRAD SHERMAN, California
BRIAN BAIRD, Washington
DENNIS MOORE, Kansas
ANTHONY D. WEINER, New York
JIM MATHESON, Utah
DENNIS A. CARDOZA, California
VACANCY

CONTENTS

May 14, 2003

	Page
Witness List	2
Hearing Charter	3

Opening Statements

Statement by Representative Sherwood L. Boehlert, Chairman, Committee on Science, U.S. House of Representatives	9
Written Statement	9
Statement by Representative Ralph M. Hall, Minority Ranking Member, Committee on Science, U.S. House of Representatives	10
Written Statement	10
Prepared Statement by Representative Nick Smith, Chairman, Subcommittee on Research, Committee on Science, U.S. House of Representatives	11
Prepared Statement by Representative Jerry F. Costello, Member, Committee on Science, U.S. House of Representatives	12
Prepared Statement by Representative Eddie Bernice Johnson, Member, Committee on Science, U.S. House of Representatives	12
Prepared Statement by Representative Sheila Jackson Lee, Member, Committee on Science, U.S. House of Representatives	13

Witnesses:

Dr. Charles E. McQueary, Under Secretary for Science and Technology, Department of Homeland Security	
Oral Statement	15
Written Statement	18
Biography	21
Dr. Rita R. Colwell, Director, National Science Foundation	
Oral Statement	21
Written Statement	23
Biography	27
Dr. Arden L. Bement, Jr., Director, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce	
Oral Statement	27
Written Statement	29
Biography	34
Dr. Anthony J. Tether, Director, Defense Advanced Research Projects Agency	
Oral Statement	35
Written Statement	38
Biography	41
Discussion	42

Appendix 1: Answers to Post-Hearing Questions

Dr. Charles E. McQueary, Under Secretary for Science and Technology, Department of Homeland Security	72
Dr. Rita R. Colwell, Director, National Science Foundation	76
Dr. Arden L. Bement, Jr., Director, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce	81

Page

Appendix 2: Additional Material for the Record

Letter from the Information Security and Privacy Advisory Board to The Honorable Mitchell E. Daniels, Jr., Director, Office of Management and Budget, dated April 8, 2003 86
Current Activities of the National Institute of Standards and Technology in Cyber Security and Related Programs 89
Public Law 107–305—Nov. 27, 2002 97

CYBER SECURITY RESEARCH AND DEVELOPMENT

WEDNESDAY, MAY 14, 2003

HOUSE OF REPRESENTATIVES,
COMMITTEE ON SCIENCE,
Washington, DC.

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

COMMITTEE ON SCIENCE
U.S. HOUSE OF REPRESENTATIVES

Cybersecurity Research and Development

Wednesday, May 14, 2003
10:00 AM
2318 Rayburn House Office Building (WEBCAST)

Witness List

Dr. Charles McQueary
Under Secretary for Science and Technology
Department of Homeland Security

Dr. Rita Colwell
Director
National Science Foundation

Dr. Arden Bement, Jr.
Director
National Institute of Standards and Technology

Dr. Anthony Tether
Director
Defense Advanced Research Projects Agency

Section 210 of the Congressional Accountability Act of 1995 applies the rights and protections covered under the Americans with Disabilities Act of 1990 to the United States Congress. Accordingly, the Committee on Science strives to accommodate/meet the needs of those requiring special assistance. If you need special accommodation, please contact the Committee on Science in advance of the scheduled event (3 days requested) at (202) 225-6371 or FAX (202) 225-0891.
Should you need Committee materials in alternative formats, please contact the Committee as noted above.

HEARING CHARTER

COMMITTEE ON SCIENCE
U.S. HOUSE OF REPRESENTATIVES

Cyber Security Research and Development

WEDNESDAY, MAY 14, 2003
10:00 A.M.—12:00 P.M.
2318 RAYBURN HOUSE OFFICE BUILDING

1. Purpose

On Wednesday, May 14, 2003, the House Science Committee will hold a hearing to examine federal cyber security research and development (R&D) activities and implementation of last year's *Cyber Security Research and Development Act* (P.L. 107–305).

2. Witnesses

Dr. Charles E. McQueary is the Under Secretary for Science and Technology at the Department of Homeland Security. Prior to joining the Department, Dr. McQueary served as President of General Dynamics Advanced Technology systems, and as President and Vice President of business units for AT&T, Lucent Technologies, and as a Director for AT&T Bell Laboratories.

Dr. Rita R. Colwell is the Director of the National Science Foundation (NSF). Before joining the Foundation, Dr. Colwell served as President of the University of Maryland Biotechnology Institute and Professor of Microbiology at the University Maryland. She was also a member of the National Science Board from 1984 to 1990.

Dr. Arden L. Bement, Jr. is the Director of the National Institute of Standards and Technology (NIST). Prior to his appointment as NIST director, Dr. Bement was professor and head at the School of Nuclear Engineering at Purdue University. Before Purdue, he served in a variety of positions, including Vice President of Technical Resources and of Science and Technology for TRW Inc. and Deputy Under Secretary of Defense for Research and Engineering. Dr. Bement has also served as a member of the National Science Board and as chair of the NIST Visiting Committee on Advanced Technology.

Dr. Anthony J. Tether is the Director of the Defense Advanced Research Projects Agency (DARPA). Until his appointment as Director of DARPA, Dr. Tether held the position of Chief Executive Officer and President of The Sequoia Group. He has also been Chief Executive Officer for Dynamics Technology Inc. and Vice President of Science Applications International Corporation's (SAIC) Advanced Technology Sector. Dr. Tether has served on Army and Defense Science Boards.

3. Overarching Questions

The hearing will address the following overarching questions:

1. What is the current status of federally-supported cyber security research and development programs in the United States? What level and types of effort are needed to meet existing and emerging cyber terrorism threats?
2. How are cyber security research and development activities coordinated among federal agencies? How are gaps in the research portfolio identified and filled? How will the new Department of Homeland Security affect the coordination process? How will it change the overall portfolio of programs?
3. What efforts are being made to develop a strong cyber security workforce and to establish and expand university educational and research programs relevant to cyber security?
4. How do the federal agencies work with industry on cyber security research and development efforts?

4. Brief Overview

- Information technology systems underpin key industries such as telecommunications and financial services, and also play a vital role in the

smooth functioning of critical infrastructures and services, such as transportation systems, the electric power grid, and emergency response capabilities. As the number of ways in which our economy depends on network and computer systems has grown, so has the number of attacks on these information technology systems. For example, the number of incidents reported to the computer security incident response center at Carnegie Mellon University increased 275% from 2000 to 2002, and over 42,000 incidents have already been reported in 2003.

- Active research and development programs to produce new cyber security tools and techniques are necessary to enable us to maintain the performance of important networks and systems and improve our ability to defend against cyber and physical terrorism. Currently, cyber security research and development is supported and performed at a variety of federal agencies, including the National Science Foundation (NSF), the National Institute of Standards and Technology (NIST), and the Defense Advanced Research Projects Agency (DARPA). Within the new Department of Homeland Security, the Science and Technology Directorate will have responsibility for managing research and development programs relevant to cyber security.
- In November of 2002, the President signed the *Cyber Security Research and Development Act* (P.L. 107–305), which authorized appropriations for the National Science Foundation and the National Institute of Standards and Technology to strengthen their programs in computer and network security (CNS) research and development and to support CNS research fellowships and training programs. However, FY 2003 appropriations and FY 2004 proposed funding are significantly below the authorized levels.
- New hardware and software technologies are rapidly adopted in many industries and new ways of interfering with computer systems develop just as fast. Multiple federal agencies will need to coordinate their efforts to ensure that new understanding of information and network security is generated and that this knowledge is transitioned into useful cyber security products. Institutions of higher education will have develop and expand degree programs to ensure that an adequate workforce exists to put the new tools and techniques into practice. The private sector has a critical role to play, as it will contain the developers and suppliers as well as the major purchasers of new cyber security technologies and services.

5. Background

Cyber Threats to Critical Infrastructures

Information technology systems underpin key industries such as telecommunications and financial services, and also play a vital role in the smooth functioning of critical infrastructures and services, such as transportation systems, the electric power grid, and emergency response capabilities. Remote operation of chemical plant functions and management of the aircraft control system also depend on software and computer networks. Thus vulnerabilities in various components of networks and computers could be exploited to disrupt and damage these critical systems. For example, distributed denial of service attacks could slow Internet traffic and bring down important web sites. Cyber attacks on supervisory control and data acquisition (SCADA) systems could shut down power plants or disrupt processes at chemical manufacturing facilities. Interference with emergency responder communications technology could amplify the effects of a physical terrorist attack.

The vulnerability of the Nation's information technology infrastructure has been demonstrated many times in the past several years. "Hackers" are arrested for breaking into computer systems to steal and corrupt data, or just to disrupt government or industry services. Major "infections" of computer viruses and worms[1] make the news, and smaller "outbreaks" occur daily.[2] While the impact on physical systems has been minimal to date, the economic impact of successful attacks can be significant. For example, in 2001, the Code Red and Nimda worms spread through

[1] A computer virus is a program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves. They are often capable of attaching themselves to other files or e-mail and transmitting themselves across networks and bypassing security systems. Some of the destructive things that viruses can do include deleting or corrupting files and using all the available memory on a system (thereby bringing the system to a halt). A worm is a special type of virus that can replicate itself and use memory, but cannot attach itself to other programs.

[2] In 2002, 82,094 incidents were reported to the CERT Coordination Center at Carnegie Mellon University, up 275% from 2000. Also in 2002, the center published 41 security alerts and handled over 200,000 mail messages and over 800 hotline calls.

e-mail, corporate networks, and Web browsers. Together, they are estimated to have produced $3 billion in costs worldwide due to lost productivity and expenses related to testing, cleaning, and deploying patches to computer systems. In January of 2003, the Slammer (or Sapphire) Worm took advantage of vulnerabilities in server software to generate a damaging level of network traffic, so Internet users experienced difficulty accessing web sites and sending e-mail. In addition, Bank of America automated teller machines were taken off line, Continental Airlines reservation computer systems experienced widespread problems, and an emergency call center in Seattle was essentially blacked out. Thus developing new defenses is critical to ensure that small weaknesses are not exploited to produce major economic consequences.

The above examples show how a terrorist could target computer systems or networks and create a great deal of disruption and damage. However, terrorists could also use information technology systems to amplify the effects of a physical attack on people or property. For example, a terrorist planning to release a chemical or biological agent could first send an e-mail that appears to be from a trustworthy source (a police department or a news agency) to order or urge evacuation of buildings in order to increase the number of people out in the streets when he spreads his toxin. Cyber attacks could also be used to interfere with first responder communication and coordination systems, hindering the ability to respond to a crisis. Thus protection of information systems is a critical part of homeland defense.

The National Strategy to Secure Cyberspace was released by the Administration in February 2003. It includes a number of recommendations to improve the Nation's cyber security now, both in federal systems and in privately-owned infrastructures. Currently the Federal Government's effort to deploy cyber security tools and techniques (the "operational" cyber security programs) are scattered over many agencies. The National Institute of Standards and Technology provides guidance and tools to federal agencies and to private industry that enable them to evaluate their cyber security needs and the performance of their security systems. The National Security Agency has significant programs in encryption. The Department of Homeland Security will have significant responsibilities in this area, both in new programs in its Information Analysis and Infrastructure Protection directorate, and in programs that are being transferred in, like the Federal Computer Incident Response Center (FedCIRC), which provides civilian agencies and departments with offerings in computer security incident prevention, reporting, analysis, and recovery. There are also private organizations, such as the federally-funded CERT Coordination Center at Carnegie Mellon University,[3] whose activities include providing technical advice about and coordinating responses to security incidents, publishing security alerts, and tracking information about vulnerabilities and intruder activities.

The Need for Cyber Security Research and Development Programs

In addition to discussing ways to reduce cyber infrastructure vulnerabilities now, *The National Strategy to Secure Cyberspace* also emphasizes the importance of developing and carrying out a cyber security research and development agenda for the Federal Government.

Cyber security research and development programs focus on ways to prevent attacks, to detect them as they are occurring, to respond to them effectively, to mitigate the severity of their effects, to recover as quickly as possible from them, and to find the people responsible. In addition to enabling us to avoid damage from cyber terrorism, a greater understanding of the weaknesses in computer systems and networks and how to protect them will allow computer operators to deflect the actions of cyber criminals—out to steal credit card numbers and personal information—and hackers—out to disrupt and destroy for the fun of it.

In March 2003, the National Academy of Science released *Information Technology for Counterterrorism: Immediate Actions and Future Possibilities.* This report outlines an extensive research agenda for information technology research in many areas. In the information and network security field, the areas of emphasis are: authentication (determining that a system's users are those with permission to use it), detection (being aware that an attack, or attempted attack, is occurring), containment (mitigating the effects of an attack), and recovery (getting the system back up and functioning after an attack). The report also lists a number of research areas in which advances will impact all facets of the effort to improve cyber security. These areas include reducing the "bugginess" of software, managing the trade-offs between security and functionality more successfully, and gathering information on new and emerging techniques for cyber attacks.

[3] While "CERT" originally stood for "Computer Emergency Response Team," today the center's name is officially just "CERT."

Existing Federal Cyber Security Research and Development Programs

The National Science Foundation (NSF) and the National Institute of Standards and Technology (NIST) currently have active cyber security-related programs. To support and expand these programs, the *Cyber Security Research and Development Act* was signed in November 2002. Under this Act, NSF was authorized to expand its computer and network security grants programs and establish new research centers in this area and to provide grants to institutes of higher education and provide fellowships to students to increase the number of people receiving degrees in this area. NIST was authorized to create new program grants for partnerships between academia and industry, new post-doctoral fellowships, and a new program to encourage senior researchers in other fields to work on computer security. The Act authorizes $903 million over five years for these new programs, to ensure that the U.S. is better prepared to prevent and combat terrorist attacks on private and government computers. Specifically, for FY 2004, $110.25 million was authorized for NSF, and $47.29 million for NIST, to enable them to carry out the above programs. However, actual appropriations in FY 2003 and the presidential proposals for FY 2004 both fall far short of the authorized numbers.[4] As a result, NIST will be entirely unable to establish the grants program for academic-industrial research partnerships, and NSF's grants programs will be significantly smaller than those envisioned in the Act.

The Department of Homeland Security is currently setting up its organizational structure and defining its programmatic priorities for FY 2003 and FY 2004. In the department, responsibility for managing research and development efforts relevant to cyber security rests in the Science and Technology directorate, while operational responsibilities for implementing cyber security fall in the Information Analysis and Infrastructure Protection directorate. Public statements have been made indicating that there will be no "box" in the organization with specific responsibility for cyber security in either the operational or research arenas. Operationally, programs to secure the cyber infrastructure will be an element of the broader critical infrastructure protection efforts. In the Science and Technology directorate, cyber security research and development programs will be part of the Threat and Vulnerability, Testing and Assessment program, and will focus on meeting critical needs of other DHS units, such as the Information Analysis and Infrastructure Protection directorate and the U.S. Secret Service. Less than 1 percent of the Science and Technology directorate's $803 million budget will be directed toward cyber security research and development. The absence of a clear advocate for cyber security at the Department is of particular concern in light of the Administration's decision in February 2003 to eliminate the President's Critical Infrastructure Protection Board. The Board, which was established after the attacks of September 11, 2001, authored *The National Strategy to Secure Cyberspace* and the Board's director, Richard Clarke, did much to raise the level of awareness about the vulnerabilities of the Nation's cyber infrastructure and the need for improved cyber security.

The Defense Advanced Research Projects Agency (DARPA) has played a critical role in information technology research, including cyber security programs. The first firewall,[5] significant advances in intrusion detection systems, and important Internet security protocols were all developed through DARPA programs. In the late 1990's, the agency made a large investment in "defensive" information warfare, which included unclassified research on computer systems' security and survivability. However, DARPA does not have a history of sustained, stable support of cyber security research and development programs, and, since 2000, the size of this program has declined (from approximately $90 million in 2000 to $30 million in 2003). Part of this decline is due to the fact that DARPA's focus has shifted to classified research on "offensive" information warfare. Classified research on information security is also done by the National Security Agency (NSA). NSA's funding for information assurance work is estimated to be roughly $750 million, with roughly half spent on research, development, testing, and evaluation; a significant part of this effort focuses on cryptography. While defense-related work on cyber security is necessary, it is important to recognize that the impact such classified work has on the overall national cyber security is often limited because the research is mainly

[4] For example, NSF cyber security research programs received $28 million in FY 2003 (as compared to $47 million authorized in this area), and the FY 2004 proposal is for $35 million (authorization was $64 million).

[5] A firewall is a system designed to prevent unauthorized access to or from a private network. Firewalls are frequently used to prevent unauthorized people from accessing private networks (like those used at companies, universities, and government agencies) over the Internet. All messages (like e-mail) entering or leaving the private network pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

performed at government facilities and contractors, and the results are seldom shared publicly or transferred to the commercial sector.

Overall, it is currently very difficult to determine the total spending on cyber security research and development programs across the Federal Government. Information is currently collected and reported on a variety of relevant areas (such as networking and information technology research and development), but the programs specifically devoted to cyber security research and development have not been pulled out. OSTP has indicated that agencies will be asked to quantify cyber security research and development funding within their FY 2005 request.

Another factor to be considered in assessing the quality of cyber security operations and cyber security research in the United States is the critical role of the private sector in both areas. As new results emerge from cyber security research and development activities, information technology companies will have to turn new knowledge into new technologies and services, and industries from banking to electric power will have to choose to take advantage of these new capabilities. Therefore, federal cyber security research and development programs will have to consider ways to encourage technology transfer and facilitate technology uptake.

Workforce Issues

Research and development goals and useful new cyber security tools are of no use if there are not people to carry out the research programs and put the new techniques into practice.[6] The *Cyber Security Research and Development Act, The National Strategy to Secure Cyberspace,* and the National Academy of Sciences' report all emphasize the importance of expanding the relevant workforce. Recommended actions range from developing undergraduate and masters programs to train operational cyber security personnel to fellowships for post-doctoral and senior scientists and engineers to increase participation in information security research programs. Current programs in this area are quite small. The National Science Foundation has a Cyber Security Scholarship for Service program ($16 million requested for FY 2004). This program provides scholarships to students in the fields of information assurance and computer security in return for a commitment following graduation to work for a federal agency. The Department of Defense started a program[7] in 2000 to provide re-training fellowships for researchers and recent Ph.D.s looking to transfer into the cyber security field, but this program is ending in 2003. The *Cyber Security Research and Development Act* authorizes NIST to establish a senior research fellowship program that will be open to established researchers who seek to change fields into cyber security research, but no funds were requested for that program in FY 2004.

6. Current Issues

The most pressing issue in cyber security research and development is the underfunding of relevant programs. The NSF and NIST programs are well under the authorized levels. DARPA is ramping down relevant unclassified programs. The proposed effort in DHS is small. Yet the cyber infrastructure of the United States penetrates all critical infrastructures and forms a fundamental base of the Nation's physical security and economic and social stability. Significant investment in research and development in computer and network security will be needed to maintain homeland security. Delaying this investment will not only increase current and future vulnerabilities, but will also raise future cyber security expenses, from the costs associated with damage done by cyber attacks to the expenses of retrofitting security systems onto existing hardware and software.

Each federal agency has its own mission and thus each has its own special role to play in cyber security research and development. Multi-agency collaboration and a coherent cross-agency strategy are needed to maximize the impact of federal investment and to ensure that gaps do not develop in the effort to develop the tools needed to build a multi-layer defense of the cyber infrastructure. In addition, since many information technology products and their implementations in critical infrastructures are developed and owned by the private sector, close communication with industry will be required. Finally, growth is needed in educational programs to expand research and development programs and to train the workforce required to implement security techniques in critical computer and network systems.

7. Witness Questions

The witnesses were asked to address the following questions in their testimony:

---

[6] According to NSF, only approximately seven Ph.D.s in cyber security are awarded each year.

[7] The Critical Infrastructure Protection and Information Assurance Fellows (CIPIAF) Program provided funds to cyber security principal investigators to pay post-doctoral fellows coming from non-cyber security backgrounds.

Questions for Dr. Charles McQueary

- How will the cyber security research and development agenda at the Department of Homeland Security be defined? Will the department's science and technology directorate develop in-house cyber security expertise and programs? How will it coordinate with the department's operational cyber security programs?
- What mechanisms will the Department of Homeland Security use to coordinate its cyber security research and development activities with other federal agencies, such as NSF, NIST, and DARPA, with active programs in this area?
- How will the department interact with cyber security research and development efforts underway in industry? How will it interact with university-based cyber security programs?

Questions for Dr. Rita Colwell

- What actions has the National Science Foundation (NSF) taken in response to the *Cyber Security Research and Development Act?* In particular, how is NSF fulfilling its role as the lead agency for cyber security research and development as specified in Section 7 of the Act?
- What are NSF's priorities in cyber security research and development? How are these priorities determined?
- How does NSF coordinate its cyber security research and development activities with other federal agencies?
- To what extent is NSF identifying and working to fill gaps in the federal cyber security research and development portfolio?

Questions for Dr. Arden Bement

- What actions has NIST taken in response to the *Cyber Security Research and Development Act?*
- How does NIST coordinate its cyber security research and development activities with other federal agencies? How does NIST interact with industry on cyber security research and development activities?
- What are NIST's priorities in cyber security research and development? How are these priorities determined?

Questions for Dr. Anthony Tether

- How have DARPA's information assurance research and development programs evolved over the past few years? Is there an increased emphasis on military or offensive applications? How is the balance between classified and unclassified efforts changing?
- How does DARPA coordinate its cyber security research and development activities with other federal agencies?
- How is information about results or technologies that are applicable to the protection of commercial networks and privately-owned infrastructures provided to relevant research and development communities in industry and academia?
- What are DARPA's priorities in cyber security research and development? How are these priorities determined?

Appendix I

Links to referenced documents on cyber security research and development:

Public Law 107–305: The *Cyber Security Research and Development Act* (November 2002):
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ305.107.pdf

The National Strategy to Secure Cyberspace (February 2003)
http://www.whitehouse.gov/pcipb/

Information Technology for Counterterrorism: Immediate Actions and Future Possibilities, National Academy of Sciences (March 2003):
http://bob.nap.edu/html/IT_counterterror/

Chairman BOEHLERT. The hearing will come to order. It is a pleasure to welcome everyone here this morning for a hearing on a subject that has consumed the Committee over the past couple of years: cyber security research and development. We have been focused on this topic for good reason. The Nation, quite simply, has been under-investigating—investing woefully in cyber security R&D and as a result, we lack both the experts and the expertise we ought to have in a world that relies so heavily on computers and networks for the necessities of everyday life.

Last year, led by this committee, Congress passed, and the President signed into law, two landmark bills to try to remedy this problem: the Cyber Security Research and Development Act and the Homeland Security Act. Both established new programs and authorized new funds for cyber security R&D.

Today is our first chance to see what has happened as a result. At first blush, the answer appears to be: not nearly enough. Agencies have neither sought nor set aside adequate funding to implement the Cyber Security R&D Act. We hear complaints from throughout the research community that the Department of Homeland Security is not focusing sufficiently on the problem and DARPA is actually reducing its investment in this area.

I am sure our witnesses today will describe positive actions that have been taken, and there are some, but it is impossible not to conclude that far more needs to be done. I assure you that this committee, we will continue pressing for more action on cyber security R&D. This hearing is only the beginning. We need to work together now to prevent devastating attacks in the future.

I look forward to hearing from all of our witnesses, and we are going to do just that. And we have a very distinguished panel, and I think all of my colleagues should be very impressed with the panel.

With that, let me introduce the distinguished Ranking Member from Texas, not Oklahoma, Texas, Mr. Hall.

[The prepared statement of Mr. Boehlert follows:]

PREPARED STATEMENT OF CHAIRMAN SHERWOOD BOEHLERT

It's a pleasure to welcome everyone here this morning for a hearing on a subject that has consumed the Committee over the past couple of years cyber security R&D.

We've been focused on this topic for good reason. The Nation quite simply has been under-investing woefully in cyber security R&D, and as a result we lack both the experts and the expertise we ought to have in a world that relies so heavily on computers and networks for the necessities of everyday life.

Last year, led by this Committee, Congress passed, and the President signed into law, two landmark bills to try to remedy this problem. The "Cyber Security Research and Development Act" and the "Homeland Security Act" both established new programs and authorized new funds for cyber security R&D. Today is our first chance to see what's happened as a result.

At first blush, the answer appears to be "not nearly enough." Agencies have neither sought nor set aside adequate funding to implement the Cyber Security R&D Act. We hear complaints from throughout the research community that the Department of Homeland Security is not focusing sufficiently on the problem. And DARPA is actually reducing its investment in this area.

I'm sure our witnesses today will describe positive actions that have been taken and there are some—but still one can only conclude that far more needs to be done. I assure you that this committee will continue pressing for more action on cyber security R&D. This hearing is only the beginning.

We need to work together now to prevent devastating attacks in the future. I look forward to working with all our witnesses to do just that.

Mr. Hall.

Mr. HALL. You know, all my exes are in Oklahoma this morning.

I want to join Chairman Boehlert in welcoming everyone to this morning's hearing, because first, you are selected on the basis of your knowledge and your service. And I know it takes time to get ready. It takes time to come here. It takes time to testify. And we appreciate the gift that you give to this committee, and through us, to the rest of the Congress.

Not a day—as Chairman Boehlert has very aptly set out, not a day goes by without some mention of information technology in the news and as this information technology has become a part of almost every aspect of our economy and of our society. As this has happened, we have become familiar with the negative aspects of the information revolution: cyber crime. The threats we fear range all the way from nuisance hackers, theft and fraud, to the breakdown of the information infrastructure and everything that depends on it.

With the events of the last few years, the security of the information infrastructure has received even more public attention. In February, the President released *The National Strategy to Secure Cyberspace.* The President's strategy emphasizes the need for more research efforts, and what I hope to learn today is the context for these research efforts and the amount of coordination that occurs between agencies and with the private sector.

In addressing any public policy question, the first thing to ask is: "What problems need to be solved?" As was pointed out in a recent article in *Issues in Science and Technology,* "Cyber Security: Who's Watching the Store?", we still lack a solid assessment of this threat. Despite the attention that cyber attacks receive in the media, there is little real data for estimating the size of the cyber security threat. And although I like a good story as much as anyone, the plural of anecdote is not data. Without the research to define the problem, I think it is difficult to determine the amount of money and the effort required to develop a solution to it.

So I hope today's witnesses can tell us what they are doing to define the scope and size of the problem with real data. We can't afford to have agencies going off on their own to develop a cyber security program and then hope the sum will be greater than the parts. Because their information infrastructure is largely in the hands of the private sector, any effective research agenda must be developed with input from the industry. A strategy that relies on simply training personnel and then hoping they find jobs is not sufficient. Research efforts need to be focused on the real problems, so I hope our witnesses will tell us about the interactions with industry and developing research agendas.

And I want to thank the witnesses for appearing before the Committee, and I look forward to their input on this issue. And I yield back my time.

[The prepared statement of Mr. Hall follows:]

PREPARED STATEMENT OF REPRESENTATIVE RALPH M. HALL

I want to join Chairman Boehlert in welcoming everyone to this morning's hearing.

Not a day goes by without some mention of information technology in the news. As information technologies have become a part of every aspect of our economy and society, we have become familiar with the negative aspects of the information revo-

lution—cyber crime. The threats we fear range from nuisance hackers, theft and fraud, to the breakdown of the information infrastructure and everything that depends upon it.

With events of the few years, the security of the information infrastructure has received even more public attention. In February, the President released *The National Strategy to Secure Cyberspace.* The President's strategy emphasizes the need for more research efforts. What I hope to learn today, is the context for these research efforts and the amount of coordination that occurs between agencies and with the private sector.

In addressing any public policy question, the first thing to ask is "What problem needs to be solved?" As was pointed out in a recent article in *Issues in Science and Technology,* "Cyber Security: Who's watching the Store?", we still lack a solid assessment of the threat. Despite the attention that cyber attacks receive in the media there is little real data for estimating the size of the cyber security threat. And although I like a good story as much as anyone, the plural of anecdote is not data. Without the research to define the problem, I think it's difficult to determine the amount of money and effort required to develop a solution. So I hope today's witnesses can tell us what they are doing to define the scope and size of the problem with real data.

I don't believe we can simply spend our way out of this problem. Therefore, I'm hoping that our witnesses can tell us how they coordinate the development of their research programs. We can't afford to have agencies going off on their own to develop a cyber security program and then hope the sum will be greater than the parts. Because our information infrastructure is largely in the hands of the private sector, any effective research agenda must be developed with input from the industry. A strategy that relies on simply training personnel and then hoping they find jobs is not sufficient. Research efforts need to be focused on the real problems. So, I hope our witnesses will tell us about their interactions with industry in developing the research agendas.

I want to thank our witnesses for appearing before the Committee and I look forward to their insight on this issue.

[The prepared statement of Mr. Smith follows:]

PREPARED STATEMENT OF REPRESENTATIVE NICK SMITH

Today we meet to examine federal efforts to address an extremely important—but often under-appreciated—threat to our country: the potentially devastating attacks on our nation's computer networks and infrastructure.

Almost immediately after the September 11th attacks, the Science Committee held multiple hearings to examine just how vulnerable we were to the threat of cyber attacks. These hearings revealed that the United States uses more and has become more dependent on "cyber" than any other country. Technological advancements in computers, software, networks and information technology greatly improved our lives, but they also made our society more vulnerable to disruption.

We also learned that the threat from other risks, such as computer viruses, hacking, and electronic identity theft, present significant hazards to general commerce, personal privacy, and our overall economic system. Finally, and in large part due to the interconnectedness of our technological age, we learned that physical security was permanently linked to cyber security. As a result, we concluded that Congress needed to address cyber security with the same vigilance with which we were addressing our physical security at home and abroad.

So we responded to these realizations by drafting and passing into law the *Cyber Security Research and Development Act of 2002.* This legislation provided a comprehensive, coordinated research framework to address the threats to our computer systems.

I am interested today to learn not only how the Federal Government is implementing the research coordination provisions of the cyber security bill, but also how they are working to ensure implementation of the technologies we now have readily available today. Although I am pleased that the Department of Homeland Security has requested over $800 million for applied research and development in its Science and Technology Directorate, it is not clear whether cyber security will receive appropriate attention within the Directorate.

We have a very esteemed panel of agency witnesses with us here today, and I have many important issues to discuss with them. I look forward to their testimony and I am confident that Congress, the Administration, the university community, and the private sector will be able to work together to find solutions to the cyber security challenges facing America.

[The prepared statement of Mr. Costello follows:]

PREPARED STATEMENT OF REPRESENTATIVE JERRY F. COSTELLO

Good morning. I want to thank the witnesses for appearing before our committee to examine the federal cyber security research and development activities and implementation of the *Cyber Security Research and Development Act* (P.L. 107–305).

The *Cyber Security Research and Development Act* authorized $903 million over five years for new federal programs to ensure that the U.S. is better prepared to prevent and combat terrorist attacks on private and government computers. The legislation was developed following a series of post-September 11th Science Committee hearings on the emerging cyber-terrorist threat and the lack of a coordinated U.S. response. Despite this new legislative and programmatic initiative, our computer and communications networks, upon which the country's economic and critical infrastructures for finance, transportation, energy and water distribution, and health and emergency services depend, are still among the Nation's vulnerabilities. In addition, funding for FY 2003 and proposed funding for FY 2004 is significantly below the authorized levels.

As a result, valid concerns remain that the U.S. is still not appropriately organized and prepared to counter and respond to cyber security. Multiple federal agencies, as well as institutions of higher education and the private sector, have critical roles to play; yet, no enactment of or planning for the National Strategy has occurred and there is no evidence of coordination among agencies as they developed their research and development budget requests for FY 2004. The absence of a clear advocate for cyber security at the Department of Homeland Security, coupled with the Administration's decision in February 2003 to eliminate the President's Critical Infrastructure Protection Board, is of particular concern. Further, I am interested to know from our witnesses how the Administration determines where the emphasis should be in cyber security and how this is reflected in the agency's budget requests.

I again thank the witnesses for being with us today and providing testimony to our committee.

[The prepared statement of Ms. Johnson follows:]

PREPARED STATEMENT OF REPRESENTATIVE EDDIE BERNICE JOHNSON

Thank you, Chairman, for calling this important hearing to examine federal cyber security research and development (R&D) activities and the *Cyber Security Research and Development Act* (P.L. 107–305) and I also want to thank our witnesses for agreeing to appear today.

Cyber security is an emerging concept that will redefine computer science and engineering in our nation as we know it.

Last February, the Administration released its long-awaited National Strategy to Secure Cyber Security. However, it seems that cyber security has slipped in importance for the Bush Administration. Rather than target specific industry segments and require that they secure themselves by recommending tough new laws and regulations, the Administration's plan recommends that industry and individuals simply take greater care.

Overall, the new DHS's $37.7 billion budget earmarks only $3 billion for cyber security. So the Infrastructure Protection directorate, one of five directorates in the DHS, appears in line for less than 10 percent of funds.

To be fair, the DHS is an immense undertaking, the biggest government reorganization effort since the Department of Defense was created after World War II. Such a reorganization will require time.

Unfortunately, the Administration does not address criticism that its lack of regulations render it toothless. For example, previous, unpublished drafts had included measures that would have forced Internet service providers to offer firewalls to their users and would have a required wireless hardware makers to improve security.

It is very important that any plan from the Administration does an effective job at identifying threats. Regrettably, this plan does not propose to collect reliable data and perform the analysis necessary to define the threat. Without a reliable threat assessment, it is almost impossible to tailor an R&D program to meet real needs, let alone allocate the appropriate amount of funding to develop solutions. Hopefully, our witnesses today will be able to provide answers to our questions that will shine light on some of the short comings of the Administration's proposals.

[The prepared statement of Ms. Lee follows:]

PREPARED STATEMENT OF REPRESENTATIVE SHEILA JACKSON LEE

Mr. Chairman,

Thank you for calling this extremely timely and enlightening hearing. I also serve on the Select Committee on Homeland Security, which is now several months old. Despite the continuous pressure from Ranking Member Turner and all of the other Democratic Members, that Committee—charged with providing Congressional oversight to our nation's domestic efforts to protect the American people—has yet to hold a single substantive hearing. I am glad that as usual, the Science Committee has risen to the challenge, to ask tough questions on sensitive issues.

National security is obviously foremost on everyone's minds these days. As we work to improve our country's security, it is important that we take inventory of all systems that are vital to the functioning of the Nation, and do all we can to protect them. This certainly includes our computer networks systems that can be attacked anonymously and from far away. These networks are the glue that holds our nation's infrastructure together. An attack from cyberspace could jeopardize electric power grids, railways, hospitals and financial services, to name a few.

We are all aware of the growing number of Internet security incidents. These incidents can come in many flavors: annoying attacks through e-mails, involving such things as computer viruses, denial of service attacks, and defaced web sites; or cyber crime, such as identity theft. Such events have disrupted business and government activities, and have sometimes resulted in significant recovery costs.

Our hospitals and power grids, our communications, our transportation systems, are all critically dependent on computers and information flow and the satellites above us. A terrorist or other criminal tampering with those systems could devastate entire industries and potentially cost lives. While we have been fortunate so far in avoiding a catastrophic cyber attack, Richard Clarke, the President's cyber-terrorism czar from last year, I guess I should say "two czars ago," said that the government must make cyber security a priority or face the possibility of a "Digital Pearl Harbor."

This was truly a frightening prospect. It motivated me to get more knowledgeable and active in the area of cyber security. It motivated this committee, the Chairman and Ranking Member, to get busy on hearings and legislation. The *Cyber Security Research and Development Act* is the product of our work. Now I look forward to hearing how the Administration and the Agencies are stepping up the challenges that are before us.

Of course here in the Science Committee, we tend to appreciate good Science—good data to guide smart policy. I am troubled by the fact that it seems we still do not have good data as to what is the scope of our cyber-vulnerability. We hear almost daily anecdotal reports of viruses, or worms, and crashes, but still do not know the true magnitude of the problem. We do not know how much is at risk, how much is being spent to protect ourselves, and what needs to spent in the future.

That has led to a fairly arbitrary set of appropriations figures, probably considerably lower than what is needed, and probably not always targeted to the programs that are most likely to produce results. I am troubled by the Administration's FY04 budget request which under-funds cyber security priorities dictated by the *Cyber Security Research and Development Act.* I do not understand why NIST grant programs, which have been successful in the past, are being discarded for the near to distant future. I hear that we need to save money so that we can offset giant tax cuts for the rich that are supposed to grow our economy and create jobs.

But what kind of economy will we have if our power grid is compromised, or if people are afraid to fly because the computers that run our air-traffic have been hacked, or if we lost the Internet shopping industry? We need to make smart investments now. We need to make sure our agencies are communicating well and covering all bases, and filling in security gaps.

We are in a massive restructuring now of all of our nation's homeland security efforts. We cannot do this in the dark. We need congressional insight and oversight. We need public and private sector input. And we need guidance from the top, from the Administration.

I look forward to the dialogue. Thank you.

Chairman BOEHLERT. Thank you very much. For the purpose of an introduction, the Chair recognizes Mr. Miller of North Carolina.

Mr. MILLER. Thank you, Mr. Chairman. I am pleased to introduce Dr. Charles McQueary, who is here and I believe is a con-

stituent, so—although I think as we were chatting just before the Committee began, have you now moved within Greensboro?

Dr. MCQUEARY. Yes, I have.

Mr. MILLER. And where do you now live?

Dr. MCQUEARY. I now live in the Grandover complex, which I believe is Congressman Coble—if I am not mistaken.

Chairman BOEHLERT. The gentleman's time is expired.

Mr. MILLER. Well, I have this all prepared. I might as well go ahead.

Chairman BOEHLERT. Please do.

Dr. MCQUEARY. But I still do—I do own a home in your district, though, as you point out, that I haven't sold it yet.

Mr. MILLER. And I will speak—I hope you will speak to whoever buys the home and mention my name to them. Well, my former constituent, Dr. McQueary, is well regarded in Greensboro in both the business community and in—for his civic work. In the private sector, he was the president of the General Dynamics Advanced Technology Systems. That company focused on electro-optic undersea systems, networking and decision support systems, active control systems, and signal processing solutions and software solutions. I am told that that was a good job for Dr. McQueary. He also was a respected member of the community for his civic leadership. He was a member of the Board of Trustees of North Carolina A&T, North Carolina State University. He was on the Guilford Technical Community College as President, CEO Advisory Board. He was chairman of Action Greensboro, a political—a public education initiative, and a member of the Board of Guilford County Education Network. He was also chairman of the Board and a campaign chair for the United Way of Greensboro and a member of the Board of the World Trade Center of North Carolina. So I am pleased to welcome my former constituent, Dr. McQueary.

Dr. MCQUEARY. Thank you.

Chairman BOEHLERT. Mr. Hall was tempted to claim him for Texas. This is Dr. McQueary's first visit to the Committee, and we welcome him here. I gave you the privilege, Mr. Miller, of introducing——

Mr. HALL. Mr. Chairman, we all own Dr. Colwell, though.

Dr. COLWELL. Thank you, sir.

Chairman BOEHLERT. The other three witnesses are all good friends of long standing and have appeared many times and are valuable resources for the Committee, but this is your maiden voyage, Dr. McQueary, and we wish you smooth sailing. I avoided introducing you, because this committee created the position of Under Secretary for Science and Technology, because we thought it was so important. And I was so pleased that the Administration agreed with that and Governor Ridge did, also. But I wasn't sure if I was—I would be well-received in introducing you, because I am not sure if you want to thank me or shoot me right about now, because you have got a most demanding position. But we are glad to have you here.

And we are always pleased to see Dr. Rita Colwell back. This Committee has worked long and well with you. And we are very proud of your outstanding accomplishments and the work of the National Science Foundation. And with NIST, Dr. Arden Bement,

a good friend of long standing. We have a special relationship, too, and we are glad to welcome you back. And Dr. Tether, it is good to see you back.

I think we should all appreciate the fact that we have four critically important people performing exceptional service for the Nation in their positions. And so we anxiously await your testimony. We will start with you, Dr. McQueary. You are first up.

STATEMENT OF DR. CHARLES E. McQUEARY, UNDER SECRETARY FOR SCIENCE AND TECHNOLOGY, DEPARTMENT OF HOMELAND SECURITY

Dr. MCQUEARY. Thank you. Good morning, Chairman Boehlert, Congressman Hall, and all Members of the Committee. It is a pleasure for me to accept the opportunity to be with you today and discuss the cyber security R&D from a Homeland Security perspective. It is an honor and a great responsibility to lead the Department of Homeland Security's scientific efforts to meet the challenges of securing the technology supporting our nation's infrastructures, loosely referred to as "cyber". And I do want to say thank you for having created this position, and it is an honor for me to be the first person to fill the position. And I do thank you for the work that this committee did in forming that group.

An important mission of the Science and Technology Directorate is to develop and deploy leading technologies and capabilities so those who serve to secure the Homeland can perform effectively and efficiently. This Directorate will respond, then, to the needs and requirements in this area from within the Department.

The threats to our Homeland are many. We must constantly monitor these threats and assess our vulnerabilities to them. We must develop new or improved capabilities to counter chemical, biological, radiological, nuclear, explosive, and cyber threats and mitigate the effects of terrorist attacks, should they occur.

The Science and Technology Directorate's program must also enhance the conventional missions of the Department to protect and provide assistance to civilians in response to national disasters, law enforcement needs, and other activities. Thus, Science and Technology's key specific areas of emphasis are as follows: develop and deploy state-of-the-art, high-performance, low operating cost systems to prevent the illicit traffic of radiological and nuclear materials and weapons into and within the United States. The second item is to provide state-of-the-art, high-performance, low operating cost systems to rapidly detect and mitigate the consequences of the release of biological and chemical agents. Third, provide state-of-the-art, high-performance, low operating cost systems to detect and prevent illicit, high-explosive transit into and within the United States. Fourth, enhance the missions of all of the departmental operational units through targeted research, development, test and evaluation, and systems engineering and development. Fifth, develop and provide capabilities for protecting cyber and other critical infrastructures. The sixth item is to develop capabilities to prevent technology surprise by anticipating emerging threats. And last, develop, coordinate, and implement technical standards for chemical, biological, radiological, and nuclear countermeasures.

This Directorate will implement its activities through focused portfolios that address biological, chemical, radiological, nuclear, and cyber threats; secondly, support the research and development needs of the operational units of the Department; and last, receive innovative input from private industry and academia as well as national and federal laboratories.

Now allow me to specifically address the Science and Technology Directorate in response to cyber security concerns. The operational responsibility for this mission within Homeland Security resides with the Under Secretary for Information Analysis and Infrastructure Protection. The Under Secretary for Science and Technology carries the responsibility for ensuring that the necessary research, development, test and evaluation activities are carried out to support the IAIP mission in cyber security. In practice, the term "cyber security" is broadly defined within the community. S&T uses "cyber security" to mean "securing the availability, integrity, and confidentiality of those services provided through technology, such as hardware and software systems connected to public and private networks that support the critical infrastructures".

Our approach to cyber security is essentially to apply the technology that supports the infrastructures. To address cyber security issues, we recognize that R&D efforts are one facet of a larger mosaic that includes elements, such as identification and mitigation of the threat, industry partnership and compliance, and physical security.

Today, there are many cyber security R&D efforts underway and more yet to be established that address a range of cyber security issues. These represent opportunities for Science and Technology, our organization, to leverage existing work in order to address those needs and technology gaps that Department of Homeland Security identifies as important to securing the Homeland.

We have started to work with familiarization and coordination across the federal sector. During the DHS transition and start-up period, members of the Transition Team began to participate in the INFOSEC Research Council. Members of this Council include DARPA, the NIST, and National Science Foundation, and it is our method of coordinating with the community on this topic.

Additionally, within our staff for Homeland—for the Science and Technology Directorate, we have detailees from NIST, the Secret Service, National Science Foundation, and NSA to help craft a national strategy in cyber R&D that is required by the Homeland Security Act and to identify areas for investment that would be carried out by Science and Technology.

One of the S&T's key areas of emphasis is our role in establishing DHS technical standards, which will establish DHS performance criteria for acceptable cyber security—cyber protection technologies. Currently, there is a Memorandum of Understanding nearing completion for signature between DHS and the technical administration of the Department of Commerce. This MOU is an agreement to work together to develop common standards to support U.S. industry and the Department of Homeland Security.

As I noted earlier, it is this Directorate's role to support the needs and requirements of DHS and, in particular, those defined by the Information Analysis and Infrastructure Protection Direc-

torate to provide an enduring resource and ensure the—to provide an enduring resource and assure that the necessary RDT&E activities are carried out.

To support the IAIP mission in cyber security, we intend to create a DHS R&D cyber security center. The DHS R&D cyber security center will team with, through partnership and cooperation, with those representatives here at this table with me today. This center will provide DHS focus for R&D activities and leverage the many, many cyber security RDT&E efforts underway in the defense and intelligence, academic, and private laboratory communities. We see this as a critical—this is critical to coordinate the resources and efforts across the government R&D community to accelerate technical capabilities that address DHS priorities.

The center will have five primary roles or functions as follows. The center will promote and coordinate cyber security research, innovation, invention, and evaluation in support of the DHS mission needs. It will develop strategic research and development programs and create testing and evaluation programs to address specific gaps in U.S. cyber security capabilities. For example, a unique feature of the center will be the utilization of existing or the development of new test beds where cyber security methods, tools, and approaches can be exercised in a controlled environment and evaluated against common, accepted standards.

Developing the test beds and measurement performance standards will be an element of the center's program. It will provide communication and coordination among various public and private organizations dealing with the many diverse aspects of cyber security. The center will foster national and international cooperation in creating a robust and defensible cyber security infrastructure. It will support the operational needs of the IAIP Directorate relative to vulnerability assessments and new tools and methods for enhancing cyber security. In addition to responding to DHS research, development, test, and evaluation needs, the center will provide emergency response and reach-back capabilities to on-call technical experts to support rapid vulnerability mitigation in response to cyber threats. It will cooperate with the National Science Foundation to foster educational programs and curriculum development to help ensure the Nation has the necessary human resources to present—who possess the requisite knowledge and skills to advance and secure the Nation's cyber infrastructure. This will be done in conjunction with participating universities, who will serve as a nucleus for creating the next generation of scientists and engineers.

In closing, I would like to thank the Members of the Science Committee for the opportunity to speak with you today about the Science and Technology concept for addressing cyber security research and development. We will work hard to partner with the community to address the needs and requirements of DHS as well as those gaps that exist between the many significant projects already developed. S&T is determined to support the mission of DHS to protect the critical infrastructures of this nation by working to secure the technology that supports them.

Mr. Chairman and Members of the Committee, this concludes my prepared remarks, and I would be happy to take any questions that you might have at this time.

[The prepared statement of Dr. McQueary follows:]

PREPARED STATEMENT OF CHARLES E. MCQUEARY

Good morning Chairman Boehlert, Congressman Hall, Congressmen and Members of the Committee. It is a pleasure for me to accept your invitation to be with you today to discuss cyber security R&D. It is an honor and great responsibility to lead the Department of Homeland Security (DHS), Science and Technology Directorate's efforts to meet the challenges of securing the technology supporting our nation's information technology infrastructures, often termed "cyber." An important mission of this Directorate is to develop and deploy leading technologies and capabilities so those who serve to secure the homeland can perform effectively and efficiently—they are my customers. This Directorate will respond then to the needs and requirements in this area from within the department.

The threats to our homeland are many. We must constantly monitor these threats and assess our vulnerabilities to them; develop new or improved capabilities to counter chemical, biological, radiological, nuclear, explosive and cyber threats; and mitigate the effects of terrorists attacks should they occur. The Science and Technology (S&T) Directorate's program must also enhance all of the Department's missions, whether or not they are focused on the threat of terrorism.

Throughout the initial planning process for the S&T Directorate we have been guided by current threat assessments, our understanding of capabilities that exist today or that can be expected to appear in the near-term, and, importantly, by the priorities spelled out in the President's National Strategies for *Homeland Security, Physical Protection of Critical Infrastructures and Key Assets* and *to Secure Cyberspace.*

Thus Science and Technology's key specific areas of emphasis are to:

1. Develop and deploy state-of-the-art, high-performance, low-operating-cost systems to prevent the illicit traffic of radiological/nuclear materials and weapons into and within the United States.
2. Provide state-of-the-art, high-performance, low-operating-cost systems to rapidly detect and mitigate the consequences of the release of biological and chemical agents.
3. Provide state-of-the-art, high-performance, low-operating-cost systems to detect and prevent illicit high explosives transit into and within the United States.
4. Enhance missions of all Department operational units through targeted research, development, test and evaluation, and systems engineering and development.
5. Develop and provide capabilities for protecting cyber and other critical infrastructures.
6. Develop capabilities to prevent technology-surprise by anticipating emerging threats.
7. Develop, coordinate and implement technical standards for chemical, biological, radiological and nuclear countermeasures.

We have requested $803M in FY04 to provide applied research, development, demonstrations, and testing of products and systems that address these key areas of emphasis. This directorate will implement its activities through focused portfolios that address biological, chemical, radiological and nuclear, and cyber threats; support the research and development needs of the operational units of the Department; and receive innovative input from private industry and academia as well as national and federal laboratories. In particular, the Homeland Security Advanced Research Projects Agency (HSARPA) will have an essential role in meeting the goals and objectives of the Department and the Directorate across the range of the portfolios.

Allow me now to specifically address the Science and Technology Directorate (S&T) response to critical infrastructure protection concerns, including cyber security. Consistent with law and policy, the operational assistance and advisory role and responsibilities for certain elements of cyber security resides with the Under Secretary for Information Analysis and Infrastructure Protection (IAIP). The Under Secretary for S&T carries the responsibility for ensuring that the necessary research, development, test and evaluation (RDT&E) activities are carried out to sup-

port the IAIP mission in cyber security. In practice, the term "cyber security" is broadly defined within the community. S&T uses "cyber security" to mean securing the availability, integrity and confidentiality of those *services* provided through technology such as hardware and software systems, connected to public and private networks (i.e., voice, data and Internet Protocol networks) that support the critical infrastructures. Our concern with cyber security is essentially applied to the technology that supports the infrastructures. To address cyber security concerns, we recognize that R&D efforts are an element of a larger mosaic that includes elements such as identification and mitigation of the threat, industry partnership and compliance, and physical security.

Today there are many cyber security R&D efforts already underway, and more yet to be established, that address a range of cyber security issues. These represent opportunities for S&T to leverage existing work in order to address both those needs and technology gaps for the Federal Government and industry as important to securing the Homeland. Federal gaps are identified through annual agency and Inspector General reports required under the *Federal Information Security Management Act.* Vulnerability assessments will also help identify federal gaps. There is a wide array of technologies that address many needs today not only in government laboratories, but also throughout the commercial sector. However, the existence of many hard and currently unsolved problems, and the changing nature of the threat, will require an ongoing research effort.

We have started the work of familiarization and coordination across the federal sector. During the DHS transition and startup period, members of the transition team began to participate in the Infosec Research Council. Membership in this council includes DARPA, NIST and NSF; and it is our means of coordinating with the community on this topic. In addition, we have been in communication with the Office of Science and Technology Policy, and will be participating in the interagency R&D coordination activities of the National Science and Technology Council.

One of S&T's key areas of emphasis is our role in establishing DHS technical standards, which will establish DHS performance criteria for acceptable cyber-protection technologies. Currently, there is a Memorandum of Understanding presented for signature between DHS and the Technology Administration at the Department of Commerce; this MOU is an agreement to work together to develop common standards to support U.S. Industry and DHS. We will work closely with NIST in this endeavor, and have a person on staff detailed from NIST to address cyber security programs and standards.

As I noted earlier, it is this directorate's role to support the needs and requirements of DHS, in particular those defined by the IAIP Directorate. The Science and Technology directorate carries the responsibility for ensuring that the necessary RDT&E activities are carried out to support the IAIP mission in cyber security. To provide an enduring resource to help meet our mission and responsibilities, we intend to create a DHS R&D Cyber Security Center.

The DHS Cyber Security R&D Center will team through partnership and cooperation with NSF and NIST. This center will provide a DHS focus for R&D activities and leverage the many cyber security RDT&E efforts underway in the defense and intelligence, academic and private laboratory communities. We see this as critical to coordinate the resources and efforts across the government R&D community to accelerate technical capabilities that address DHS priorities.

The center will have five primary roles or functions, as follows:

- Promoting and coordinating cyber security research, innovation, invention and evaluation in support of the DHS mission needs. It will develop strategic research and development programs, and create testing and evaluation programs to address specific gaps in U.S. cyber security capabilities. For example, a unique feature of the Center will be the utilization of existing, or the development of new, test beds where cyber security methods, tools, and approaches can be exercised in a controlled environment and evaluated against common, accepted standards. Developing the test beds and measurement-performance standards will be an element of the Center's program.
- Providing communication and coordination among various public and private organizations dealing with the many diverse aspects of cyber security. The Center will foster national and international cooperation in creating a robust and defensible cyber infrastructure.
- Supporting the operational needs of the IAIP directorate relative to vulnerability assessments and new tools and methods for enhancing cyber security.
- Cooperating with NSF to foster educational programs and curriculum development to help ensure the Nation has the necessary human resources who possess the requisite knowledge and skills to advance and secure the Nation's

cyber infrastructure. This will be done in conjunction with participating universities who will serve as a nucleus for creating the next generation of scientists and engineers.

Although much of the S&T portfolio will be focused on very difficult problems requiring extensive research, a portion of the program will be dedicated to addressing nearer-term problems in support of DHS mission requirements. In addition to establishing the center through FY03 funding, S&T will begin work on the following specific areas:

- Supporting the U.S. Secret Service National Threat Assessment Center and CERT/Coordination Center at Carnegie Mellon University on a comprehensive assessment of Insider Threats and defense strategies.
  - The need to identify and mitigate the insider threat is critical to the physical and cyber security plans of the critical infrastructures of the United States.
  - Reducing the ability of inside actors to assist outside threats will provide increased security to the critical infrastructures of this country.
- Conducting a feasibility study for trace-back and geo-location of source attack.
  - The watch and warning mission of the IAIP directorate requires the ability to identify and track the source location of cyber attackers.
  - This study will determine the status of currently available trace-back and geographical location technology, capability gaps, and potential policy implications.
- Developing patch verification technology in support of IAIP's patch management efforts to accelerate the speed with which cyber-protection software updates are evaluated, validated, and applied to civilian organizations.
  - Computer network attacks have historically exploited known, published vulnerabilities. All of the infected systems were without the appropriate patches in time to close the vulnerabilities and ensure protection. As a result, there was significant economic impact and resource availability issues to the private businesses that participate in the critical infrastructure of this country.
  - Many times the failure to apply the patch was a result of time required to test the patch against a duplicate of a critical system to ensure there would be no negative impact on business or government critical services. The goal of this project is to provide an efficient, low cost solution to this problem.
  - This study will determine the feasibility of this technology and recommend potential solutions for further RDT&E.
- Expanding development of technologies for detecting covert threats that carry the risk of creating major disruption to critical infrastructures such as financial systems before they are discovered.
  - Existing intrusion and threat detection systems utilizing signature based identification often provide false positives or large amounts of log data so that their effectiveness has diminished in the overall cyber security architecture. The benefits of the next-generation intrusion detection system will identify and categorize all intrusions regardless of the threat signature.
  - This project will begin research, development, test and evaluation on next generation detection systems.
- Conducting a feasibility study for the scalability and technology application of Secure Border Gateway Protocol and Secure Domain Name Services.
  - The Secure Border Gateway Protocol and Secure Domain Name Services protocol seek to secure two vulnerable protocols, on which the movement of network traffic is depends.
  - This study will determine the feasibility and scalability of these protocols on existing network infrastructure; and make any recommendations on the need for further RDT&E if required.

We are therefore taking steps in S&T to establish key relationships with the major cyber security R&D organizations to provide a focus for DHS technology innovation and capability development in a new Center, and have defined initial projects

in support of the Secret Service and IAIP near-term needs. As the IAIP Directorate begins to define its long-term goals and needs, we will leverage other federally funded activities, academia, and private industry to provide solutions.

In closing, I would like to thank the Members of the Science Committee for the opportunity to speak with you today about the Science and Technology concept for addressing cyber security research and development. We will work with diligence to partner with the R&D community to address the needs and requirements of DHS, as well as those gaps that exist between the many productive projects already developed. S&T is determined to support the mission of DHS to protect the critical infrastructures of this nation by working to secure the technology that supports them.

Mr. Chairman and Members of the Committee, this concludes my prepared statement. I would be pleased to address any questions you may have.

BIOGRAPHY FOR CHARLES E. MCQUEARY

On January 10 President Bush announced his intention to nominate Dr. Charles E. McQueary to be Under Secretary for Science and Technology.

Most recently, Dr. McQueary served as President, General Dynamics Advanced Technology systems, in Greensboro, N.C., a company that focuses on electro-optic undersea systems, networking and decision support systems, active control systems, signal processing solutions and software solutions.

Prior to General Dynamics, Dr. McQueary served as President and Vice President of business units for AT&T, Lucent Technologies, and as a Director for AT&T Bell Laboratories.

In addition to his professional experience, Dr. McQueary has served his community in many leadership roles—as Chair of the Board, and Campaign Chair, of the United Way of Greensboro; Member of the Board of Trustees of North Carolina Agricultural and Technical (A&T) State University; Member of the Guilford Technical Community College (GTCC) President's CEO Advisory Committee; Member of Board of World Trade Center North Carolina; Chair for Action Greensboro Public Education Initiative; and as a Member of the Board of Guilford County Education Network.

Dr. McQueary holds both a Ph.D. in Engineering Mechanics and an M.S. in Mechanical Engineering from the University of Texas, Austin. The University of Texas has named McQueary a Distinguished Engineering Graduate.

Chairman BOEHLERT. Thank you very much. You are now a veteran testifying——

Dr. MCQUEARY. Thank you.

Chairman BOEHLERT [continuing]. Before the Science Committee.

Dr. MCQUEARY. Thank you.

Chairman BOEHLERT. Welcome back, Dr. Colwell. You are up next.

STATEMENT OF DR. RITA R. COLWELL, DIRECTOR, NATIONAL SCIENCE FOUNDATION

Dr. COLWELL. Mr. Chairman and Members of the Committee, I appreciate the opportunity to appear before you today to discuss the importance of improving the security of our information infrastructure.

Last November, as a result of your strong leadership, Mr. Chairman, Congress enacted and the President signed into law the *Cyber Security Research and Development Act of 2002.* This law authorizes important research and education activities to protect the Nation's critical information technology systems against failures from accident or attack. NSF is fully supportive of this action.

NSF's attention to cyber security dates back to at least 1978 with an investment in cryptography that led to the public key infrastructure that is widely used to secure cyber transactions today. In 2001, and I would point out September 6, 2001, we established a trusted computing research program to focus attention on the continuing need for research in this area. In 2002, we saw a rapid rise

in cyber security interest by the research community. And this year, I have to tell you, we are dealing with a flood of proposals as I previously shared with you. The *Cyber Security Research and Development Act* provides us with new authority and an additional sense of urgency to expand our capacity to guard against attacks on our nation's computer and network systems.

Let me briefly share with you the current state of NSF funding for cyber security research, tell you where we are—what we are doing, and then indicate where we are going. When the appropriation process was completed in February, our Cyber Directorate doubled its funding for research to $30 million. In addition, the NSF Federal Cyber Service—Scholarships for Service program provides $11 million to increase the production of information assurance and computer security professionals. A total of about $53 million is focused on cyber security, because NSF clearly understands the urgency of the need for cyber security. With these investments, NSF is focusing on discovery, learning, and innovation to secure today's systems, to embed contemporary security principles and practices in all aspects across the board of cyber systems design in many—in all disciplines, and to prepare a world-class workforce of information technology professionals with state-of-the-art security skills that span research all the way to operations.

Beginning in 2004, the entire suite of cyber security activities will be managed under one integrated, crosscutting program called "Cyber Trust." The Cyber Trust portfolio of awards will include a range of multidisciplinary, multi-investigator awards, as well as the more focused single investigator awards. And we believe this will ensure the NSF's whole investment in cyber security research and education is greater than simply the sum of its parts.

In order to generate innovative approaches to the complex computer and network security problems that our nation faces, NSF will fund projects of sufficient scope and scale to foster multidisciplinary collaboration between computer scientists, engineers, mathematicians, and social science researchers. We will make awards that range in size from single investigator grants to multi-investigator center-scale awards of up to $3 million. Now this portfolio of Cyber Trust investments will ensure that a powerful mix of cutting-edge research is funded through a number of competitive awards.

NSF will also inform the community of opportunities to compete for the center-scale awards in these, and other related areas, through programs like the STC's, the science and technology centers, the engineering research centers, and the Industry/University Cooperative Research Centers.

Now I would like to point out that we changed the title "Cyber Trust," because our understanding is that the public not only wants their information systems to be secure, but they want to be able to trust them in all kinds of situations. As a simple example, they need to be able to trust the data, their data, will be kept private. NSF believes that a highly collaborative and inclusive coordinated effort is necessary to overcome the many technological challenges that are inherent in securing the Nation's cyber systems. Accordingly, NSF will seek to establish a multi-sector cyber security partnership, a public/private partnership that will allow NSF

to develop strategic frameworks to guide future research and education investments in the field, investments that must be made by both the public and the private sectors.

NSF will engage key federal agencies in the partnership endeavor, and we have already begun to do so in discussions with NIST. We will draw on the current interagency efforts in this area. The coordination has begun strongly with NIST, because NIST has the powerful connections to industry. In addition, NSF staff are very active in formal interagency activities that support cyber security collaborations, like the INFOSEC Research Council and the 12-agency Networking and Information Technology Research and Development Interagency Working Group. We refer to this as NITRD, which NSF chairs. The Working Group, we chair.

NSF will convene a series of workshops this summer to engage researchers, educators, and practitioners in finding the most effective ways to build capacity and to build it quickly. The workshops will also examine implementation strategies to support faculty trainee-ships in cyber security. These are programs that will enable existing Ph.D.s to pursue academic careers in cyber security.

And we scheduled the meeting for mid-August to facilitate multidisciplinary research and education activities by bringing together all of the principal investigators, the PIs, from the newly integrated Cyber Trust program. Now this group of PIs will form a research collaboration network, which will facilitate interaction between groups of investigators to communicate and coordinate research efforts across disciplinary, organizational, institutional, and geographical boundaries. And the network can then be coupled to the NIST activities to speed up the practical application of the research efforts.

Mr. Chairman, the *Cyber Security Research and Development Act* addresses a very, very critical need for our nation. NSF is appreciative of the confidence you have expressed in us to lead this effort, and we intend to build on that confidence. And we will make sure that all of the funds we are allocated and appropriated will be very well used. We eagerly look forward to working with you and your staff to ensure that all of the goals of the Act are fulfilled.

Thank you.

[The prepared statement of Dr. Colwell follows:]

PREPARED STATEMENT OF RITA R. COLWELL

Mr. Chairman and Members of the Committee, I appreciate the opportunity to appear before you today to discuss the importance of improving the security of our information infrastructure. Last November, as a result of the strong leadership that you provided, Congress enacted the *Cyber Security Research and Development Act* (Public Law 107–305) of 2002. This law authorizes important research and education activities to build our capacity to gird the Nation's critical information technology systems against failures from accident or attack.

The *Cyber Security Research and Development Act* accurately focuses on the need for research, enhanced integration of activities from the diverse disciplines that impact our ability to secure our systems, and production of computer professionals with the requisite skills needed to implement the latest cyber security techniques.

NSF agrees wholeheartedly with this focus and we are moving expeditiously to address these needs, both through focused investments with current year appropriations and by carefully fashioning plans for implementation in FY 2004 and beyond.

Persistent Challenges and Preceding Actions

Computers and networked systems are ubiquitous in our society. Over the past decade, the Internet has grown tremendously, from its early state as a small net-

work of academicians, into a full-fledged vital information infrastructure that Americans rely on as much as they rely on electricity, water, and roadway networks. Entire sectors of our economy run minute-to-minute mission critical operations over nationally and internationally networked systems. The increase in our reliance on these systems, combined with the increased threat of malicious attack, has shed new light on the importance of generating new knowledge to secure them. New knowledge workers are also needed to deploy and operate these systems safely and reliably.

Today's computing and communications infrastructure does many things well, but suffers from a number of flaws and weaknesses that make it less than dependable, particularly in the case of attacks. These shortcomings include (1) latent flaws in widely distributed software, (2) decreasing diversity of software components, (3) poor technical means for managing security infrastructure, (4) inadequate technical controls for needed collaboration policies, (5) lack of convenient, scalable, strong authentication, and (6) inadequate security mechanisms for new technologies. Further, the infrastructure lacks effective means for detecting when these flaws and weaknesses are exploited, and for responding when such exploitations are detected.

It is appropriate that government devote substantial public resources to develop knowledge and capabilities in the area of cyber security. Market pressures tend to emphasize time-to-market of software and systems. Often IT products are released with known flaws that weaken reliability of the system and may create severe vulnerabilities. Improving the quality and diminishing the costs associated with embedding security principles into all cyber systems design and development will be essential to our success.

NSF has a longstanding commitment to creating new knowledge that will improve the security of our nation's computer and network infrastructure. NSF attention to cyber security dates back to a 1978 investment in cryptography, which led to the public key infrastructure that is widely used for secure cyber transactions today. Our expanded FY 2003 investments in Trusted Computing, Data and Applications Security, Network Security and the Federal Cyber Service programs shows how our sense of urgency in this field has grown. With the passage of the *Cyber Security Research and Development Act,* Congress has allowed us to act on this sense of urgency and expand the Nation's capacity to guard against attacks on our computer and network systems.

Current Year Actions

Mr. Chairman, you and this committee were an important part of the support for the appropriation increase that NSF received in February. Cyber security research funding has increased by $15 million over FY 2002 to reach $30 million. With the Scholarships for Service program, this brings the agency's total FY 2003 investment in cyber security to $41 million.

A Strategic Approach

In short NSF seeks to enable discovery, learning and innovation that will:

- Secure today's systems;
- Embed contemporary security principles and practices in all aspects of cyber systems design and development of tomorrow's systems; and
- Prepare a world-class workforce of information technology professionals, with state-of-the-art security skills spanning research to operations.

NSF will do so, informed by the interests and efforts of its partners in the cyber security field, including those in academe, industry and other government agencies.

Our investments are guided by three core strategies that have proven effective across all science and engineering domains.

1. Develop intellectual capital.

NSF invests in cyber security activities, including multidisciplinary projects, which enhance the individual and collective capacity to contribute cyber security solutions, thus building cyber security capacity for many years to come. The agency uses its competitive, merit-review process to ensure that only research and education projects of the highest quality are funded.

2. Integrate research and education.

NSF investments in cyber security integrate research and education, assuring that findings and methods of cyber security research are quickly and effectively communicated in a broader context, to a larger audience and are thus more effectively embedded in practice.

3. Promote Partnerships.

Effective collaboration and partnerships between researchers, educators and practitioners in academe, industry and government will enable the timely transformation of research outcomes into technological innovation that will secure critical cyber systems resident in both the public and private sectors. NSF has a strong institutional tradition of enabling partnerships among the Nation's leading scientists, engineers and educators. In convening researchers, educators, and other stakeholders we draw on the expertise and deliberations of a vigorous and critical scientific community, exposing new ideas and building consensus for them.

In FY 2003 and beyond, NSF will build on and increase coordination between the activities that we have supported for some years. Beginning in FY 2004, the entire suite of cyber security activities will be managed under one integrated, cross-cutting program called Cyber Trust.

I would note that we chose the title "Cyber Trust" because our understanding is that the public not only wants their information systems to be secure, but that they want to trust them in all kinds of situations. As a simple example, they need to be able to trust that data will be kept private.

The Cyber Trust portfolio of awards will include a range of multidisciplinary, multi-investigator awards, as well as more focused single investigator awards. This will ensure that NSF's *whole* investment in cyber security research and education is greater than the *sum of its parts*.

In order to generate innovative approaches to the complex computer and network security problems that our nation faces, NSF will fund projects of sufficient scope and center-scale to foster multidisciplinary collaboration between computer scientists, engineers, mathematicians, and social science researchers. Awards will range from single investigator types to multi-investigator awards of up to $3,000,000. This portfolio of Cyber Trust investments will ensure that a rich mix of cutting-edge research is funded. NSF will also inform the community of opportunities to compete for center-scale awards in these and related areas through activities like the Science and Technology Center, Engineering Research Center, and Industry/University Cooperative Research Center programs.

Identification and Coordination of Cyber Security Priorities

NSF, in its discussions with the scientific and engineering community, has identified five vital research areas at the frontier:

1. Manageable security
2. Empirical cyber security studies
3. Cyber security foundations
4. Cyber security for next generation technology
5. Cyber security across disciplines

These research areas include and are representative of the many research areas included in Section 4(a) of the Act.

NSF believes that a highly collaborative and inclusive, coordinated effort is necessary to overcome the many technological challenges inherent in securing the Nation's cyber systems. Only by drawing upon the expertise resident in relevant stakeholder organizations, including industry, academia, and government, and by aligning the interests and investments of these broad stakeholder groups, can we ensure that the best solutions are identified and enacted to protect the Nation's vital information technology resources.

Accordingly, NSF will seek to establish a multi-sector cyber security partnership. The partnership will allow NSF to develop a strategic framework to guide future research and education investments in the field; investments likely to be made by both the public and the private sectors.

NSF will engage key federal agencies in the partnership endeavor, by drawing on current interagency efforts in this area. For example, NSF staff are very active in formal interagency activities that support cyber security collaborations, such as in the Networking and Information Technology Research and Development (NITRD) Interagency Working Group (IWG) that includes representatives from the Defense Advanced Research Projects Agency, the Department of Defense, the National Security Agency, and others.

Dr. Peter Freeman, the NSF Assistant Director for Computer and Information Science and Engineering (CISE) has talked with Dr. Arden Bement to establish formal collaboration between NSF and NIST in the area of cyber security and program staff will carry the coordination forward. As chair of the NITRD IWG Dr. Freeman has also met with Dr. David Nelson, Director of the National Coordination Office for NITRD, to discuss ways to enhance the coordination activities of the IWG in the area of cyber security.

Demonstrating further NSF leadership in cyber security, an NSF/CISE Program Officer co-chairs the High Confidence Software and Systems program coordination area of NITRD. This subgroup is working to define the federal portfolio of cyber security research and development, and will identify gaps. NSF will draw upon the work of this group to inform its future research investments.

NSF also has a long tradition of working with industry partners in science and engineering. By encouraging strong industry participation in the development of a cyber security research and education framework, and in the subsequent funding of appropriate research and education activities, NSF hopes to improve both the transfer of new knowledge into the marketplace and the capacity of current and future generations of IT and information assurance professionals.

Capacity Building

To establish the partnership, NSF will convene a series of workshops to begin in summer 2003. These workshops will engage researchers, educators and practitioners representing academic, industry, and government stakeholder organizations to develop community consensus on cyber security research and education needs and opportunities. In addition to refining research opportunities, the workshops will focus on integration, scale, and capacity building.

The first workshops planned are described below.

1. Comprehensive Cyber Security Needs Assessment

In August 2003, NSF will convene an invitational workshop of academic, industrial, and government leaders to help assess the needs and identify the strategies necessary to prepare a world-class cyber security workforce. In order to facilitate educational innovation in cyber security, design concepts for new cyber security-related curricula will be devised. Implementation strategies will be discussed to determine the best way to deliver cyber security education to a broad audience. Strategies will focus on curriculum for three levels of education:

- Bachelor's/Associate's degree programs to prepare systems administration and IT security operations professionals.
- Bachelor's and Master's degree programs to prepare systems design and development professionals with specified skills in security.
- Ph.D. programs to prepare researchers and educators for careers in information security.

The workshop will also examine implementation strategies to support faculty traineeships in cyber security. These programs will enable recent Ph.D. graduates to pursue academic careers in cyber security.

Following this workshop, NSF will assess the extent to which its current capacity-building programs address the needs defined by the workshop attendees. For example, the Advanced Technology Education (ATE) centers are comprehensive national or regional cooperative efforts involving two-year colleges, four-year colleges and universities, secondary schools, business, industry, and government. This program might serve as a valuable model for other such activities in the future. In the meantime it will provide a potential platform for cyber security activities at the Bachelor's and Associate's degree levels.

I should also note that the Federal Cyber Service: Scholarships for Service (SFS) program "seeks to increase the number of qualified students entering the fields of information assurance and computer security and to increase the capacity of the United States higher education enterprise to continue to produce professionals in these fields to meet the needs of our increasingly technological society." This program directly addresses the future needs of the Federal Government for access to skilled information security Bachelor's, Master's, and Ph.D. recipients. The program also provides funding to schools to "improve the quality and increase the production of information assurance and computer security professionals through professional development of information assurance faculty and the development of academic programs."

2. Cyber Security Community

In order to facilitate multidisciplinary research and education activities, NSF will convene a meeting of all Principal Investigators (PIs) from the newly integrated Cyber Trust Program. This group of PIs will form a Research Collaboration Network. The RCN will facilitate interaction between groups of investigators, to communicate and coordinate research efforts across disciplinary, organizational, institutional, and geographical boundaries. It will lead to integration of the research activities of scientists working independently on cyber security topics of common interest, to nurture a sense of community among cyber security researchers, to attract new

scientists to the field, and to minimize isolation and maximize cooperation in research, training, outreach and educational activities. Together, the members of this network will explore further means by which to address the complex issues faced by the cyber security community as a whole.

The *Cyber Security Research and Development Act* addresses a critical weakness in the security of our nation. NSF is appreciative to the Committee for extending its confidence to us. We look forward to working with you to ensure that the goals of the Act are fulfilled.

BIOGRAPHY FOR RITA R. COLWELL

Dr. Rita R. Colwell became the 11th Director of the National Science Foundation on August 4, 1998.

Since taking office, Dr. Colwell has spearheaded the agency's emphases in K–12 science and mathematics education, graduate science and engineering education/training and the increased participation of women and minorities in science and engineering.

Her policy approach has enabled the agency to strengthen its core activities, as well as establish support for major initiatives, including Nanotechnology, Biocomplexity, Information Technology, Social, Behavioral and Economic Sciences and the 21st Century Workforce. In her capacity as NSF Director, she serves as Co-chair of the Committee on Science of the National Science and Technology Council.

Under her leadership, the Foundation has received significant budget increases, and its funding recently reached a level of more than $4.8 billion.

Before coming to NSF, Dr. Colwell was President of the University of Maryland Biotechnology Institute, 1991–1998, and she remains Professor of Microbiology and Biotechnology (on leave) at the University Maryland. She was also a member of the National Science Board from 1984 to 1990.

Dr. Colwell has held many advisory positions in the U.S. Government, non-profit science policy organizations, and private foundations, as well as in the international scientific research community. She is a nationally respected scientist and educator, and has authored or co-authored 16 books and more than 600 scientific publications. She produced the award-winning film, *Invisible Seas,* and has served on editorial boards of numerous scientific journals.

She is the recipient of numerous awards, including the Medal of Distinction from Columbia University, the Gold Medal of Charles University, Prague, and the University of California, Los Angeles, and the Alumna Summa Laude Dignata from the University of Washington, Seattle.

Dr. Colwell has also been awarded 26 honorary degrees from institutions of higher education, including her Alma Mater, Purdue University. Dr. Colwell is an honorary member of the microbiological societies of the UK, France, Israel, Bangladesh, and the U.S. and has held several honorary professorships, including the University of Queensland, Australia. A geological site in Antarctica, Colwell Massif, has been named in recognition of her work in the polar regions.

Dr. Colwell has previously served as Chairman of the Board of Governors of the American Academy of Microbiology and also as President of the American Association for the Advancement of Science, the Washington Academy of Sciences, the American Society for Microbiology, the Sigma Xi National Science Honorary Society, and the International Union of Microbiological Societies. Dr. Colwell is a member of the National Academy of Sciences.

Born in Beverly, Massachusetts, Dr. Colwell holds a B.S. in Bacteriology and an M.S. in Genetics, from Purdue University, and a Ph.D. in Oceanography from the University of Washington.

Chairman BOEHLERT. Thank you very much. And thank you very much for giving us some precise figures. And Dr. McQueary, when we get back to you, we would like some figures, if we may.

Dr. Bement.

STATEMENT OF DR. ARDEN L. BEMENT, JR., DIRECTOR, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, TECHNOLOGY ADMINISTRATION, U.S. DEPARTMENT OF COMMERCE

Dr. BEMENT. Thank you, Chairman Boehlert. It is good to be back. I want to thank you, Mr. Hall, and Members of the Com-

mittee for allowing me to testify today about the contributions of NIST to strengthen the Nation's cyber security. Let me congratulate you for your tremendous leadership in advancing robust programs to protect our nation's information infrastructure from attack.

We at NIST fully agree with the Committee that helping to ensure the confidentiality, integrity, trust, and availability of civilian information is essential to the functioning of our economy. The Cyber Security R&D Act and FISMA emphasize NIST's long-standing statutory responsibilities for developing federal cyber security standards and guidelines and conducting related research.

Let me review just a few of NIST's activities and accomplishments. In 2001, Secretary Evans approved the Advanced Encryption Standard as a federal security standard. I am pleased to report that the AES is being actively adopted by voluntary standards bodies and implemented by vendors. In fact, over 70 commercial implementations of the AES have already been validated through our Cryptographic Module Validation Program. This program has also validated over 500 other modules and another 100 or more are expected within the next year.

To give you a sense of the quality improvement that the program achieves, statistics from the testing laboratories show that 48 percent of the modules brought in for voluntary testing had security flaws that were corrected during testing. In other words, without our program, the Federal Government would have had only a 50/50 chance of buying correctly implemented cryptography.

In support of our federal responsibilities, we have published security guidelines for e-mail, firewalls, telecommuting, and business systems contingency planning. We have also published guidelines on certification and accreditation, which are key components needed for successfully implementing E-government and the new FISMA mandates for federal agencies. Hundreds of thousands of copies of our guidelines have been downloaded from our computer security resource center website. For example, over 400,000 copies of our contingency planning guide for information technology have been downloaded since its publication less than one year ago.

Our guidelines and standards provide leadership to industry as well, as much as our work is voluntarily adopted by industry. Our Smart Card Interoperatability Specification has been adopted by federal agencies and is now being considered as an ANSI standard and eventually as an international standard.

The complexity of systems is growing as components become smaller. And some of the biggest challenges are in ensuring the integrity of information as it flows from component to component within a system. This is a major area of research on our horizon, so while we are moving ahead with critical tasks that are already on our agenda, we are giving new activities priority in our base program as resources become available.

This is only a partial representation of our many cyber security-related projects and activities. Over the past three years, we have had appropriations of $26 million for grants, critical infrastructure protection, expert assist teams of which $5 million is recurring in NIST laboratory-based programs. And since 9/11, we have been

leveraging another $12 million in our Information Technology Research Program toward cyber security-related priorities.

In summary, in fiscal year 2003, approximately $24 million is being directed toward cyber security research and related programs. And I can report to you, Mr. Chairman, we have already moved out on many of the requirements specified for NIST under the Cyber Security R&D Act.

With your permission, I would like to—and also in the interest of time, submit a list of our current activities for the record.

[NOTE: The information referred to appears in Appendix 2: Additional Material for the Record.]

Chairman BOEHLERT. Without objection, so ordered. It will be included as part of your testimony.

Dr. BEMENT. We accomplished our mission working side-by-side with our federal partners. NIST understands the Committee's desire for greater interagency coordination and collaboration, and we have been reaching out to assist other federal agencies. As Dr. McQueary indicated, Under Secretary Bond will be meeting with him very soon, I think it is scheduled for May 19, to sign a Memorandum of Understanding. This MOU will establish a formal mechanism for NIST to cooperate with the Science and Technology Directorate of DHS. We continue to have regular interactions with NSF and OSTP, and we have had a long and successful relationship with both DARPA and NSA. We are moving forward with the NRC study called for in the *Cyber Security R&D Act.* We have already identified the Study Director and are ready to initiate this study, and I am pleased to say that DARPA will be joining with us in conducting this study.

Not all of our work has been accomplished from within the Federal Government. NIST awarded $5 million to nine grant recipients in intrusion detection, telecommunications, wireless security, electric power infrastructure, and compiler security, and we are expecting important advances from this grant program.

In conclusion, I continue to view cyber security research and development as having high priority for NIST and the Nation. NIST takes its role in cyber security seriously, and we will work with the Committee to ensure that we are able to carry out our mandate to work with industry, academia, and standards development organizations to assure the secure flow of vital and sensitive information throughout our society.

Mr. Chairman, I am grateful to you and this committee for your support of NIST's programs, and this concludes my prepared remarks.

[The prepared statement of Dr. Bement follows:]

PREPARED STATEMENT OF ARDEN L. BEMENT, JR.

Chairman Boehlert, Mr. Hall, and Members of the Committee, thank you for this opportunity to testify today about the contributions of the National Institute of Standards and Technology (NIST) to strengthen the Nation's cyber security. Let me congratulate you for your tremendous leadership in advancing robust programs to protect our nation's information infrastructure from attack. I know that Technology Administration Under Secretary Phil Bond and I look forward to working very closely with you to turn your visions into reality. I would like to address the questions you asked in your invitation to testify and tell you about the many important cyber security activities currently underway at NIST.

Protecting our nation's critical infrastructure is of critical importance to our economy and our well-being. The terrorist attacks of September 11, 2001 brought to the forefront the Nation's physical and economic vulnerability to an attack within our borders. Among the Nation's vulnerabilities are the computer and communications networks on which the country's financial, transportation, energy, and water systems and health and emergency services depend. These critical are the underpinning of the Nation's infrastructure and commerce. 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. . .[a cyberterrorist attack] could be more widespread and just as economically destructive." We will not be able to address these vulnerabilities without applied research and development of enabling technologies in cyber security.

The success of the Internet—connecting more than 100 million computers and growing—has far outstripped its designers' wildest expectations. Although the Internet was not originally designed to control power systems, connect massive databases of medical records or connect millions of homes, today it serves these functions. It was not designed to run critical safety systems but it now does that as well. We rely heavily on an open system of networks, so complex that no one person, group or entity can describe it, model its behavior or predict its reaction to adverse events. The porous nature of the U.S. network infrastructure leaves the Nation, including critical federal systems, open to the constant possibility of cyber attacks. Such attacks include the massive distributed denial of service attacks that overwhelm servers with access requests; defacement of web sites and the modification of electronically stored information to spread disinformation and propaganda; "Zombies" that use computers (located anywhere) as conduits for wide-scale distribution of destructive worms and viruses; and, unauthorized intrusions and sabotage of systems and networks, potentially resulting in critical infrastructure outages and corruption of vital data.[1]

Helping to ensure the confidentiality, integrity and availability of civilian information is essential to the functioning of our economy and indeed to our democracy. And, to this end, NIST has had a long-standing and successful role in working with federal agencies and industry by ensuring the protection of non-national security related cyber and information systems through standards and guidelines development, testing methodologies, conformity assessment and complementary supporting research.

In 2001, Secretary Evans approved the Advanced Encryption Standard (AES) as a federal security standard. I am pleased to report that the standard is being actively adopted by voluntary standards bodies and implemented by vendors. In fact, over 70 commercial implementations of the AES have already been validated through our Cryptographic Module Validation Program.

Enactment of the *Cyber Security Research and Development Act (CSRDA) of 2002* and the *Federal Information Security Management Act (FISMA) of 2002* has reinforced our long-standing statutory responsibilities for developing federal cyber security standards and guidelines and conducting commensurate security research. We fully appreciate and are grateful for the trust and support provided by the House Science Committee to NIST in assigning us responsibility for these critical roles. We see both of these new important laws as a "vote of confidence" in our past work and an expectation of continuing successful achievements in the future.

Today I would like to review new statutory assignments to NIST, provide you an overview of NIST's cyber security activities, and discuss some of the challenges we continue to confront.

NIST Responsibilities Under the *Cyber Security Research and Development Act of 2002*

Under the legislation, NIST is assigned responsibilities to

- Establish a program of assistance to institutions of higher education that enter into partnerships with for-profit entities;
- Institute a program to award post-doctoral research fellowships to individuals seeking cyber security research positions;
- Develop checklists that minimize security risks associated with Federal Government computer hardware or software systems;

[1] *CNET News,* "Calculating the Cost of Slammer," Robert Lemos, February 3, 2003.

- Ask the National Research Council of the National Academy of Sciences to study the vulnerabilities of the Nation's infrastructure and to make recommendations for appropriate improvements;
- Support and consult with the Information System Security and Privacy Advisory Board, which has the mission to identify emerging issues related to computer security, privacy, and cryptography;
- Conduct intramural cyber security security research; and
- Coordinate with NSF and OSTP on cyber security research.

NIST Responsibilities Under the *Federal Information Security Management Act (FISMA) of 2002*

Responsibilities assigned to NIST under FISMA include:

- Developing IT standards for federal systems,
- Conducting research to identify information security vulnerabilities and developing techniques to provide cost-effective security;
- Assessing private-sector policies, practices, and commercially available technologies;
- Assisting the private sector, upon request; and
- Evaluating security policies and practices developed for national security systems to assess potential application for non-national security systems.

FISMA also contained a number of specific assignments, including development of:

- Standards and guidelines to be used by federal agencies to categorize levels of information security according risk;
- Minimum information security requirements, such as management, operational, and technical security controls;
- An Incident Handling Guideline and a Guideline to Identifying a System as a National Security System;
- Security performance indicators; and
- An annual public report of our FISMA activities.

With these broad legislative mandates in mind, let me review NIST's activities and accomplishments in the area of intramural research, security grants, and a planned National Research Council study.

Recent NIST Intramural Cyber Security Accomplishments

In addition to the extraordinary success of the Advanced Encryption Standard, NIST has made a number of major contributions to cyber security standards and guidelines, research, and testing in order to thwart the kinds of economically disabling attacks noted previously. Here are but a sampling of numerous successes and ongoing activities:

Security Guidelines and Standards

Our base program targets the development of standards and guidelines in support of our federal responsibilities. In 2002–2003, NIST published 12 security guidelines covering a wide variety of topics such as e-mail, firewalls, telecommuting and business systems contingency planning. We have also published 10 draft guidelines for review by federal departments and agencies as well as other interested organizations and individuals concerning such topics as certification and accreditation, awareness and training, and considerations in Federal Information technology procurements. The certification and accreditation guidelines are a key component needed for successful implementation of the e-government and FISMA mandates for federal agencies. Additionally, we have issued numerous NIST Information Technology Laboratory (ITL) Bulletins during the last year to provide guidance to agencies and others on a broad list of topics. Our guidelines and standards provide leadership to industry as much of our work is voluntarily adopted in industry. For example, our Smart Card Interoperability Specification has been adopted by federal agencies and is now being considered for adoption by an ANSI Standards committee and eventually as an international standard. All of our work is posted on our Computer Security Resource Center website. Hundreds of thousands of copies of our guidelines have been downloaded from this online site. For example, over 400,000 copies of our Contingency Planning Guide for Information Technology have been downloaded since its publication less than a year ago.

Security Testing

I mentioned previously the Cryptographic Module Validation Program through which a number of new algorithms that use the Advanced Encryption Standard are being tested. The CMVP as it is known is operated in conjunction with the Government of Canada's Communication Security Establishment. The Cryptographic Module Validation Program has now validated over 500 modules with another 100 or more expected within the next year. This successful program utilizes private-sector accredited laboratories to conduct security conformance testing of cryptographic modules against the cryptographic federal standards NIST develops and maintains. To give you a sense of the quality improvement that the program achieves, consider that our statistics from the testing laboratories show that 48 percent of the modules brought in for voluntary testing had security flaws that were corrected during testing. In other words, without our program, the Federal Government would have had only a 50/50 chance of buying correctly implemented cryptography!

In addition, in recent years we have worked to develop the "Common Criteria" which can be used to specify security requirements. These requirements are then used by private-sector laboratories, accredited by NIST, for the voluntary evaluation of commercial products needed for the protection of government systems and networks. This work is undertaken in cooperation with the Defense Department's National Security Agency in our National Information Assurance Partnership (NIAP). You may be aware that the *National Strategy to Secure Cyberspace* calls for a review of the NIAP. We have begun staff discussions with NSA to identify ways we might improve the process, through research, process changes, and to understand the resources needed for NIAP to fully succeed.

Access Control

One of the basic tenets of IT security is controlling access to vital IT resources—answering the question, "who is allowed to do what?" A NIST research team created a new approach to controlling user access, called Role-Based Access Control (RBAC). What is most striking about RBAC is its rapid evolution from a theoretical model to commercial implementation and deployment. An independently conducted NIST-sponsored economic impact study, estimated that RBAC will soon be used by some 30 million users for access to sensitive information. Further, the study estimated that RBAC technology will save the U.S. software development industry $671 million, and that NIST was responsible for 44 percent of the savings.

And, there are many, many other activities too numerous to describe here, including significant efforts in the critical areas of the security of systems controlling the U.S. Critical Infrastructure, mobile device security, network security, and security awareness. We also need to be aware of specific needs of our federal customers and work closely with them to achieve our mission. For example, OMB has asked us to assist in the preparation of E-Authentication technical guidelines in support of the E-Government initiatives. And, there are related areas of research, such as biometrics (under mandates from the USA Patriot Act) and computer forensics (used to build evidence for court cases against terrorists) in which NIST is making extraordinary contributions to the Nation's efforts to secure the critical infrastructure of the country. So, in addition to our $10M base funding for cyber security, we leverage another $14M to enable the use of technologies that support the Nation's cyber infrastructure.

But, even with our very active program and considerable interactions with industry and federal agencies, the list of critical tools still to be developed is daunting. The need for trustworthy computing systems is a theme we hear from various economic sectors on a daily basis—from financial institutions, from health care professionals, from owners and operators of utility companies—all are in need of mechanisms by which they can be assured that the information they exchange is available, confidential and that its integrity is assured. And, the complexity of systems is growing as components become smaller, and systems on a chip become ubiquitous, some of the biggest challenges are in ensuring the integrity of information as it flows from component to component within a system. This is a major area of research on our horizon. So, while we move ahead with critical tasks that already are on our agenda, we will give new activities priority in our base program as resources are available.

Interaction with Other Federal Government Agencies

We accomplish our mission working side by side with our federal partners. NIST understands the Committee's desire for greater interagency coordination and collaboration for successful science and technology initiatives and we have been reaching out to supplement and assist other federal agencies. Our Technology Administration is preparing a Memorandum of Understanding with the Science and Tech-

nology Directorate of the Department of Homeland Security (DHS) which will be signed by Under Secretary Bond and DHS Under Secretary McQueary. This MOU will establish a formal mechanism for NIST to cooperate with DHS in fulfilling their many homeland security responsibilities including cyber security R&D. The MOU is being prepared for signature by the two departmental bureaus on May 19. We have detailed one NIST senior scientist to the DHS S&T Directorate to assist with standards efforts and to avoid duplication of effort. Also, we have regular interactions with NSF and OSTP, for example in the INFOSEC Research Council (IRC). The IRC provides a community-wide forum to discuss critical information security issues, convey the research needs of their respective communities, and describe current research initiatives and proposed courses of action for future research investments. Additionally, we have also invited NSF representatives to meet with our Information System Security and Privacy Advisory Board at its June meeting. We have had a long and successful relationship with DARPA in a number of research areas, particularly in areas of networks, biometrics and language recognition technologies.

National Research Council Study of Network Vulnerabilities

As mandated by CSRDA, we are also moving forward with a National Research Council study to review the vulnerabilities and inter-dependencies in our critical infrastructure networks and identify appropriate research needs and associated resource requirements. Working with our NRC colleagues we have already identified a study director and are ready to initiate this study.

Cyber Security Research Grants

Now, not all of our work has been accomplished from within the Federal Government. NIST has provided twelve cyber security research grants in the past: one to the Critical Infrastructure Protection Project; nine under the NIST 2001 Critical Infrastructure Protection Grants Program, and two to the Institute for Information Infrastructure Protection (I3P) at Dartmouth College's Institute for Security and Technology Studies.

NIST Critical Infrastructure Protection Grants Program

In September 2001, NIST awarded $5M to nine grant recipients under the FY 2001 Critical Infrastructure Protection Grants Program (CIPGP) to improve the robustness, resilience, and security information in all the critical infrastructures. Under the competitive grant application process, we received 133 proposals requesting roughly $73M from applicants in both industry and academia. We selected proposals in intrusion detection, telecommunications, wireless security, electric power infrastructure, and compiler security.

Funded research addresses a variety of topics to include tools and methods for analyzing security and detecting attacks due to vulnerabilities introduced by merging of data networks (i.e., the Internet) and voice networks (i.e., the public switched telephone network). Other topics addressed are attack detection for wireless and converged networks, the development of security controls for protecting the North American power grid, and methods for evaluating intrusion detection systems.

While results are still preliminary from the Grants program and some projects will not be completed due to a discontinuation of program funding in FY 2002, we will still produce important results especially in the wireless area, converged data/IP networks and security of the electric power infrastructure.

Cyber Security Funding Increases

NIST takes its cyber security responsibilities very seriously and we appreciate your confidence in our abilities as witnessed by passage of the *Cyber Security Research and Development Act* and the *Federal Information Security Management Act (FISMA).* We also appreciate that in FY 2003 Congress provided $1M in funding for operation of our Computer Security Expert Assist Team capability, and approximately $2M for wireless security and networks via our Program to Accelerate Critical Information Technologies initiative.

The President's FY 2004 budget request includes increased funding for two existing NIST program areas related to cyber security research:

Biometrics Standards

The FY 2004 request includes $1M specifically for standards for biometric identification in continuing support of the USA PATRIOT Act to develop a national biometric identification system, using unique physical characteristics such as fingerprints, facial features, and eye patterns, to accurately identify people entering the United States or applying for visas. With the funding requested, NIST will help to develop effective, efficient, and interoperable biometric identifier standards, certifi-

cation tests, guidelines, and techniques for fingerprint and face recognition and verification.

Quantum Information Systems

The FY 2004 $3M requested for work in quantum information science will also have significant cyber security benefits. Quantum mechanics, the strange behavior of matter on the atomic scale, provides an entirely new and uniquely powerful way for computing and communications, potentially replacing the current binary computing and digital communications based on ones and zeros, and could have enormous impacts in homeland security. Quantum computers could perform processing tasks that are currently impossible. They also could solve problems that conventional computers could not manage given realistic amounts of time, memory, and processing power.

This enormous computational power would be particularly valuable in cryptography, making codes that would be unbreakable by the best supercomputers of tomorrow, or breaking codes in seconds that could not be cracked in years by the most powerful binary computers. Quantum information also can be used for remarkably secure communications. In this particular area, we are partnering closely with DARPA.

With the requested funding, NIST will work to develop the measurements and standards infrastructure (hardware and software) critical to the development of a quantum communications system. This includes methods to test and verify the actual performance characteristics of these systems, to determine their security properties, and to enable integration of such systems into the existing communications infrastructure.

In conclusion, NIST takes its role in cyber security seriously and will work with the Committee to ensure that we are able to carry out our mandate to work with industry, academia, and standards development organizations to assure the secure flow of vital and sensitive information throughout our society. These examples of our work and accomplishments demonstrate NIST's commitment to cyber security, across the government and the Nation. They also demonstrate the base upon which NIST hopes to build our efforts. It is an absolutely critical national need, and it is fundamental to providing the technical testing, standards and guidelines needed to protect our information infrastructure.

I am grateful to Chairman Boehlert for holding this hearing, and for his support of NIST's programs.

This concludes my prepared remarks.

I will be pleased to answer your questions.

BIOGRAPHY FOR ARDEN L. BEMENT, JR.

Arden L. Bement, Jr., was sworn in as the 12th Director of NIST on Dec. 7, 2001. Bement oversees an agency with an annual budget of about $812 million and an on-site research and administrative staff of about 3,000, complemented by a NIST-sponsored network of 2,000 locally managed manufacturing and business specialists serving smaller manufacturers across the United States. Prior to his appointment as NIST director, Bement served as the David A. Ross Distinguished Professor of Nuclear Engineering and head of the School of Nuclear Engineering at Purdue University. He has held appointments at Purdue University in the schools of Nuclear Engineering, Materials Engineering, and Electrical and Computer Engineering, as well as a courtesy appointment in the Krannert School of Management. He was director of the Midwest Superconductivity Consortium and the Consortium for the Intelligent Management of the Electrical Power Grid.

Bement came to his position as NIST director well versed in the workings of the agency, having previously served as head of the Visiting Committee on Advanced Technology, the agency's primary private-sector policy adviser; as head of the advisory committee for NIST's Advanced Technology Program; and on the Board of Overseers for the Malcolm Baldrige National Quality Award.

Bement joined the Purdue faculty in 1992 after a 39-year career in industry, government, and academia. These positions included: Vice President of Technical Resources and of Science and Technology for TRW Inc. (1980–1992); Deputy Under Secretary of Defense for Research and Engineering (1979–1980); Director, Office of Materials Science, DARPA (1976–1979); Professor of Nuclear Materials, MIT (1970–1976); Manager, Fuels and Materials Department and the Metallurgy Research Department, Battelle Northwest Laboratories (1965–1970); and Senior Research Associate, General Electric Co. (1954–1965).

Along with his NIST advisory roles, Bement served as a member of the U.S. National Science Board, the governing board for the National Science Foundation, from

1989 to 1995. He also chaired the Commission for Engineering and Technical Studies and the National Materials Advisory Board of the National Research Council; was a member of the Space Station Utilization Advisory Subcommittee and the Commercialization and Technology Advisory Committee for NASA; and consulted for the Department of Energy's Argonne National Laboratory and Idaho Nuclear Energy and Environmental Laboratory.

He has been a director of Keithley Instruments Inc. and the Lord Corp. and was a member of the Science and Technology Advisory Committee for the Howmet Corp. (a division of ALCOA).

Bement holds an engineer of metallurgy degree from the Colorado School of Mines, a Master's degree in metallurgical engineering from the University of Idaho, a doctorate degree in metallurgical engineering from the University of Michigan, and a honorary doctorate degree in engineering from Cleveland State University. He is a member of the U.S. National Academy of Engineering.

Chairman BOEHLERT. Thank you very much. And thank you for the kind words about the Committee's leadership in this area. I guess the question we have is is there a follower-ship, and we will address that in the questions.

Dr. Tether, welcome back. And I hope in your testimony you will enlighten us as to why we are moving in the wrong direction with respect to funding in DARPA for cyber security or Cyber Trust, as we now occasionally refer to it.

Dr. TETHER. Thank you very much, Chairman Boehlert, Members of the Committee. I am pleased to be here to discuss our work in cyber security, which we really refer to as "information assurance." If you would, please, accept my written testimony for the record.

Chairman BOEHLERT. Without objection, the entire written statements will appear in the record in their entirety, and we appreciate the others summarizing, and we would welcome your summary, but we are not being arbitrary with the five minutes, so don't get nervous about the green light, red light. It is just to see if we are colorblind.

STATEMENT OF DR. ANTHONY J. TETHER, DIRECTOR, DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Dr. TETHER. As you know, DARPA's mission is to maintain the technological superiority of the U.S. military by sponsoring high payoff research that basically bridges the gap between fundamental discoveries and the—their military use. The testimony goes into a little bit more detail of how we go about doing that, so I won't bother to go into that.

However, all of—DARPA is a very low-overhead organization. I would say about 98 percent of the money that is appropriated to us literally goes out to performers, and only about $100 million, or I will say three billion is really for security, operating the building, operating DARPA, paying for salaries. All the rest goes out to performers. These performers are mostly industry, but there are universities and also government labs involved. Now in doing that, we really—we partner with the services quite heavily. In fact, we contract to these performers through service organizations.

A major service organization in this area, information assurance, is AFRL in Rome, New York, as you know. They are a great partner with us, and probably—and really carry the longevity of the projects.

Basically, we mine the talents and discoveries that are created by organizations, such as NSF. We collaborate with NSF at the Program Manager level primarily to make sure that we are aware of what new is happening. And what we try to do is we try to find when an idea is ripe to be taken from an idea to an application, to a product in itself. And that is what we do and that is what DARPA has done very successfully for nearly 45 years now.

The military, however, is moving to what they are calling "network centric warfare." And this requires—and this will require that we seamlessly network the organizations, weapon platforms, people, immediately upon entry into a theater. Now this allows us to plan and execute operations more quickly and effectively than opponents. We are able to be very agile with this network centric warfare. And the recent conflicts in Afghanistan and Iraq really have given you only a hint of the power of the network centric techniques that are coming to our military.

However, while moving to a network centric warfare has created for us an enormous capability in—capability to handle—be very agile, it has also created a tremendous vulnerability. Basically, the network now must achieve the same availability, reliability, et cetera, that we used to enforce on our platforms, our weapon platforms itself. The network itself now has become the weapon.

Our enemies are watching this, and our enemies know this. So our enemies are clearly going to go and attack the network in the future as they have attacked our platforms and so in the past. Because of this, we are working hard on techniques and all to make sure that these networks can not be attacked because of the—if they are attacked, the whole—our whole capability goes down. Because of that, this is one of the reasons why our work is becoming more classified now than it has been in the past, because this—the network itself is becoming a capability and if the vulnerabilities of those networks were known, obviously it would be easy for an enemy to attack them. And if the techniques that we were developing to prevent from attacking them were known, then that is valuable information as well to an aggressor. So that is one of the reasons why you will find that in the future more and more of our work in this area will, by definition, have to become classified.

Because we are idea or project-oriented in the sense that we don't work in general, we take ideas and we create a project, it sometimes appears that we don't have a consistent thrust. But what you see—what I believe you are seeing are just the natural variations as projects are started and as projects are finished. It is true that from 2002 to 2004 it looks like our—at least our unclassified budget is decreasing in this area. What you don't have is the classified budget, and I would be happy to give that to you in a closed session. And if you saw that, you would see it probably wasn't decreasing that——

Chairman BOEHLERT. I would be a little more comfortable.

Dr. TETHER. Yeah. And most of that, by the way, once again goes through AFRL in Rome, New York. But for example, as these projects variations, in the early '90's, somebody got an idea, "Well, let us not let the attackers in." And the result of that research were firewalls. And all of the—most of the firewalls that you have now being used by people came from a DARPA program back in

the early '90's on the techniques to keep—just keep the attackers from ever getting in. However, it turns out that firewalls have flaws, and these flaws aren't necessarily the firewalls, the people that implement them.

So next we moved to detecting that an attack was going on and trying to limit the damage. However, in order to do this, we end up with high false alarm rates or false positives where we say an attack is going on and an attack really is not going on. So we developed technology to greatly reduce that false alarm rate so that when an attack—we said an attack was going on, it truly was.

Third, we finally—somebody had an idea that said, "Look, we can't keep them out. We are getting pretty good at detecting these attacks, but what we really have to do now, because the networks are becoming, really, the weapon system, is learn how to operate through the attack." In other words while the attack is ongoing to be able to still have the network operate, perhaps at a reduced capability, but degrade more gracefully than just falling off the cliff because there was an attack going on. So we have technology developments going on there.

Some of the projects we have were listed in the testimony: Cyber Panel, Fault Tolerant Networks, Dynamic Coalitions, OASIS. And what we are doing is we are taking all of this technology and we are building a prototype system where we are going to be able to take our technology and implement it in a prototype network, a very large network, 400 nodes or so, typical of a military network, and then attack it and really be able to test our technology. Unfortunately, that will be, obviously, for obvious reasons, classified.

So the last question is: Where are we going and what are our priorities? I believe that you asked that. As I said, we are focused on the problems that DOD must solve for network centric warfare. And these include problems not currently faced by the commercial world. DOD networks are—can be characterized as large, distributed, mobile networks of networks becoming increasingly wireless. We are facing very sophisticated attackers. I mean, these aren't just hackers going and erasing for mischief but really attackers whose life depends upon taking the network down. These networks have to assemble and reassemble on-the-fly, and they have to do this without any fixed infrastructure. In other words, we can't go in and put towers up and then have the networks arrive. These networks have to basically be what is known as a peer-to-peer network where each node in itself becomes the relay for communicating with other people.

We are really far ahead of the commercial world in this regard, but there is great commercial interest in these DOD networks, especially those that do not require a fixed infrastructure, and the reasons for that are obvious: cost. If we could have a cellular network that didn't require the towers where each cell phone itself was a relay, you obviously have saved a lot of money on building the towers and also saved a lot of money in trying to get the towers put up.

Now I know that—again, and I will close with that—you have been concerned about our level of funding, but let me assure you that we have, and will continue to have, a very robust program in information assurance, because we have to. The whole structure of

the DOD depends upon that. And while we are putting more emphasis on the military's specific problems, the work we are doing will have a long-term beneficial impact on the commercial world, mainly because we are developing all of the capability in industry, and industry will undoubtedly take that capability and go two ways with it: one for the military and also one for the commercial world.

And with that, I will be glad to answer any questions you might have.

[The prepared statement of Dr. Tether follows:]

PREPARED STATEMENT OF ANTHONY A. TETHER

Mr. Chairman, Committee Members, and staff: I am Tony Tether, Director of the Defense Advanced Research Projects Agency (DARPA). I am pleased to appear before you today to talk about DARPA's work to develop secure Defense networks and how that work relates to the subject of cyber security, or what we call information assurance.

Some of you may not be familiar with DARPA, so let me begin by saying a few words about who we are and what we do.

Since the time of Sputnik, DARPA has had a special mission within the Department of Defense (DOD): maintain the technological superiority of the U.S. military and prevent technological surprise from harming our national security. DARPA does this by sponsoring revolutionary, high-payoff research that bridges the gap between fundamental discoveries and their military uses.

Let me tell you a little bit about how DARPA works.

Imagine a science and technology (S&T) investment time-line that runs from "Near" to "Far," indicative of how long it takes for an S&T investment to be incorporated into an acquisition program. On the "Near side" of this timeline we have a lot of investment that represents most of the work of the Service S&T organizations. This S&T tends to gravitate towards the Near side because the Services emphasize providing technical capabilities critical to the mission requirements of today's warfighter. This excellent work continuously hones U.S. military capabilities. However, it is typically focused on known systems and problems.

In contrast, out at the other end of the investment timeline—we'll call this the "Far side"—there is a much smaller investment that represents funding fundamental discoveries, where new science, new ideas, and radical new concepts typically first surface. People working on the Far side have ideas for entirely new types of devices, or new ways to put together capabilities from different Services in a revolutionary manner. But, the people on the Far side have a difficult, and sometimes impossible time obtaining funding from the larger, near side investors because of the near side's focus on current, known, and pressing problems.

DARPA was created to span the gap between these two groups. DARPA's mission is to find the promising ideas (and people) out on the Far side and accelerate those ideas to the Near side as quickly as possible. DARPA emphasizes what future commanders might want and pursues opportunities for bringing entirely new core capabilities into the Department.

Hence, DARPA mines fundamental discoveries—the Far side—and accelerates their development and lowers their risks until they prove their promise and can be adopted by the Services. DARPA's work is high-payoff *precisely* because it fills the gap between fundamental discoveries and their military use.

What is surprising to many people, but entirely in-line with DARPA's mission, is that only about five percent of DARPA's research is *basic* research. Basic research, much of that "Far side" investment, is primarily supported by organizations like the Office of Naval Research (ONR), the National Science Foundation (NSF), the National Institutes of Health (NIH), and the Department of Energy (DOE).

Basic research creates new knowledge and technical *capacity,* whereas DARPA creates new *capabilities* for national security by accelerating that knowledge and capacity into use. So we count on institutions like ONR, NSF, NIH, and DOE to provide us with a feedstock of revolutionary technical concepts that we, at DARPA, can then develop and turn into revolutionary Defense capabilities.

Through the years, DARPA has refocused its work in response to evolving national security threats and technological opportunities, and DARPA's *Strategic Plan* describes how we are pursuing our mission today. One of our eight strategic thrusts is Robust, Self-Forming Networks, which contains our work in information assurance.

Let me briefly describe it to you:

DARPA's Strategic Thrust in Robust, Self-Forming Networks

The Department of Defense is in the middle of a transformation to what is often termed "network centric warfare." In simplest terms, network centric warfare is when military organizations and systems are seamlessly networked to change the terms of any conflict to favor U.S. and coalition forces. It will allow the United States and our allies to go beyond a simple correlation of local forces by providing them better information and letting them plan and coordinate attacks far more quickly and effectively than our adversaries can.

However, at the heart of this concept are survivable, assured, spectrum-agile communications at both the strategic and tactical levels. The goal of this work is a high capacity network that degrades softly under attack, while always providing a critical level of service.

To support this vision, DARPA is conducting research in areas that include: (1) self-forming *ad hoc* networks; (2) high capacity, multiband, multimode communications systems; (3) ultra-wideband communications; (4) spectrum sharing; (5) low probability of detection/intercept/exploitation communications; and, (6) information assurance or cyber security.

I could spend pages describing our efforts in the first five areas. However, our focus today is cyber security, so let me turn to what we are doing to ensure that those military networks are secure and reliable.

DARPA's Information Assurance Research

What we at DARPA call "information assurance" (often referred to as "cyber security") is crucial to having the robust, self-forming networks required to successfully conduct network centric warfare. One must look no further than the ongoing Iraq War to see that the United States has been moving toward network-centric warfare.

While people can debate the extent to which we have achieved network centric warfare, today's U.S. military forces are unmistakably *network-dependent*. Therefore, the very first thing that a sensible adversary would do to asymmetrically negate the U.S. force is take down our military networks. For quite some time, we have faced the very difficult problem of figuring out how to protect our military networks.

DARPA has had information assurance work going on in some form and by some name for decades. But, in the early 1990s we started to concentrate in earnest on the problem of information assurance, with the usual DARPA focus on solving extremely hard problems. Initially, our emphasis was to secure hardwired computer networks. DARPA's approach to solving the problem of information assurance evolved, over time, to a layered approach.

The first layer that we worked on in the early 1990's was preventing, or "locking out" cyber attacks. This resulted in the "firewalls" that are commonly available in the commercial world today.

In fact, today's commonly available commercial firewalls started with a DARPA project to protect the World Wide Web at the White House. The DARPA contractor that did this work published the firewall source code in the open literature, and from that work grew over a hundred firewall companies and an entire market for firewall products.

The second layer in DARPA's approach to information assurance has been detecting attacks and limiting their damage. In addition to intrusion detection, DARPA has more recently demonstrated both hundred-fold reduction in the false alarm rates that plague current intrusion detection systems, and the ability to detect new and novel forms of attack through anomaly based detection. Over the last two years, DARPA has demonstrated such detection capabilities in the field in major exercises such as the Navy Fleet Battle Experiment series.

A third pursuit, and one that DARPA has been increasingly emphasizing, is developing the ability to operate *through* cyber attacks. The simple logic here is that we simply cannot block all attacks, nor can we completely limit the damage from attacks. So we have to be able to continue operating while an attack is underway, in spite of the damage that the attack may inflict.

Let me give you a flavor of where we are today in some of the information assurance programs that we are working on at DARPA right now:

- The **Cyber Panel** program is working on ways to detect new attacks in real-time, including previously unknown attacks, predict what damage the attacks will inflict, and implement effective defenses.
- The **Fault Tolerant Networks** program is working on ways to ensure that a network remains available, even during an attack, while restricting the network resources available to the attacker. In fact, this program has resulted

in a commercial product, Peakflow™, that is being used to protect against Distributed Denial of Service attacks.

- The **Dynamic Coalitions** program is working on methods to quickly set up secure networks—a critical problem for today's U.S. fighting forces. Some of this technology is being used in the joint DARPA–Army Future Combat Systems program, a program that has network centric warfare as a starting assumption.
- The **Organically Assured and Survivable Information Systems** (OASIS) program is working to provide a "last line of defense" by developing ways to enable critical DOD computers (as distinct from the network level) to operate through a cyber attack, degrade gracefully if necessary, and allow real-time, controlled trade-offs between system performance and system security through such techniques as redundancy and diversity of operating systems.

A prototype military system to produce Air Tasking Orders for the U.S. Air Force is also being developed. The system, and the underlying information assurance technology, will be tested in 2004 by subjecting it to a sustained cyber attack from a "red team."

Much of what we have done, particularly for wired systems, has proved useful in both commercial and military systems. But, our focus is the specific problems DOD needs solved for network centric warfare.

The military-specific problems that we are working on go beyond those faced by the commercial world today. Military networks, more than commercial networks, involve large-scale, highly distributed, mobile networks-of-networks that are increasingly wireless, deal with time-critical problems, and face potential attackers who are extremely dedicated and sophisticated. Failure in military networks has extreme consequences.

Moreover, network centric warfare involves networks that must assemble and reassemble on-the-fly on an *ad hoc* basis without having a fixed or set infrastructure in-place. In effect, we must achieve what has been called, "critical infrastructure protection" without infrastructure.

In the most advanced cases, these are peer-to-peer or "infrastructure less" networks. There is no fixed, in-place network equipment—the whole network architecture is fluid and reassembles dynamically. It could be that, in the long-term, commercial networks will acquire some of these features, but, for now the Department of Defense is in the lead in facing these problems.

DARPA is taking a broad-based view of information assurance. When we think about information assurance, we include technology such as communications security and encryption as part of our solution. The threat to military networks is not simply hackers, but organized and well resourced nation states that want to eavesdrop on military network traffic, or interfere with it at precisely the wrong time.

In fact, information assurance in a world of growing network centric warfare must become a regular feature of most military programs—in the same sense that everyone building an airplane must consider materials, not *only* material scientists.

A significant and growing element of DARPA's work in information assurance is classified, and cannot be discussed in this forum. The future thrust is for more of these efforts to become classified. Why? Because of our increasing dependence on networks, their vulnerabilities and techniques for protecting them become more and more sensitive. Accordingly, our efforts have become classified.

In the longer-term, I expect that DARPA's strategic thrust in Cognitive Computing could also lead to important contributions to information assurance. While I cannot discuss it at length today, our Cognitive Computing thrust aimed at developing computers and networks that are "self-aware"—that is, computers that actually *know* what they're doing and *know* what is happening to them.

Future network-centric warfare systems will be able to leverage "self-aware" capabilities to determine when they are under attack and autonomically respond, and reconfigure themselves in much the same way as the human body reacts to an infection. If such systems could be built, they should be able to do a much better job of protecting themselves because they will understand that they're being attacked.

I realize that there has been some concern about DARPA's level of funding in the area of information assurance. For example, some have expressed the opinion that our budget for this effort is dropping drastically.

Let me reassure you that we have a robust program in information assurance, and we plan to continue this robust program in the coming years. There are natural variations in our budget, and they are due to several factors such as when large programs like Fault Tolerant Networks and OASIS come to an end.

The budget structure does not always capture the great variety of information assurance work going on, particularly when it is an integral part of another program, as it is in Future Combat Systems. And, there are the aforementioned classified programs that obscure the budget picture.

Thus, while we are putting more emphasis on military-specific problems, we will continue to have a robust program that will, in the long-term, have a broad, beneficial impact on the commercial world.

Finally, I understand that a particular interest of the Committee is how we coordinate and disseminate the results of our research to other federal agencies and to the commercial world.

Much of our interaction with industry stems from using companies as performers of our research, and the strong desire of smaller commercial firms to commercialize their technology. For instance, in 1999 DARPA foresaw the threat of Distributed Denial of Service that hit Yahoo and e-Bay a few years later, and invested accordingly to create the Fault Tolerant Networks program. Today, the nascent market for solutions against this threat consists primarily of technologies that have their roots in DARPA research, technology that can protect the military, like the example I mentioned earlier.

DARPA also makes efforts to broadly communicate our results in a more structured way by sponsoring the DARPA Information Survivability Conference and Exposition (DISCEX) conferences. The audience at DISCEX is very broad, and it includes the extended research community, the operational military, developers of military systems, and the commercial industry that generates the "off the shelf" systems that comprise most military information systems.

Our goal in these meetings is to stimulate scientists, developers, and joint operational customers with research products, experimental results, and capabilities emerging from DARPA research to better address the military's needs for information security. The most recent conference included over 250 attendees with 60 researchers giving technology demonstrations and produced two volumes of technical proceedings.

In addition, while many ideas on information assurance are being exchanged informally through the professional relationships between researchers and the U.S. Government officials who sponsor their work, DARPA is the primary sponsor of the Infosec Research Council (IRC), an informal coordinating body begun in 1996 that is comprised of U.S. Government members concerned with funding and conducting research in information security/information assurance/cyber security. The IRC members include DARPA, the National Security Agency, the National Science Foundation, the National Institute of Standards and Technology, the Department of Energy, and the Federal Aviation Administration.

I should also mention the collaborations and consultations between NSF and DARPA personnel. This interaction goes beyond the simple exchange of technical information that typically characterizes interagency information exchange programs.

DARPA and NSF personnel for example co-fund particular projects where a true synergistic opportunity exists. NSF's program, "Ultra-High-Capacity Optical Communications: Challenges in Broadband Optical Access, Materials Processing, and Manufacturing" has direct participation by DARPA personnel and a modest level of DARPA funding. NSF personnel likewise take part in DARPA source selection panels where similar technical interests can be found.

NSF's "Networking Research Testbeds Program" is of special interest to DARPA in that it offers the possibility of making available world-class network testbeds to DOD contractors and personnel. Network testbed collaboration meetings are now routinely held by DARPA and NSF program managers, and I expect that these testbeds will be very useful as we explore alternative architectures, systems and protocols for future optical networks; wireless networks based on spectrum sharing; distributed sensor networks; and networking in highly dynamic and/or harsh environments. We have also been having discussions with NSF personnel about our thrust in Cognitive Computing.

The Department of Defense is steadily increasing its dependence on information systems that are crucial to our future vision of network centric warfare. I hope my remarks today have given you a sense of what DARPA is doing to ensure that those networks perform reliably and that they remain secure.

I would be happy to answer your questions.

BIOGRAPHY FOR ANTHONY J. TETHER

Dr. Anthony J. Tether was appointed as Director of the Defense Advanced Research Projects Agency (DARPA) on June 18, 2001. DARPA is the principal Agency within the Department of Defense for research, development, and demonstration of

concepts, devices, and systems that provide highly advanced military capabilities. As Director, Dr. Tether is responsible for management of the Agency's projects for high-payoff, innovative research and development.

Until his appointment as Director, DARPA, Dr. Tether held the position of Chief Executive Officer and President of The Sequoia Group, which he founded in 1996. The Sequoia Group provided program management and strategy development services to government and industry. From 1994 to 1996, Dr. Tether served as Chief Executive Officer for Dynamics Technology Inc. From 1992 to 1994, he was Vice President of Science Applications International Corporation's (SAIC) Advanced Technology Sector, and then Vice President and General Manager for Range Systems at SAIC. Prior to this, he spent six years as Vice President for Technology and Advanced Development at Ford Aerospace Corp., which was acquired by Loral Corporation during that period. He has also held positions in the Department of Defense, serving as Director of DARPA's Strategic Technology Office in 1982 through 1986, and as Director of the National Intelligence Office in the Office of the Secretary of Defense from 1978 to 1982. Prior to entering government service, he served as Executive Vice President of Systems Control Inc. from 1969 to 1978, where he applied estimation and control theory to military and commercial problems with particular concentration on development and specification of algorithms to perform real-time resource allocation and control.

Dr. Tether has served on Army and Defense Science Boards and on the Office of National Drug Control Policy Research and Development Committee. He is a member of the Institute of Electrical and Electronics Engineers (IEEE) and is listed in several Who's Who publications. In 1986, he was honored with both the National Intelligence Medal and the Department of Defense Civilian Meritorious Service Medal.

Dr. Tether received his Bachelor's of Electrical Engineering from Rensselaer Polytechnic Institute in 1964, and his Master of Science (1965) and Ph.D. (1969) in Electrical Engineering from Stanford University.

DISCUSSION

Chairman BOEHLERT. Thank you very much. Thank all of you. Which one of you is the lead agency in cyber security? Tell me what that means being the lead agency.

Dr. COLWELL. As the lead agency in cyber security, we, particularly in the area of research, work together with the other agencies to coordinate the focus of the research and to ensure that there is integration of the research effort, non-duplication, and there is enhancement in access, particularly the role of NSF, access to outstanding science to the other agencies. And we——

Chairman BOEHLERT. So that is sort of an interagency coordinating committee? Is that——

Dr. COLWELL. Yes, we have a working group, the NITRD Working Group, the Networking and Information Working Group that is chaired by Peter Freeman. We also have another—we have other information technology coordinating groups, and we work together in ensuring that we know what the other is doing, particularly strong with NIST, because NIST acts as the standards——

Chairman BOEHLERT. But am I—are we to assume that your coordinating group, for example, as Dr. Tether pointed out to us that increasingly a higher percentage of their work is in a classified arena, do we assume that all of the members of the coordinating group or Working Group have the necessary security clearance in order to deal in the responsible way that that work that DARPA is doing and—in the black area and that you can factor that in as you determine the direction you are going——

Dr. COLWELL. Yes.

Chairman BOEHLERT [continuing]. For the government?

Dr. COLWELL. Yes, as a matter of fact, that is the case. And we have detailed to Dr. McQueary's—an NSF individual, who has been cleared and who is working to connect to agencies and to provide, initially, the capability for cyber security within Homeland Security.

Chairman BOEHLERT. Well, I hope you all can comfort me and the Members of the Committee, so if you know the answer, I would like, but I am not sure it is the answer that you can feel comfortable in giving me. But are each of you convinced that in your agency and within the government we are giving sufficient priority to the needs of cyber security? We will start with you, Dr. McQueary.

Dr. MCQUEARY. If you ask are we giving sufficient priority, today the answer is probably no, but I do believe that we have a plan in place to be implemented quickly that will put the proper emphasis on it. And that major emphasis from a Department of Homeland Security standpoint, will come from the Information Analysis and Infrastructure Protection Directorate, and the Science and Technology Directorate will be actively working with them to—from the scientific and technological aspect of it.

Chairman BOEHLERT. Dr. Colwell, I think you have already really answered that question.

Dr. COLWELL. Yes. I would say that I agree with Dr. McQueary. We—as a Nation, we are not focusing sufficiently on this very real threat. I have just come back last night from a meeting in London of the science—my counterparts in the science agencies. It is an international problem. And we also need to understand that we are increasingly being cyber security attacked from outside the country as well as hackers within. And I think we are beginning to understand how serious this problem is that we haven't really gotten to where we should be, in my opinion.

Chairman BOEHLERT. Dr. Bement.

Dr. BEMENT. This requires a very comprehensive approach. Through our work, we have worked not only with industry but academia and also international bodies and also all of the federal interagency coordinating boards and councils to improve the information technology R&D working group, which up until recently was chaired by a person from NIST, Cita Furlani, who is now our CIO. We have a pretty good fix on where the vulnerabilities are. I think we have done enough workshops with industry and different industrial sectors that we know where many of the vulnerabilities are in some of their control networks and in information systems. And you are right. This is going to require a much higher level of effort than we have currently engaged in, and it is going to have to come fairly soon if we are going to meet some of the vulnerabilities that currently exist.

Chairman BOEHLERT. Dr. Tether.

Dr. TETHER. Given that we are idea oriented and project oriented, I—we are not lacking for funds. We are, perhaps, lacking for ideas. And what you see happening right now is—and one of the reasons why the budget is coming down is that current programs are ending very successfully. But on the other hand, we don't really have the number of ideas in this area to solve the problem that the DOD faces. I have funded every idea that has come forth in this

area over the last year, including building the infrastructure to allow people to have a test bed and a lot of other things. So we are more idea limited right now than we are funding limited. Now that is why we spent a lot of time dealing—collaborating with organizations like NIST and NSF, and we will with Chuck as soon as we figure out where—what his address is.

Chairman BOEHLERT. Well, in all fairness to DHS, I mean, they just stood up, what, 1 March, and they have got a monumental task, but——

Dr. TETHER. But we will do that, and in fact, in this case, he has got quite a few DARPA people there, so the—you know, the relationship between the two organizations is very good from the start. But we are constantly searching for ideas. And right now, this is a very tough problem. And from the DOD viewpoint, we can't fail. I—see, we are not as concerned—we are not concerning ourselves, and that may be discomforting to you, on the commercial networks. Hopefully somebody is doing that. We believe our technology will apply, but if we don't solve this problem of making these networks reliable and available through attacks, the whole military structure that we are building in the future is at stake. And so we really can't fail in this area. And I hope that answers your question.

Chairman BOEHLERT. Yeah, it does. And if I were to summarize, I would think I would summarize in this way, that you all feel that we are not giving sufficient priority now, but we are moving in that direction. And we need to give it the highest of priority.

Dr. TETHER. Oh, it has to be the highest priority.

Chairman BOEHLERT. And I see all heads nodding yes, for the record. Thank you very much. My time is expired. Mr. Miller.

Mr. MILLER. Thank you. Dr. McQueary, the realization that you were no longer my constituent diminishes only slightly the pride that I feel that you were in—being in the position that you are in. And I know that the people in Greensboro feel a great deal of pride as well.

Dr. MCQUEARY. Thank you.

Mr. MILLER. And your resume does seem to be exactly what we need for your position. You have the technical expertise, and you supervise people with similar expertise. But I am wondering to whom you speak within the Executive Branch. When you are preparing a budget, who do you present it to at OMB? What is their background? What is their level of expertise? What is the highest level person in OMB who really deals only with cyber security?

Dr. MCQUEARY. I don't know—personally know the answer to that question because I haven't engaged anyone in a discussion directly in that area. I am sure I have got someone behind me who can answer the questions. If you would like me to ask them, I would be happy to do so.

Mr. MILLER. Okay.

Dr. MCQUEARY. I am told Steve McMillin is the name of the individual that we deal with, and he, of course, works for Mark Forman in OMB.

Mr. MILLER. And do you know what Mr. McMillin's title is?

Dr. MCQUEARY. No, I don't. He has the homeland security responsibility and R&D, I am told.

Mr. MILLER. Okay. I think it was just in April that Richard Clarke, who had been at the White House and involved in cyber security, said that the answer to the question who is the highest ranking person at OMB who works just on cyber security was pretty frightening. Is that still the case? Is it still a fairly low-level person or is it something that does get attention at what appears to be the appropriate levels of OMB with someone with that expertise?

Dr. MCQUEARY. I do not know the answer to the question, sir.

Mr. MILLER. Okay. A second question, it certainly appears that if—in—within the private sector that if one industry's, one company's cyber security was insufficient, if it suffered an attack, there would likely be a ripple of economic loss, a disruption to others that that business deals with. Is that generally correct?

Dr. MCQUEARY. I would say that would certainly gain a lot of attention. And I think—if I could just inject, I think it is very important that private industry play a key role in this whole issue of cyber security, because it would be—since some 85 percent of the industry is privately—what we have in this infrastructure in the country is privately held and therefore private industry has to have a strong interest in helping determine what kind of cyber security protection we must have. In fact, any CEO of a company has a responsibility to his or her shareholders to be concerned about such an issue would be my view.

Mr. MILLER. Okay. Or a little concerned not just about their—maybe to their shareholders, because their duty to their shareholders is just to be profitable, but the duty to the people with whom they do business. I know that the Administration's—or I understand the Administration's approach has been not to require by regulation cyber security standards but that the Department promulgates best practices and methodologies——

Dr. MCQUEARY. Um-hum.

Mr. MILLER [continuing]. And that that would be advice—encouragement to the private sector to adopt the appropriate level of precautions. Is that generally the approach, not require by regulation but promulgate best practices and methodologies?

Dr. MCQUEARY. If you would let me defer that question to one of my peers, who are more knowledgeable about it, I would certainly appreciate it, because I simply have not engaged myself in the short time I have been in this job and the subject to be able to speak adequately to it.

Mr. MILLER. Does anyone on the panel—yes, sir.

Dr. BEMENT. We regularly hold workshops with industry to try to understand their vulnerabilities. In fact, it has been major activities of ours over the last two or three years since 9/11. And in addressing that, we had been working with the standard development organizations to not only develop standards but also we have been working to develop prototypes to understand better what those vulnerabilities are along with test beds. In order to accelerate standards developments, we are working with the Department of Homeland Security. We have detailed one of our senior scientists, who heads up the standards activities within Dr. McQueary's organization. And we have also detailed another person, who is an expert in cyber security. And in addition to that, we have one of our

senior people working with ANSI in what is now called the Homeland Security Standards Panel, which is working with the standard development organizations to try and fast track new standards to bring new products in the marketplace that will meet the reliability and the security requirements that will meet the needs of industry in this area. So it is almost a full court press at the present time.

Chairman BOEHLERT. All right. The gentleman's time has expired. I know he has, as we all do, more questions. So we will have a second round of questioning. We will go now to the distinguished Chairman of the Subcommittee on Research, Mr. Smith of Michigan.

Mr. SMITH OF MICHIGAN. Thanks for an exceptional, qualified panel to help us decide where we should go on encouraging the directions that we think we should go to protect ourselves. It seems to me—help me understand a little bit in terms of the technology. It would seem like it is almost a weapon system. If you develop a better weapon system and then the other side develops a better weapon system, and it keeps building up from firewalls to mitigating attacks to how to operate even if the attacks are there, like you suggested, Dr. Tether. But following up a little bit on Mr. Bell's comment and Dr. McQueary's suggestion that, look, the private sector on how we use computers and software to decide how our food is going to be shipped where so it gets where it belongs to how we transmit electricity to how we run our airlines, how do you decide the balance, Dr. Tether, in protecting the kind of classified research that is going to enable our Defense Department to communicate and do things without intervention with the need to use some of that research in the private sector?

Dr. TETHER. Well, we have a—logistics is a good example of what you are talking about, which is very close to—you know, most of the Department of Defense is moving supplies. And there is a logistics organization called Transcom, which happens to be located in Illinois. We are developing for them a technique which will allow them to basically be able to go into the distributed databases to find out where supplies are and then create all of the transportation required to get those supplies to the place they are needed. And we are concerned about, once you have distributed databases, of somebody getting into that distributed database and not—either not allowing you to do it or changing the data. So it is a very crucial thing for the Department of Defense to have this be secure and assured.

Mr. SMITH OF MICHIGAN. But still, my—both my points, the more that you accommodate the need to protect in the private sector, the more vulnerable you are to discovering some of the vulnerabilities of that system after you—because it is more available.

Dr. TETHER. That is correct. And in this particular case, the technology that is being used is what we happen to call "intelligent agents". These are little software modules that effectively—think of it as a—really as an agent that goes out and looks for you and brings you back answers.

Now this is working very well. We have made it very secure. We have shown that—doing it this way, that we can, with high confidence, know that the data is not being corrupted, and that the

system can operate through an attack. The details of how we do it, in the military, are classified. However, the technology of intelligent agents, distributed intelligent agents working together to do this, is unclassified. And again, we are developing this technology with a company. And this company sees a business in it, not only for supplying the military with this capability, but also supplying private industry. Ford Motor Company has the same problem. I mean, they buy parts all around the world, and they basically have a logistics problem. How do they get parts here and there? And they are very interested in making sure that their databases are secure and that somebody doesn't get in.

So here is a company that will take the technology that was developed by the military, which will remain classified in the terms—in the context of the details, but is able to use that technology for a commercial application. I hope I am answering your question.

Mr. SMITH OF MICHIGAN. Yeah, you are, certainly.

Dr. TETHER. Okay.

Mr. SMITH OF MICHIGAN. My next question, Dr. Colwell. Anyway, good to see you. In terms of virtual centers compared to bricks and mortar centers, in our—in this Act, in our *Cyber Security Research and Development Act,* we put in language that would be directing the National Science Foundation to develop physical centers. And we put in similar language, so it is a two-fold question in the area of interest that I have expressed many times, is the biological centers that we asked for in our NSF authorization bill. And it seems in both cases you have tended to lean toward virtual centers rather than following what I consider the intent of both bills in terms of developing real centers.

Dr. COLWELL. Actually, we have physical sites that are connected. The approach that we take, and we feel is very powerful, is to bring the versatility and the diversity of capability that is located in different parts of a given region and to link them, even though they represent physical sites, to link them by the capacity of a cyber infrastructure. That means that you have, for example, the—at—in Missouri, Indiana, Illinois, and Washington State, you have different capabilities, but when brought together, it becomes a very powerful approach to addressing sequencing and getting it done rapidly and effectively. And I think similarly, what we are trying to do here, and actually it is in response, I think, to an interest of the Chairman, is to bring together, as fast as we can, the capability that is there, strengthen it, and at the same time, determine how we build further capacity through specific programs.

And I would like to address the comment about ideas. NSF is focusing research on embedded systems, like those that are used to control the Nation's power grids. And we are also looking at the interplay between the human and the computer to better understand human behavior and the use of computers and then future generations of systems that would be beyond the currently used systems. And I must tell you that there is an enormous interest in the community, because we have many, many more proposals than we can possibly fund. And these are good ideas. These are very good ideas, and they need to be pursued.

And then one very brief sideline, Congressman Smith, because I know of your interest in this, the British are very—how should I

say? They are understanding that they have got to get beyond this genetically modified food situation, and they are pushing really hard to get the acceptance——

Mr. SMITH OF MICHIGAN. I think you might be talking to the scientists rather than the traders.

Dr. COLWELL. These were folks that——

Mr. SMITH OF MICHIGAN. Oh, these are policy issues.

Dr. COLWELL [continuing]. Are policy folks. These are policy folks.

Mr. SMITH OF MICHIGAN. Mr. Chairman, thank you. But you know, both in the centers that we call for and the computer network security research centers in this cyber security bill, the advantages of the interdisciplinary individuals being able to talk to each other and feel each other out seems to me that it has a great advantage over virtual centers where you are simply putting out grants. And I yield back my time.

Chairman BOEHLERT. The gentleman's time is expired. Mr. Davis.

Mr. DAVIS. I yield two minutes of my time to Mr. Miller.

Chairman BOEHLERT. Mr. Miller is recognized for two minutes.

Mr. MILLER. Thank you, Mr. Davis. Dr. Bement, just a couple more questions. Essentially, the same question I asked of Dr. McQueary, has there been an assessment within the private sector of whether vulnerability to one entity within the private sector does have ripple effects if it causes—obviously it can cause, as Dr. McQueary points out, huge economic disruption and vulnerability to that entity. But does——

Dr. BEMENT. Yes.

Mr. MILLER [continuing]. It have a ripple effect? Does it cause—is there—would there be an expectation when this assessment of what effect it may have on others and—in—within the private sector?

Dr. BEMENT. Yes, there have been those vulnerability assessments, and let me just cite three examples. All of you know what the impact was of the strike out on the West Coast and how that tied up supply chains throughout the country and how that rippled through our economy. So our transportation systems are all interconnected and all—interconnected in terms of their vulnerabilities, and that would be a major backup. Also, with regard to our manufacturing enterprises because there is a supply chain linkage. And many of these enterprises are global in nature and depend on, again, the global supply of parts and so forth. Any disruption, especially across our borders, and especially in the Great Lakes Area with Canada and south with Mexico, that would also have a ripple effect as far as our whole logistics trains throughout the supply chain.

The other part that I would also cite is the vulnerability of our electric power grid. I might mention parenthetically that before I came to NIST, I was at Purdue University and using intelligent agents in a project co-sponsored by the Department of Defense to use intelligent agents to come up with more robust control systems to deal with upset conditions in our electric power grid. But that would also have a ripple effect, because the loss of a shunt or the loss of a major element, critical element in the electric power grid

could, of course, be propagated across the country. So that would have major implications. And one of the vulnerable components there is the Supervisory Control and Data Acquisition System, or the SCADA control system, which do have to be made secure. And NIST has been working with the industry. We have been giving grants in this area to figure out how we can deal with the security aspects of information flows that control these SCADA control networks, some of which now operate on the Internet. So you know, this is a new development in recent years using the Internet to control operations across the country.

Chairman BOEHLERT. The gentleman's time has expired. Mr. Davis, you can reclaim your time, but just let me observe that what George Carlin might refer to as the stuff of comic book lore is now a reality. I mean, we have to redefine what war is. It is very possible that the next war would not be fought with guns and bullets but with computers and—from afar. They don't even have to leave their point of origin. A nation could effectively wage war on another nation. That might not be as devastating in terms of loss of life, obviously, but the losses would be just monumental. And it is the—that is why, I mean, this committee is so concerned about cyber security and we are so avid in our pursuit of attention for this subject and trying to get people to realize what you have all acknowledged. But too many people are much too casual about it.

Mr. Davis.

Mr. DAVIS. Mr. Chairman, thank you. And I do reclaim the remainder of my time. I have basically one question. It will have a two-part to it. Many of the questions I have would have been asked and perhaps would have been asked by many, such as Mr. Miller and others, but the President, our Administration basically has described our national strategy for—to secure cyberspace is through the Office of Science and Technology Policy, which is referred to as OSTP, which basically will be coordinating, supposedly, and every year will be—each of your entities will be coordinating, bringing together information starting with fiscal year 2004. As I hear each of you giving testimony, Dr. McQueary and Dr. Tether basically mentioned the INFOSEC Research Council. Dr. Colwell, you made reference to the network and—Networking and Information Technology Research Development Interagency Working Groups. Now as I listened to each of those, I assume that perhaps each one that is providing research development is somewhere assimilating the information and then you get together with someone as you discuss what you are doing, what your research and development is providing. Are you finding working with the Office of Science and Technology Policy is—are you able to effectively work there? Are you coordinating your information together or do you find that you are basically out on your own on an island?

Dr. COLWELL. No, we are coordinating. In fact, we have had discussions, particularly on computing research, and especially effective is the—putting together the budget requests, making sure that it is coordinated, because the—I mean, I can not speak for the Science—the Director of OSTP except for my interactions and say that this is a major interest and concern of OSTP and making sure that all of the agencies are doing a coordinated effort toward solving the problem. Yes, I see that happening.

Mr. DAVIS. And that is happening, and you are happy with the coordination of it and with getting results?

Dr. COLWELL. Well, I have to, again, just as we all four of us have said, that even though we had a Cyber Trust program started September 6, before 9/11, and have gone—our work goes back to 1978, it is only in the last—I would say the last year or so that this intensive understanding of the disasters that hacking into systems creates that we now are putting a very strong attention to this.

Mr. DAVIS. Is there a plan in place, step-by-step how this is going to happen? And are you also working with private industry to gather information?

Dr. COLWELL. Yeah, the—we are developing a plan, and I think probably Dr. Bement can speak more conversantly with private industry, but we, too, work with industry in our centers, our science and technology centers, our engineering research centers, and certainly in developing a center approach for cyber security.

Mr. DAVIS. So there is not a plan currently step-by-step that is being developed?

Dr. COLWELL. Being developed.

Mr. DAVIS. I certainly hope it occurs pretty quickly. Dr. Bement.

Dr. BEMENT. Of course, one of NIST's responsibilities is look—is to look after the security of our federal agencies as far as sensitive information flows. And that work is coordinated through any number of councils: the CIO Council, the PITAC, the PCAST, the INFOSEC Research Council that has been mentioned. There is a federal security program managers' forum. And we take that information and we pull it together to develop our program and to establish our priorities. But within each one of these bodies, there are plans that, in many cases, tie back to the Office of Management and Budget, which links to the President's cyber security plan, so that—there has been a lot of planning being done. We are doing a lot within NIST. We are doing a lot of it interactively with the organizations that are represented here along with NSA and other agencies. And we look pretty much to OSTP for the coordination of the research and development program within the federal agencies through their information technology R&D working group.

Dr. COLWELL. I would like to, if I may, provide a reassurance in the fact that what you don't see, what isn't obvious, is that there is strong collaboration and cooperation. As I have said earlier, we have detailed one of our very good people to Homeland Security to help get that started up. We have been working with the intelligence agencies, the Defense agency and DARPA and with our scientist panels inviting scientists from those agencies to sit in on the NSF panels. And then where there is interest in the research that is being proposed and discussed, they can add funds to it and make sure that it gets enhanced. So we are doing quite a lot of what would be not openly and clearly visible. But there is a great deal of interaction.

Mr. DAVIS. What my hope would be, obviously, is that each different entity that is doing research and development would be able to follow a plan that would provide the information. And I am not sure that—I don't sense that that is happening today, so my hopes

are that from this hearing that there will be efforts to encourage such action to be taken.

Chairman BOEHLERT. The gentleman's time is expired. The Chair recognizes the distinguished Chairman of the Subcommittee on Environment, Technology and Standards, Dr. Ehlers.

Mr. EHLERS. Thank you. Mr. Chairman. First of all, I have been struck with all of the work that is going on in cyber security, and it sounds like very good work, what we may call "cyber defense against enemies foreign and domestic." Dr. Tether, what do you have going on in the what you might call "cyber offense," in other words cyber warfare? What—do you have programs within Defense dealing with how you would attack enemies——

Dr. TETHER. Yes, we do. And unfortunately, I probably can't say much more than yes we do.

Mr. EHLERS. All right.

Dr. TETHER. But I would be happy to come and tell you about it, I just——

Mr. EHLERS. Yeah. I——

Dr. TETHER [continuing]. Can't here. It is——

Mr. EHLERS. There may be several of us who would like to do that at some point.

Dr. TETHER. Okay. That would be fine.

Mr. EHLERS. I also was struck by, and I am paraphrasing what you said, I hope correctly, that Dr. Tether, that you said you are looking for a lot of good ideas that you can try and implement. Dr. Colwell, you were saying you have a lot of ideas but no money to do it. I would suggest the two of you get together afterwards.

Dr. TETHER. Well, we do. In fact, as Dr. Colwell said, there is an enormous amount of collaboration going on——

Mr. EHLERS. Right.

Dr. TETHER [continuing]. At the—what I would—we would call at DARPA the Program Manager level. In fact, when this hearing was called, I asked, I said, "How much"—"What is going on between us and NSF?" And I was amazed at how much was going on that I didn't know about.

Mr. EHLERS. I realize that. Dr. Bement.

Dr. BEMENT. Yes.

Mr. EHLERS. First of all, I commend you for your efforts to try to speed up the standards process for the——

Dr. BEMENT. Thank you, sir.

Mr. EHLERS [continuing]. Information technology. That is absolutely essential, because they are very frustrated and ready to set up their own informal standards organization. So I encourage you to pursue that diligently. I appreciate——

Dr. BEMENT. I will.

Mr. EHLERS [continuing]. What you have done. First question is on a type of cyber security we haven't discussed here at all and that is voting security.

Dr. BEMENT. Yes.

Mr. EHLERS. I am very, very concerned about that, because I think that is essential to the proper functioning of a democracy. And we passed a bill last year, which provided money for local governments to buy new equipment. At my insistence, responsibility was given for you to establish standards for these. And I am very

concerned. States and localities are already going out and buying equipment and—without an assurance of security. And I just covered in my conversations with elected—pardon me, election officials, who are very, very knowledgeable about the process, but many are not knowledgeable about cyber security. They just don't realize the pitfalls, and it is possible for a good hacker to basically steal an election without anyone even knowing about it the way some of the voting machines are constructed. So what is the progress on setting up the commission, setting up the standards, and so forth?

Dr. BEMENT. First of all, I agree, entirely, with your assessment. We have looked into this matter. We have research going on, and we have dealt with many vendors in trying to understand their systems. Unfortunately, much of the information is proprietary, and we almost have to reverse engineer to understand them completely. But with regard to electronic voting machines, the interface between the software and the hardware leaves plenty of room for cyber attack, for fraud, for lack of trust. We talked about trust earlier. And this is an area where we have to be very active in standards, and we feel this needs to be attended to, and we need to put much more effort behind it.

Mr. EHLERS. I urge you to pursue that very, very aggressively, because it is a major problem, and the public is simply not aware of it.

Dr. BEMENT. It has high priority, as far as I am concerned.

Mr. EHLERS. And if you need greater legislative authority to obtain proprietary information, that is something we should talk about as well, because I——

Dr. BEMENT. Well, I think we have the authority. I think we have some understanding, not complete understanding of what needs to be done. We just have to go out and get it done.

Mr. EHLERS. I appreciate that. The—also, another area within NIST, you have talked a lot about your activities of various sorts, but to what extent are you involving the higher education community? And I am talking about two ways: one is through supporting research there, but secondly through training of students. And I was astounded to discover recently that the number of math and science—pardon me, math and computer science majors graduating from undergraduate institutions today is less than it was approximately 15 years ago. And in fact, there was—it has dropped. It is starting to come back, but we are still not up where we were. Clearly, there is a real need for training of these people, and I am amazed. I just met someone in the airport the other day from my home state at a higher educational institution, a very prominent person in information technology, who was—degree was in master of divinity, and that shows maybe you need that to operate a computer properly. I have always wondered if there are any strange spirits inside of my computer. But it shows the extent to which we are recruiting from people who have not been trained——

Dr. BEMENT. Yes.

Mr. EHLERS [continuing]. In this field.

Dr. BEMENT. Clearly, the Committee has recognized one of the key issues, and that is a need for more education and training. And that is one of our biggest vulnerabilities. It is not just that we don't

have the policies and the procedures and the specifications; we don't have the trained personnel to manage the systems. And it is in this regard that we look to the National Science Foundation to do the manpower training, which we, of course, want to work with them on. But beyond that, in our post-doctorate program at NIST, which is managed through the National Research Council, we are trying to pull in more expertise at the post-doctorate level working at NIST in cyber security so that we can leverage some of our ongoing activities and so we can identify some of the new talent coming out of the universities who eventually, hopefully, will join our research staff.

Also, in linking up with the research community, I did mention that we did have $5 million that did go out in research grants to universities. We follow that quite actively. We have worked with Dartmouth in their program and helping them roadmap or at least reviewing their road map for cyber security research and development. We have similar interactions with other universities, but I think the most exciting opportunity is in the Cyber Research and Development Act. By coupling industry with academia and bringing an understanding of the needs and the technical insights, which industry can bring with the scientific insights, which academic researchers can bring to the table, and then finding ways to developing prototypes, standards, and test beds to try and reduce the lead time of getting new technologies and new approaches to cyber security into the marketplace in the earliest time possible.

Chairman BOEHLERT. The gentleman's time is expired. Ms. Woolsey.

Ms. WOOLSEY. Thank you, Mr. Chairman. Dr. Colwell, it is nice to see you, gentlemen. Thank you for knowing so much. Mr. Chairman, I have a letter here from the Information Security and Privacy Advisory Board, which is a board established and funded by the Science Committee, the Computer Security Act of 1987. And it is responding to the President's report, which is huge, that was dated February 2003. And the very final statement, I am not—of course I want to enter this into the record and ask unanimous consent to do that, but——

Chairman BOEHLERT. Without objection.

[NOTE:The information referred to appears in Appendix 2: Additional Material for the Record.]

Ms. WOOLSEY [continuing]. The last statement in the letter regarding the reports, "Additionally, the strategy minimally acknowledges the critical issues of information and citizen privacy and fails to provide specific actions or recommendation. The Board believes this must be addressed as well." And so my question to you is are we addressing—I know nothing will be perfect, but are we addressing the tradeoff between privacy and confidentiality and the need for security?

Dr. BEMENT. Well, let me respond to that. That particular board is funded by DARPA and is advisory to me—I am sorry, by NIST and is advisory to me as the Director of NIST. So we support the board and its activities. And of course, we do take their recommendations very seriously, and those eventually become priorities in our program. Recently, we have, through our interactions with the National Science Foundation and with the Department of

Homeland Security, invited them to become much more active in the workings of the board. And the board will be meeting, I think, in June. The board will be meeting in June, and we will certainly be discussing their recommendations again at that time.

Dr. COLWELL. But I would also like to add that we plan to provide more funding to make sure we understand the interplay between policy and technology and human behavior and technology and the need for privacy in developing a cyber secure system. So we intend to do a lot more research in that area as well.

Ms. WOOLSEY. And balancing the privacy piece with the security piece.

Dr. COLWELL. Yeah.

Ms. WOOLSEY. I am sure that this has been answered, but for some reason I can't wrap my mind around—my intellect around some of the technical conversation we have had here, so what I would like to do is ask you in down-to-earth questions—words a couple of things. Do we have adequate tools to—in place? Are we putting—getting ready with—for that, and if not, why not? What is holding us up? And is there a way to spread the costs of these developments among other—many agencies or private industry as well? Rita.

Dr. COLWELL. The answer is yes in that we are beginning to put together what really is needed, and that is a concerted, coordinated, and as a result of the Act that was passed, a focus on the need for cyber security. We do have components of it in place, and we are coordinating it. But we believe, at NSF, that there is a lot more research to be done, and what we are trying to do is balance the research that is needed to advance computer architecture and software development, et cetera, with this very pressing need for the security of the systems. So you can't really pull money out of the research to make better systems, because that is part of the problem, but at the same time, you can't neglect the security aspects of it. So this is a real—at this particular transition stage, this is a very difficult push and pull.

Dr. BEMENT. I would answer slightly differently. Clearly, there is a research agenda, and there is a technology agenda, but in our assessments, we find that the greatest vulnerabilities are not necessarily technical vulnerabilities. They are primarily an ill-educated user population, lack of adequate cyber security research expertise, poorly designed systems and software, specific vulnerabilities in commercial IT products, and new technologies that are coming into the marketplace with inadequate testing at the design and manufacturing stages. So a lot of what is missing is knowledge, education, and discipline in the system.

Dr. COLWELL. Could I add another comment, please, and that is to point out that what we are finding in our discussions with the community is that we really have to include in all of the information technology and computer science training an understanding of cyber security and understanding of the need for secure systems and that just having an undergraduate and graduate program on security isn't enough. It has got to go across all of the training, just as Dr. Bement has pointed out, in order for people to understand what it entails and how to address it.

Ms. WOOLSEY. I will——

Chairman BOEHLERT. The gentlelady's time—well, all right, one more.

Ms. WOOLSEY. Dr. Bement, you did say, though, we know what needs to be done, I am paraphrasing you, it's just doing it. What is stopping us?

Dr. BEMENT. Nothing is stopping us. Of course——

Ms. WOOLSEY. Is it time?

Dr. BEMENT [continuing]. Resources—we could accelerate if we had more resources, but a lot of it——

Ms. WOOLSEY. Resources. Well, that is stopping. That is an answer.

Dr. BEMENT. A lot of it is in the private sector. A lot of it requires better protocols, better metrics, better standards. We are working with the standard development organizations in this area. It will take time. It is comprehensive. Resources will help.

Chairman BOEHLERT. You know—thank you. The gentlelady's time is expired. Dr. Tether pointed out a, I think, very appropriate observation that DARPA is sort of idea limited. And that is one of the reasons why, in the cyber bill, we put in all of those programs for students and to get researchers to change fields. Shouldn't funding for those programs be a top priority? And will NSF and NIST ask for funding for those programs in '05?

Dr. COLWELL. I can respond, sir, and say that we are going to be very aggressive in our request for the area of research in '05.

Chairman BOEHLERT. Dr. Bement.

Dr. BEMENT. I would respond likewise. We are taking it seriously. We have discussed it with the Technology Administration. We are still early in our '05 planning, but we are giving this very high priority.

Chairman BOEHLERT. Thank you very much. The Chair now recognizes Mr. Smith of Texas.

Mr. SMITH OF TEXAS. Thank you, Mr. Chairman. First of all, Mr. Chairman, let me say to you that I am sorry that I missed most of the hearing today. Unfortunately, I am a Member of the Judiciary Committee, which has been marking up some legislation downstairs, and so I have had to be there for recorded votes. In fact, there is one going on now, so I will have to be brief in my questions.

Nonetheless, I did want to ask Dr. Colwell and Dr. McQueary to respond to a question that I have. And this question basically comes from a book that I read this last weekend, and I don't know if you all are familiar with it or not. It is called "Tangled Web." And this is a book that makes a compelling case that both the private sector and the Federal Government are not prepared to deal with the cyber attack today. And furthermore, Mr. Chairman, just because I am a Member of a relevant Subcommittee, and in the briefings that we have had, we had been told that there is at least a 50/50 chance that any kind of terrorist attack that might occur in the future will involve some aspect of cyberterrorism, either wholly or in part. Given the nature of that present and future threat, my question, really for the two witnesses, is do you feel that the Federal Government today is able to adequately respond to a cyber attack? It is my impression from, as I say, reading this book "Tangled Web" that we are, today, not capable of responding to a

terrorist attack and stopping it from costing American lives or perhaps disrupting the economy. But I would be interested in your perspectives.

Dr. COLWELL. Do you care to start and then I will add?

Dr. MCQUEARY. Certainly. We do have the NTAC [National Threat Assessment Center] and the Carnegie Mellon—the capability to respond if we do see a cyber attack. If—one could postulate attacks that we could not respond to, I suppose, effectively, but certainly there is a wide variety I think have been demonstrated in the past of capability to respond to any——

Mr. SMITH OF TEXAS. You feel comfortable with our ability today to not be the victim of a cyber attack?

Dr. MCQUEARY. I did not attempt to say that. What I was trying to say was that there are many kinds of attacks that we could respond to. In order to say that we couldn't respond to it, one would have to know what kind of attack——

Mr. SMITH OF TEXAS. What kind of attacks are we not able to respond to?

Dr. MCQUEARY. I don't know the answer to that, sir, off the top of my head.

Mr. SMITH OF TEXAS. How can you know what we can respond to if——

Dr. MCQUEARY. Well, because we have done this in the past through this—the NTAC and the—at the Carnegie Mellon Group, because we have demonstrated——

Mr. SMITH OF TEXAS. Right.

Dr. MCQUEARY [continuing]. That in the past, and therefore by definition, we see that we have been able to respond to things that we have seen in the past.

Mr. SMITH OF TEXAS. Dr. Colwell, do you agree with that?

Dr. COLWELL. I think that we have done research that has allowed us to build firewalls. And I think for the most part, the firewalls that protect sets of data and sets of operations are, on a daily basis, effective. Obviously, there are opportunities for attack that could be devastating. And it is hard to predict exactly what they would be, but I do feel somewhat assured by the—yesterday, the Seattle, I think it was in Seattle, there was a mock attack, which included cyber, as well, as the direct attack with chemical and biological weaponry. But I think that is important, because it shows that this is a multi-dimensional——

Mr. SMITH OF TEXAS. Right.

Dr. COLWELL [continuing]. Terrorist—potential terrorist problem. And cyber security is a component of it. And I think we are well aware of that now. And awareness is the beginning of protection.

Mr. SMITH OF TEXAS. And certainly awareness is the first step. You have both said that you feel that we have protected ourselves against cyber attacks that have already occurred, but not necessarily—we are not necessarily able to protect ourselves against all conceivable cyber attacks, is that a fair statement?

Dr. COLWELL. Well, I—yeah.

Mr. SMITH OF TEXAS. And I see Dr. Bement is shaking his head yes as well.

Dr. BEMENT. Firewalls tend to be pretty ubiquitous, but, in many cases, they don't contain all of the "four R's". And what I mean by

the "four R's", first of all, you have to recognize an attack. In many cases, you don't recognize an attack through a firewall. Second, you have to resist it once you recognize it. Then you have to respond to it, and then you have to recover from it. And those are the four R's. And——

Mr. SMITH OF TEXAS. That is exactly the point of this book that I referred to——

Dr. BEMENT. Right.

Mr. SMITH OF TEXAS [continuing]. That firewalls are not sufficient, which is what you just said.

Dr. BEMENT. And so I would say we have a long way to go, and with a determined cyber attacker, with the right kind of training, they would be able to defeat many of the systems we currently have.

Mr. SMITH OF TEXAS. Okay. Thank you, Dr. Bement, for your—thank you, Mr. Chairman. I am finished.

Chairman BOEHLERT. Mr. Smith, just let me tell you, you are right on in terms of focusing on an area we all have to focus on. And it was—our vulnerability. I recognize vulnerability that prompted this committee to try to provide some leadership, and that resulted in this *Cyber Security Research and Development Act.* And now what we are trying to do is make certain that all of the agencies for whom we have earmarked a lot of resources, insufficient I might add, but we are trying our best, are working together, are coordinating their activities, and are taking the pledge here and now that this is a matter of high priority. And you have got to give this increasing attention. And that—you were not here earlier, they have assured us of that. Department of Homeland Security has just been up since—essentially since 1 March. Dr. McQueary is the new guy on the block, and it is just a mind-boggling challenge. I think he is up to the challenge, and I think we, collectively, are up to the challenge. But we better damn well get serious about this and not just talk but act. So thank you very much for those observations.

Mr. SMITH OF TEXAS. Thank you, Mr. Chairman. Mr. Chairman, I might add, I think one of the reasons that Dr. McQueary is up to the challenge is because he has two degrees from the University of Texas.

Dr. MCQUEARY. You are very kind, sir. Thank you.

Chairman BOEHLERT. The Chair now recognizes Mr. Bell.

Mr. BELL. Thank you, Mr. Chairman. I apologize for missing your testimony. There is cyber security and there is Congressional District security, and since my district is currently under attack in the state of Texas, we decided we would go pay homage to our friends holed in Ardmore, Oklahoma. So that is why I wasn't present, and I hope you understand.

Dr. Tether, I wanted to visit with you for just a moment, because I found your remarks to be refreshing. I have only been here for four months, and I have had a bunch of people come and tell me that they have ideas but they don't have money. You are the first I have heard that has plenty of money but a shortage of ideas. So it is a nice turnaround. But I wanted to—you—I understand your reluctance to talk about cyber warfare and what is being planned in that regard, but several months ago, there was a rather exten-

sive article in the *Washington Post* about some of the plans that were being undertaken by the Department of Defense, some of the studies that were being conducted. And I sort of subscribe to the theory if it has been in the Washington Post, it is going to be hard to keep it secret after that. And they talked about looking at ways to, perhaps, wipe out the entire electrical grid in the wake of war or while involved in war, looking at maybe shutting down hospitals that use cyber technology. My question is, knowing that those efforts are going forward, what is the collaboration between those who are looking at ways to attack and using it in an offensive position and those looking to defend, because it would seem to me that there should be a great deal of collaboration in those areas?

Dr. TETHER. Well, it—even though it appeared in the *Washington Post,* I still have a hard time confirming or denying the *Washington Post.* But let me tell you, one of the—there is a great collaboration that goes on between those who look at offensive things versus those who look at defensive things, because they are really two sides of the same coin. So the people who are doing the offensive parts, when they develop techniques, we then obviously build a defense against that technique. So the people—and vice versa. When people build a defensive technique, then the offensive people need to know about it in order to try to penetrate that technique. So there is a great amount of collaboration that goes on between those two communities. Let me say, at least within DARPA, some of the operational people would not have a collaboration because it is very, very sensitive, but in our research, there is a great collaboration between the two communities: those who are coming up with techniques to penetrate and those who are coming up with techniques to prevent people from penetrating. I really can't give you any—I would be happy to give you all of the details, quite frankly, but I just can't here.

Mr. BELL. No, I understand.

Dr. TETHER. Yeah.

Mr. BELL. And I don't expect you to, and that wasn't the point of the question. I am more interested in what kind of collaboration is taking place.

Dr. TETHER. There is a lot of collaboration in—between those two communities for those—for the reasons I gave.

Mr. BELL. What is the general feeling as to where the United States stands right now in terms of cyber warfare? Are we behind in that area or are we ahead?

Dr. TETHER. I almost would have to go country by country, and I would rather not, for—again, for classification reasons. I——

Mr. BELL. But we are certainly not alone?

Dr. TETHER. Oh, no. No, we are most certainly not alone. We are most certainly not alone. And I think you can obviously—the obvious large players like the—like Russia, China, you know, these are people who are taking this very seriously, very smart people. We are not alone.

Mr. BELL. Thank you.

Chairman BOEHLERT. Excuse me, if I may interrupt here. Some would argue they are taking it more seriously than we have been in the past, but now we have a new focus.

Mr. BELL. Well, taking this whole question of collaboration a step further, because, and I am—and I don't want to put words in your mouth, but you were saying—I don't know if you said you heard about some things today or recently that you didn't know that were going on. And I would expect that. But this is an area where I would think that it is really incumbent upon those who are involved to be talking to each other. And are there steps that need to be taken to make that easier?

Dr. TETHER. Well, you know, when I said that, I was referring to the activity between DARPA and NSF. And what you learn, DARPA is really a Program Manager place, and there are 160 Program Managers. I don't know how many Dr. Colwell has, but she has a few.

And you would be amazed what goes on that the Directors don't know of, each agency doesn't know what is going on. So what I had—when this hearing came up, I put out a call to all my offices saying, "Why don't you guys tell me what you are doing with NSF?" You know. "Go and find out what the program"—and I got a lot of activity. I mean, I have got an enormous amount of activity that I did not know about. And—but it is our Program Managers farming the ideas coming out of NSF so that they could bring them back and say, "Hey, look. Here is a great idea." And this is—I am talking about cyber security type of activity now, not just in general. In general, there is a real large amount of activity, but—so they can come back with an idea, which what DARPA does is takes that idea. And we basically take it to the next step of applying it, you know, taking that idea into a technology that can be used.

But there is a great deal of activity that has—that was going on that I—quite honestly, I was not really aware of. I kind of figured it was going on, but I didn't know the specifics. And I was impressed.

Chairman BOEHLERT. The gentleman's time is expired. I am sort of surprised by that answer, a veteran like you. With Dr. McQueary, he is just in, the new guy on the block, and he knows what every one of those 180,000 people are doing within in the new Department of Homeland Security.

Mr. BELL. But Dr. McQueary went to UT.

Chairman BOEHLERT. Oh, boy. With that, Mr. Udall.

Mr. UDALL. Thank you, Mr. Chairman. I, too, want to thank the Chairman for calling this important oversight hearing today and thank him for his leadership on this whole area of cyber security. It is also—it is inspiring to see the all-stars out here on this panel, and thank you for your service to the country and for your great help and assistance you provide to the Committee.

I want to ask two general questions, and Dr. McQueary, I will give you a heads-up on the second question, which I am going to ask you first. And your Directorate has requested about $800 million in this fiscal year of 2004. And I am just curious how that money would be allocated, particularly to cyber security. If you would, set that question aside and hopefully we will get to it.

The second one—question was to yourself and Dr. Bement. And it is always great to see the NIST Director here.

Dr. BEMENT. Thank you.

Mr. UDALL. I know you have under—you have signed an MOU between DHS and NIST.

Dr. BEMENT. Pending.

Mr. UDALL. Yeah, pending. Thanks for that correction. Can you provide me, the two of you, with your understanding of the activities that would be carried out under the MOU and the respective roles of NIST and DHS? And I think most importantly for most—for all of us is will NIST have the resources to carry out the activities envisioned in the MOU?

Dr. BEMENT. The answer to the second question is yes; we will have the resources. The answer to the first question is that the MOU is very comprehensive. It includes technical support, research and development support, and standards support across the whole mission spectrum of the Science and Technology Directorate. Cyber security is clearly one of the keystone elements of that MOU, and it is one that we have already anticipated by putting one of our research staff with DHS in cyber security to begin coordinating that activity.

Mr. UDALL. Dr. McQueary, would you like to——

Dr. MCQUEARY. I would be happy to. The—in the—as you correctly point out, the fiscal year 2004 budget request is $803 million for the Science and Technology Directorate. Within that budget, we have $7 million that are specifically allocated toward cyber security-related activities. And I would like for you to keep in mind that the basis for that is that our role is one of supporting the Information Analysis and Infrastructure Protection Directorate within Homeland Security and providing Science and Technology support to them in that. We are just barely operational. And of course the Critical Infrastructure Protection Board was in existence at a time when we actually constructed that budget. And therefore, if we were to find that the money we have, we conclude, is not adequate, I have no problem whatsoever in revisiting what the budget allocation is and looking for support from people like yourself for making such an evaluation.

Mr. UDALL. Mr. Chairman, if I might, I would like to yield to my colleague, Ms. Jackson Lee, for 30 seconds. She has to leave, but she wanted to make a brief statement.

Ms. JACKSON LEE. First of all, let me thank the Chairman for this very important hearing. I was in a markup in Judiciary, and now I have been called off to another meeting. Gentlemen, I would ask the Chairman to have permission to unanimously put into the record my statement, and I will——

Chairman BOEHLERT. Without objection.

Ms. JACKSON LEE [continuing]. Proceed with the individuals on this important issue as a Member of the Homeland Security Committee. I thank you. This is a major question for our community cyber security.

Thank you, Mr. Chairman. Thank you, Mr. Udall.

Chairman BOEHLERT. Thank you very much. Mr. Udall, you have two minutes remaining.

Mr. UDALL. Thank you, Mr. Chairman. It might be, I think, of some interest to the Committee that when the MOU is signed, perhaps there is a way to get a further update as to how that might unfold and I don't know whether we would need to do that formally

or informally, but I would make that request to the two of you today and——

Dr. MCQUEARY. I would be happy to do that.

Mr. UDALL [continuing]. The Chairman as well. Do you have—when we talk about the funding, Dr. McQueary, you mentioned some of the criteria you used. Did you cover all of the criteria that had been involved in determining how this cyber security money will be directed and where you will focus those initial efforts?

Dr. MCQUEARY. Well, initially, when we—when our budget was constructed, our intent was to focus on the forensics aspect of cyber security and also attribution, those being two areas that appeared as though we could make a contribution in that area. I think that we will be continually examining what our role is, because, as you know, the IAIP organization did not have—in fact, it does not today, have an Under Secretary that leads that effort yet, although a nomination has gone forth for that, and we are hopeful that that will be approved expeditiously. And so we will be working very, very closely with the IAIP people to make sure that we do have the proper amount of budget and the right scientific areas being focused in support of their conclusions on what we need to be doing.

Mr. UDALL. The—your presence today and the Chairman's commitment to this whole area underlines the crucial nature of it. I do think—if I could just make a general comment, we all have work to do to educate the American public as to the threat we face. Like so many other areas in this modern society in which we live, we take for granted a lot of the conveniences, a lot of the systems that make our lives easier than they might have been 100 years ago. And I think anything you can do to help us, we can help—do to help you in that mission, I think, would be time well spent. I think—I am reminded of the movie "Catch Me If You Can". I don't know if you have all seen that, maybe that has been mentioned today, but in a way, we want to recruit some of those people that fit the model of that young man in that movie who would be inclined to, because they want the adventure, I think, of breaking these systems and getting into places where other people haven't been and see if we can bring them to the side of us and create a socially productive avenue, so we say, for those young hackers out there. We ought to be looking at that. That is an opportunity, I think, as well as a threat.

Thank you, Mr. Chairman, and again, I want to thank the panel.

Chairman BOEHLERT. Thank you very much. Dr. McQueary, where is the research going to be focused in DHS? Who is going to be doing it?

Dr. MCQUEARY. For cyber security specifically?

Chairman BOEHLERT. Right.

Dr. MCQUEARY. It will be conducted by the Science and Technology Directorate, yes, sir.

Chairman BOEHLERT. All right.

Dr. MCQUEARY. And that is the role that we——

Chairman BOEHLERT. Have you earmarked where within your operation?

Dr. MCQUEARY. Where specifically within——

Chairman BOEHLERT. Right.

Dr. MCQUEARY [continuing]. My organization?

Chairman BOEHLERT. Have you identified people and——

Dr. MCQUEARY. Yes, we have. In fact, we have

people——

Chairman BOEHLERT. People and dollars?

Dr. MCQUEARY. People and dollars, yes. Yes.

Chairman BOEHLERT. That is good. Could you provide that for the record——[1]

Dr. MCQUEARY. That was a—yes, sir.

Chairman BOEHLERT [continuing]. At your convenience? All right. The Chair recognizes Ms. Lofgren.

Ms. LOFGREN. Thank you, Mr. Chairman. I would also like to offer my apologies, as several other Members have. I am also a Member of the Judiciary Committee, and I also was tied down in a markup all morning, so I missed your testimony, although I have read it. And I appreciate the Chairman's calling this hearing. I would note, I am a Member of the Homeland Security Committee and ranking on the Cyber Security Subcommittee, and we have beaten Homeland Security to the punch on this hearing. And so I will see you, I guess, next week as well on some of these issues.

Chairman BOEHLERT. As we all will—several of us will.

Ms. LOFGREN. Right. I do want to just briefly return to one issue and explore another, and then I know the lunch hour is here. As I am sure you recall, Dr. Bement, there was concern last Congress about the proposal to shift some NIST activities to DHS. And the concern really—and this committee, on a bipartisan basis, objected to that, and in the end, Congress did not approve that shift. I am sure you are aware that there is anxiety in the country about the detailing of staff by NIST to DHS and whether that has the effect of accomplishing administratively what the Congress did not approve last Congress. I am not suggesting that is the case. I would like to explore that with you.

Dr. BEMENT. I would say that—I am sorry.

Ms. LOFGREN. The question really has to do is what are they doing specifically? I know you say there is a detailed MOU, but specifically, I would like to know the nature of that—their activities relative to encryption. Can you address that?

Dr. BEMENT. To my knowledge, there is no work going on in encryption at the present time. We have two people detailed to the Department of Homeland Security. One is providing a coordination role between DHS and NIST in terms of acquainting DHS with our cyber security efforts. Now the other person is working with Science and Technology Directorate in, working with Dr. Albright in back of me, as a matter of fact, in developing a national strategy for DHS and standards development. And of course, that is our area of expertise——

Ms. LOFGREN. Right.

Dr. BEMENT [continuing]. So we are willing to assist—I mean, we are happy and anxious to assist DHS in that area. And as far as the issue that you brought up, we are very grateful to the Committee for recognizing the importance of the independent role that NIST plays with the private sector in developing guidelines and in

[1] This information is provided in Dr. McQueary's answers to post-hearing questions, located in Appendix 1.

developing specifications and standards in the area of cyber security. And anything that we do with other agencies, we preserve that independence and that integrity, so I wanted to assure you of that.

Ms. LOFGREN. I wonder if I could—I know you are going to provide the draft MOU to the full Committee. I—as a Member of the Homeland Security Committee, it would be especially helpful to me if I could get a copy of that prior to our hearings next week, if I could ask that favor.

Dr. BEMENT. We—I think the signing will be taking place on Monday.

Dr. MCQUEARY. I believe the 19th is the day that we did have that set up.

Dr. BEMENT. The 19th of May, and we will provide a copy to you as soon after it is signed as we can.

Ms. LOFGREN. Let me ask another question relative—it is actually to funding, and I know that probably people who head bureaus and directorates and departments or—and are probably discouraged from complaining about their funding to Congressional Committees. But I am concerned about whether there is sufficient funding to do some of the things that I think are essential to the national security. One of the issues that has been discussed informally at the Homeland Security Committee is the lack of—or at least apparent lack of rigorous analysis of biometric standards. And what are we looking for in terms of ease of use, reliability, scalability, et cetera, et cetera?

And I am wondering—it seems to me that the absolute best home for that kind of analysis is NIST, because it is a standards issue. It is not a policy issue. It is not a political—it is a standards issue. And I know last year, I asked NIST to provide me with information about biometrics. You very kindly responded, but it was not original research. It was sort of a compilation of what is out there, and I will say it was rather thin. Is NIST sufficiently funded to accomplish that kind of biometrics analysis and standard setting if the Department of Homeland Security were to ask you to do so?

Dr. BEMENT. We certainly have the competence to do that and until now, most of the resource that has been going into that area has partly come out of our base program. Part of it has been provided by DARPA.

Ms. LOFGREN. So we would need to provide——

Dr. BEMENT. Part of it has come from——

Ms. LOFGREN [continuing]. Additional funding?

Dr. BEMENT [continuing]. Department of State, Department of Justice. And in our '04 budget request, we have requested that $1 million of additional funding in order to beef up our effort in this area. So it is in our '04 budget request.

Ms. LOFGREN. Is $1 million enough to actually accomplish that?

Dr. BEMENT. No, but it is all we could work in.

Ms. LOFGREN. All right. I—how much would you need if the DHS were to ask you to accomplish that function quickly and reliably? What would the tag be, do you think?

Dr. BEMENT. We feel it would be $3 million.

Ms. LOFGREN. All right. Thank you very much, and I see my time is expired.

Mr. EHLERS. [Presiding.] We will proceed with a brief second round of questions. I will kick off a few. First of all, Dr. McQueary, you have got a blank piece of paper in front of you for what you are going to do. And my question is—I have several questions related to that. Who is going to perform the cyber security research for you? Are you planning to hire staff members? Do you plan to have—use grants to universities or contracts or grants with the private sector companies or other federal agencies? What do you see as developing here?

Dr. MCQUEARY. I see it as being a combination of all of the things that you just talked about. The construct of the Science and Technology Directorate is such that we will largely be in the role of managing the programs that will be executed, both the federal and national labs, private sector, as well as university academia, if you will. And so we will have the leadership role. In fact, we have about four people already in roles, which I touched upon earlier, that are detailed to us with—and have experience in the cyber security area. So we will provide the leadership, oversight, program management responsibility, if you will, and contract that work out into the various sectors you talked about, always looking for where the top quality work is being done to capitalize upon that.

Mr. EHLERS. Okay. And do you think cyber security will get the attention it needs? Are you going to have sufficient funds to do all of the things you are supposed to do in your area? And given all of the different competing needs that you will have to deal with, is cyber security going to get the attention it needs?

Dr. MCQUEARY. Well, it certainly has the attention—has my attention, and I have the responsibility for constructing the—a budget and making the proposal to Secretary Ridge as to what we should do there, so if we do not get the sufficient attention, then I am the first person that one should come to to say why not, because I have that responsibility in Science and Technology.

Mr. EHLERS. Okay. Our concern would be that it would just be considered just one more aspect of infrastructure protection in the overall scheme of things in DHS.

Dr. MCQUEARY. I am sorry, I missed the question.

Mr. EHLERS. I am just worried that this may just be considered one other aspect of infrastructure protection within DHS and actually be competing with all of the different——

Dr. MCQUEARY. I believe that we will see some organizational restructuring very shortly within DHS that will, I hope, illustrate to you that we do take this issue very, very seriously.

Mr. EHLERS. Okay. And something else. I don't know if—I would be interested in what all of you have to say, but perhaps you don't have the figures with you and want to respond in writing, which would be fine. I am curious what is being spent on cyber security R&D by the Federal Government in total and how much by the private sector. Do you have an idea of this or would it be better to just ask you to send in the information?

Dr. MCQUEARY. I do not have the information, sir.

Mr. EHLERS. All right. Dr. Colwell, if you have——

Dr. COLWELL. Right now, we have about $53 million, but that can go up to as high as $75 or $76 million, depending on the outcome of some competitions that are in play at the moment for the

potential for a center award and a potential for scholarships and so forth. But we see, pretty much, coming close to the authorized number.

Mr. EHLERS. Okay. Dr. Bement.

Dr. BEMENT. Well, I can only speak for NIST. As I indicated in my testimony, we currently have $24 million of appropriated and base funding going into cyber security. We also have additional funding coming from other agencies: the National Security Agency and DARPA.

Mr. EHLERS. Um-hum.

Dr. BEMENT. I think our DARPA account is around $5.2 million, so adding that all together, it would still be less than $50 million in NIST. As far as the Federal Government at large or the Nation at large, I don't really have those numbers.

Mr. EHLERS. Okay. And Dr. Tether.

Dr. TETHER. I also don't really know what the Federal Government is spending, but at DARPA, we are spending—in '04, we will be spending around $50 million in cyber—in information awareness. But there is more that we are spending that I actually will give you for the record, because we are doing cyber security with other programs. For example, we are building networks. And then there are activities within the building of a network, which is also to make the network secure, so it is embedded. I will try to pull that out for you. But it might be another $50 million, so it might be a total of 100. And then we have the classified work, which I will tell you separately.

Mr. EHLERS. All right. And are you also including in your work efforts to prevent damage from electromagnetic pulses, or is that——

Dr. TETHER. No.

Mr. EHLERS [continuing]. Considered totally separately?

Dr. TETHER. That is considered totally separate, yeah.

Mr. EHLERS. Okay. But by and large, Defense Department facilities are hardened against that?

Dr. TETHER. They are hardened against that.

Mr. EHLERS. Yeah.

Dr. TETHER. There are requirements for them to be hardened against that.

Mr. EHLERS. Do you have any idea to what extent the private sector or—is hardened against EMP?

Dr. TETHER. I would be surprised—well, first of all, they—all—everybody has, usually, a surge suppresser——

Mr. EHLERS. Right.

Dr. TETHER [continuing]. You know, which gives them some hardening, but that would be, probably, the limit. I don't know of anything else.

Mr. EHLERS. I would think banks, at least, would want that.

Dr. TETHER. You would think so.

Dr. BEMENT. I think they would still be vulnerable against pulse power attack. I mean, if——

Mr. EHLERS. Yes.

Dr. BEMENT. If an attacker had the capability——

Mr. EHLERS. Yeah, a surge protector won't do too much.

Dr. BEMENT. No, it won't do you very much.

Dr. TETHER. No. No.

Mr. EHLERS. No. Okay. My time is expired. Anyone else wish to—Mr. Miller, you are recognized for five minutes.

Mr. MILLER. One last set of questions. Is it Dr. Bement?

Dr. BEMENT. Bement.

Mr. MILLER. Bement. Okay. What you said in response to Ms. Woolsey's questions were very reassuring to me that what we need is knowledge, education, and discipline. The security is now available, I think you said, through protocols, metrics, and standards, that we have very smart people working on this, and that there is nothing stopping us from doing it, from being secure. And I—and that is greatly reassuring to me. And Dr. McQueary pointed out correctly, of course, that anyone in the private sector is going to know the risk to their business of not being secure, of suffering an attack.

Dr. BEMENT. Yes.

Mr. MILLER. What I am concerned about, somewhat, is that there is—there will always be people who do things on the cheap, who don't—do not show knowledge, education, and discipline. And what are we doing to make sure that when people in the private sector do their kind of assessment of what it costs to adopt the security measures they should adopt versus the risk that they face if they don't, that they take into account not just the risk to them, to their business, but the risk to others that they deal with—the ripple effect that we talked about earlier? The loss of the power grid, obviously, would have a massive effect. I think you mentioned, or Dr. Tether mentioned, the possibility that—or it may have been you, that hospitals could be shut down. Obviously there is risk to others and not just the direct loss and disruption to the victim of an attack, but of all those deal with. Are we doing anything for requiring anyone in the private sector to adopt security measures? Have we thought through whether the standards that we are developing, the protocols, form the basis of a standard of care for civil liability? What are we doing to make sure that people in the private sector think through the risk, not just to them, but on down the line?

Dr. BEMENT. I can tell you this much that many of the professional societies who have begun to pay attention to these risks, which are really the product of the probability of the event plus the consequence—times the consequence of the event, have begin—have begun to develop risk models with their constituents so that industry is better informed about what the consequence of a cyber attack might be, or any other vulnerability might be. I have to say that, as a Nation, our greatest vulnerability is indifference.

I think it was Dr. McQueary that pointed out that 85 percent of our industry and productive capacity is owned by the private sector. And yet, all of the surveys that I have looked at recently in surveying the private sector on what they are doing in terms of either vulnerability assessment or dealing with risks, terrorist risks, indicate that they don't really see themselves as a target, which is sort of indifference. And in some respects, I think it may, in order to bring it home to them, require some of the kind of exercises or demonstrations that took place this last weekend to actually demonstrate what the consequence might be of these attacks so that CEOs and other leaders in industry will have it brought home to

them, what it could, in fact, mean to their manufacturing operation, their logistics train, their supply train, all of their other elements that they have to deal with on a day-to-day basis. And I feel that that is our biggest vulnerability right now is they just haven't quite stepped up to the plate.

Mr. MILLER. Do you know if the insurance industry has looked at cyber security as a liability issue?

Dr. BEMENT. I am sure they have. Yes, indeed, they have. The insurance rates have gone up dramatically since 9/11, so there clearly is a payback in being able to demonstrate that you are much better protected against these types of attacks.

Mr. MILLER. Well, is it the only——

Dr. BEMENT. It is not only insurance; it is the reinsurance rate as well.

Mr. MILLER. Right. Well, yes, the—I imagine the potential liability is massive. It would require going to the reinsurance markets. Is it being excluded for policies? Is it being included in policies? Are insurance companies—liability insurers having a word of prayer with their insureds about what they are doing?

Dr. BEMENT. Well, I must confess this is getting a little bit beyond my ken or my area of expertise, so I really can't——

Mr. MILLER. But it is a strong economic incentive——

Dr. BEMENT. Yes.

Mr. MILLER [continuing]. To do the right thing?

Dr. BEMENT. I would think so, yes.

Mr. EHLERS. The gentleman's time has expired. Mr. Udall, do you have any questions?

Mr. UDALL. Mr. Chairman, I had a last question, hopefully, thankfully, although this is a topic, which we will revisit. Dr. Tether, I was just curious in looking over your material you compiled for the Committee and the good work you did here in describing network centric warfare and suggesting we maybe aren't quite there yet, but we are certainly network-dependent. Have you gotten any indication out of the recent conflict in Iraq that the Iraqis had any kind of cyber security tools that we hadn't anticipated or that there were, perhaps, other countries or other individuals developing those for the Iraqis or for future opponents?

Dr. TETHER. The—I don't know of anything. That doesn't mean that there wasn't something. GPS jamming was the only thing that I know about.

Mr. UDALL. I am sure you are going to take a look at that, and I would bet that some of this may well be classified, but we always have, when we have these encounters, have a chance to then review our mistakes as well as our successes.

Dr. TETHER. Yes, and that is all being done.

Mr. UDALL. I hope we will—I know we will do that.

Dr. TETHER. Yeah.

Mr. UDALL. And it strikes me that the military, once again, is on the cutting edge of some of these technologies and we look at the history of the Armed Services, and much of what was generated in the Second World War is now used in civilian activities. One of my real interests, and I share with our Chairman of the Committee is energy, and the military is leading the way in certain new technologies: fuel cell technology, photovoltaic uses and others because

of the transformation we are trying to put underway in our military. So I think you all have a very—I just wanted to conclude by saying you, of course, have a very important role to play in this. And we look forward to this all-star team working together seamlessly to help lead us to a more cyber secure future.

Dr. TETHER. Well, it is clear with the—private industry really has not been able to do the tradeoff of what does it cost them to not have it. It is very clear for the military, when we are becoming really dependent upon that network being there, what happens if that network is not there. So the tradeoff is, you know, very clear. There is no—we have to make those networks secure, otherwise everything we are building for the future will not work, and that would be a disaster, I mean, to the national security.

Mr. UDALL. Mr. Chairman, I have many more questions, but I think the lunch hour does beckon. I would yield back my remaining time. I thank, again, the panel.

Mr. EHLERS. The gentleman yields back his time, and I am sure the panel appreciates it, and the audience. I just wanted to pick up on the last two comments. First of all, perhaps it is only through higher insurance rates that people will become aware of the need for protecting their equipment. And that goes to your last point, too, Dr. Tether, that most people and most businesses don't realize the risk and therefore they don't take the trouble to protect against it.

But it is a bit ironic, Dr. Bement, that you mentioned the electric power industry, because I, for roughly five years now, I have been telling my constituents in town meetings, and I had to, because I voted against the Defense appropriations for three years, because I thought they were funding the wrong things. And of course, all of the veterans show up at my town meetings and castigate me for not supporting Defense. But I simply pointed out that what we are doing is pouring a lot more money into the same old systems, and the real danger is not a major nation attacking us, it is terrorists attacking us. Unfortunately, I was correct, and so we are all now alerted to that.

But the other example I give my constituents now, because they are all terrified about aviation, and I simply say, "The problem is we always fight the last war." And we are now making our airlines super safe, and we have to worry about port security and then the power industry. I have said, for a number of times, "Give me 20 knowledgeable people about computers and explosives—and a little explosives, and I could bring down the power grid in one night." And of course, we could get it up again in probably four or five days, but can you imagine what the cost is of four or five days' productivity to our nation, particularly if this can happen repetitively?

So it is—the best way, of course, is to stop terrorism at its source. It is impossible to really totally defend against it here, but we can certainly do much more in defending against terrorism within our borders than we are currently doing. And we tend not to wake up. As you say, they are—it is indifference. The indifference goes away with each specific attack, but then we tend to prevent to guard against that attack again. And there is a plethora of possibilities for terrorist activity.

I want to thank the panel very much. It is been an outstanding panel. You have each represented very well the expertise available within your agencies or departments. And I certainly appreciate your attendance here. The information you have given will be, indeed, very valuable to us as we continue our deliberations. Thank you very much for being here. With that, the hearing is adjourned.

[Whereupon, at 12:20 p.m., the Committee was adjourned.]

Appendix 1:

Answers to Post-Hearing Questions

ANSWERS TO POST-HEARING QUESTIONS

Responses by Dr. Charles E. McQueary, Under Secretary for Science and Technology, Department of Homeland Security

Questions submitted by Chairman Sherwood Boehlert

Q1. You stated at the hearing that you would provide for the record information on the people and dollars that the Department of Homeland Security (DHS) Science and Technology directorate plans to devote to cyber security research and development activities in fiscal years 2003 and 2004. Please do so. In addition, to what extent do you expect your fiscal year 2003 funding for cyber security research and development to be spent for support of DHS personnel? For support of programs at other federal agencies and national laboratories? For grants and contracts to universities and companies? (When providing the information requested in this question, please distinguish between research and development programs and education and workforce training programs.)

A1. The Science and Technology Directorate's current plans for people and funding devoted to cyber security research and development in FY 2003 and FY 2004 are as follows:

FY 2003: 2 staff members within the DHS Science and Technology Directorate and funding of approximately $5 million.

FY 2004: 2 staff members within the DHS Science and Technology Directorate and funding of approximately $7 million.

For FY 2003: The DHS Science and Technology Directorate plans to fund about $1 million per year at universities through the National Science Foundation (NSF). A contract with a private firm for about $1 million has been awarded to continue work addressing insider threats. In addition, proposals with a total value of about $3 million over three years are pending from the National institute of Standards and Technology (NIST), a nonprofit research institute and another federal agency for additional cyber security research and development; until these are actual awards, it is not appropriate to estimate the actual amounts to these entities. We would be pleased to provide this information after actual awards are made if this is desired. Each of these existing and pending efforts are research and development activities; none are education/workforce training efforts.

Q2. At the hearing, you said that if the funding you have proposed for cyber security research and development for fiscal year 2004 "is not adequate," you would "have no problem whatsoever in revisiting what the budget allocation is." When will you begin reviewing the factors that determine what level of spending is needed? How will you decide if the level is "not adequate"? When will you let us know whether you believe the allocation should be changed?

A2. The Science and Technology Directorate has reviewed its proposed FY 2004 funding and currently believes the proposed amount for cyber security research and development (R&D) is adequate. However, we continue to assess our research and development plans in the context of the national effort in cyber security. If we determine that the proposed amount of our funding is not adequate, we would first evaluate the impact of reprioritization and re-allocation of existing budgets. If believed necessary, we would bring a request for additional funding forward for consideration through the appropriate mechanisms. Additionally, in order to accurately determine what level of funding is needed for cyber security research and development, we will continue to work with other agencies with R&D responsibilities, such as NIST and NSF, to identify requirements and gaps in funding. This coordinated approach will assist in making the right investments in this area while preventing unnecessary and wasteful duplication.

Q3. In other forums, you have stated that most of the focus of the DHS Science and Technology Directorate at first will be on shorter-term technology development. How will you balance technology development and basic research in cyber security? Do you expect that balance to change over time?

A3. The Science and Technology Directorate recognizes there are some technology needs that require immediate attention; some of these needs were identified in the *National Strategy to Secure Cyberspace,* while others have been identified by the critical infrastructure protection community. The Science and Technology Directorate believes that those cyber security issues which require basic research to solve are more within the scope of the National Science Foundation than our Directorate.

Our long-term portfolio plan may address basic research to some degree through programs directed out of the cyber security research and development center.

Q4. At the hearing, you testified that the Committee will "see some organizational restructuring very shortly within DHS that will. . .illustrate to [the Committee] that we [at DHS] do take [cyber security] very, very seriously." Since the hearing, there have been press reports that DHS will establish an office to execute the President's National Strategy to Secure Cyberspace. *Please tell us for the record what restructuring is intended and when it will occur. What will the responsibilities and size of the new office be?*

A4. The reference to the DHS restructuring around cyber security referred to the subsequent announcement of the creation of the National Cyber Security Division (NCSD) within the Information Analysis and Infrastructure Protection (IAIP) Directorate. The NCSD incorporates some of the operational capabilities of the Federal Computer Incident Response Center (FedCIRC), the National Communications System, and the National Infrastructure Protection Center (NIPC), along with new streamlined and consolidated outreach and awareness capabilities recently formed in the Directorate. The NCSD is adding new capabilities for vulnerability assessments, risk reduction methodologies, threat analysis, and enhancing training and workforce development activities in the public and private sectors. At present, it is expected that the NCSD will have about 40 FTEs total and a budget of about $86 million, including the funding for civilian salaries and operating expenses.

The Science and Technology Directorate has also organized its cyber security research and development with the intent of making it a visible and important component of its total research and development effort.

Q5. DHS, through its planned work with critical infrastructure suppliers, has an opportunity to connect researchers with companies that have real, unsolved cyber security problems. How will DHS make these connections? How will the issue of sensitive critical infrastructure information be handled in these situations?

A5. The Science and Technology Directorate is establishing a cyber security research and development center that will enable partnerships with academia, private industry and national laboratories. A principal purpose of this center is to engage the researchers with the product developers and accomplish technology transfer to the companies with specific needs. This center will engage the critical infrastructure companies through mechanisms such as industry associations and consortia, bridging the gap and connecting companies with researchers and developers as required. In addition, the IAIP Directorate will be the chief customer to the center and will deliver needs and requirements based on their interaction with the critical infrastructure sectors.

The protection of sensitive critical infrastructure information is recognized as an overarching issue of high importance, not only within the context of cyber security R&D but across the Department. In accordance with the authorities provided in the *Homeland Security Act of 2002,* the IAIP Directorate developed proposed procedures for handling Critical Infrastructure Information. The procedures detail the receipt, care, storage and marking of the submitted data. These proposed procedures were released for public comment and are now undergoing final refinement. Once these procedures are finalized, the Science and Technology Directorate will adhere to those policies to ensure that critical infrastructure information voluntarily submitted by the private sector is handled appropriately and protected accordingly.

Q6. How will DHS work cooperatively with other agencies on cyber security research and development? Specifically,

Q6a. You testified that a Memorandum of Understanding between National Institute of Standards and Technology (NIST) and DHS will be signed shortly. Will DHS provide funding to NIST for specific projects? Are there particular areas in cyber security that you are planning to work together on?

Q6b. Will DHS provide funding to support existing or new cyber security grant programs at the National Science Foundation and the Defense Advanced Research Projects Agency?

Q6c. Is DHS drawing on the expertise in the Infosec Research Council (IRC) and the High Confidence Software and Systems group within the Networking and Information Technology Research and Development Interagency Working Group? How will DHS be interacting with these interagency groups?

A6a,b,c. The Science and Technology Directorate's cyber security portfolio manager has been, and continues to be, in dialogue with the National Science Foundation

and NIST, both individually and cooperatively. NSF, NIST and DHS (S&T) recently agreed to formally organize their efforts and work collaboratively to identify the R&D agenda appropriate to each agency. As stated previously, proposals are pending from NIST and others; until these are actual awards, it is not appropriate to estimate the amount that will be awarded to NIST. The Science and Technology Directorate will provide co-funding to NSF and NIST on those programs determined to meet requirements of our customers. At present, there are no plans to fund new or existing cyber security grant programs at the Defense Advanced Research Projects Agency (DARPA).

The Science and Technology Directorate is also participating with the Infosec Research Council (IRC) where interaction across the government cyber security R&D stakeholders is accomplished. In addition, we participate in the newly established National Science and Technology Council (NSTC) Interagency Working Group on Critical Infrastructure Information Protection, created as an interagency R&D coordination working group. The Department of Homeland Security is not formally part of the Networking and Information Technology Research and Development Interagency Working Group but does interact with the relevant programs through the Infosec Research Council and the Interagency Working Group on Critical Infrastructure Information Protection.

Q7. The Cyber Security Research and Development Act makes the National Science Foundation (NSF) the lead agency for cyber security research and development, as Dr. Colwell testified at the hearing. In what ways are you interacting with NSF as it acts as the lead agency in this area? Does NSF review your budget proposal for programs in this area? Does NSF lead the agencies in a group effort to determine overall cyber security research and development priorities, and if so, how?

A7. As mentioned previously, the Science and Technology Directorate coordinates regularly with NSF to understand the existing cyber security R&D programs, the agenda and requirements not currently addressed, and identify the gaps. These interactions take place via the coordination groups mentioned in the response to the previous question, as well as on an individual basis. The Science and Technology Directorate has not relied on the NSF to directly set the agenda for DHS's cyber security research and development. Rather, DHS's cyber security R&D agenda is being driven by R&D priority areas as determined by the Department's mission and scope, e.g., those areas related to the needs and requirements that support the technology necessary for the Nation's critical infrastructures to operate and provide services.

Q8. The Committee believes that it is important to train skilled professionals to execute information technology security in the private sector and at government agencies, as well as scientists and engineers to perform cyber security research and development. What do you see as particular workforce needs in cyber security? What actions is DHS taking or planning to take to provide education and training in the cyber security area?

A8. The Science and Technology Directorate recognizes the need for cyber security experts that are well trained in technology, science, policy and privacy concerns in order to perform the advanced research and development of effective tools to protect our information systems and networks. Particular workforce needs are wide and varied in this area, ranging from programmers and developers that understand and respect cyber security concerns, to network administrators with an understanding of risk and appropriate security posture. While the mission of university education and curriculum development at the university level is something that falls more within the scope of NSF than DHS, we hope to play a role in providing information about industry educational needs to NSF. In addition, the S&T Directorate has a Homeland Security Fellowships/University Program that is specifically focused on encouraging and supporting U.S. students to study and enter fields relevant to homeland security; the field of cyber security is certainly one of those fields we will support. The Science and Technology Directorate will cooperate with IAIP, NSF, and the Office of Personnel Management to encourage and facilitate the expansion and interest in the CyberCorps program, the Cyber Defender program, and others that may be identified, to address the Nation's needs for a work force trained adequately to implement effective cyber security programs in both public and private sectors. By executing its mission well, the Department's cyber security research and development center will attract some of the best and the brightest to this field.

Questions submitted by Representative Ralph M. Hall, Minority Ranking Member

Q1. The Department of Homeland Security (DHS) will establish performance criteria for acceptable cyber-protection technologies. What exactly will this entail and who will be responsible for certifying that these technologies meet DHS performance criteria? Also, will government procurement be limited to technologies that meet these DHS standards?

A1. The Science and Technology Directorate will work with the existing processes, and particularly with NIST, for the development, review, and establishment of appropriate performance criteria. The Department of Homeland Security supports certification by private sector bodies/programs that technologies meet established performance criteria; this position is consistent with existing "standards/certification" processes in other areas. At present, government procurement of cyber-protection technologies is not limited to products that meet specific criteria.

Q2. DHS intends to establish a DHS R&D Cyber Security Center in cooperation with NSF and NIST. How much funding will DHS allocate to this Center? What will be the role of NSF and NIST in the Center's establishment?

A2. DHS's Science and Technology Directorate will establish a cyber security research center as an organizational entity. Once the center is established, we anticipate that a significant portion of the cyber security R&D funding will flow through this center. NSF and NIST have provided valuable input in the establishment of the center. The DHS Science and Technology Directorate expects to allocate funding of $1 million to the Center in FY 2003 and $2 million in FY 2004 (these amounts are approximates until contracting is finalized).

Q3. In establishing the near-term research agenda for DHS, which industry sectors did you consult with in developing this agenda, and what role did industry play in formulating your near-term research agenda?

A3. The Science and Technology Directorate developed its near-term cyber security research agenda using the areas identified in the *National Strategy to Secure Cyberspace* and from our chief customer, the Information Analysis and Infrastructure Protection Directorate. The *National Strategy to Secure Cyberspace* was developed based on extensive interactions with and input from the private sector, including sector-specific industry groups, public town hall meetings, and extensive input received in response to a public draft of the document. Additional input came from interactions with other agencies (such as those through the Infosec Research Council). Subsequent private sector input to cyber security research and development needs and requirements will be sought through the cyber security research and development center.

Q4. You mentioned in your testimony that your directorate is taking steps to establish key relationships with the major cyber security R&D organizations. What are these organizations; are they both governmental and in the private sector?

A4. The Science and Technology Directorate interacts regularly with the government cyber security R&D organizations both directly and through groups such as the Infosec Research Council and the newly-established National Science and Technology Council (NSTC) Interagency Working Group on Critical Infrastructure Information Protection (IWG on CIIP), created under the NSTC as an interagency R&D coordination mechanism. Although DHS is not formally part of the Networking and Information Technology Research and Development (NITRD) Interagency Working Group Program crosscut, DHS does interact with the relevant programs in the NITRD through the IRC and the IWG on CIIP. Government agencies that we have interacted with include NSF, NIST, Defense Advance Research Projects Agency (DARPA), National Security Agency (NSA), Department of Energy (DOE), Department of Defense (DOD), Office of Science and Technology Policy (OSTP), Advanced Research and Development Activity (ARDA), as well as Canada, the United Kingdom, and Australia. We have not yet initiated formal relationships with the private sector; however, we are planning a workshop to include private companies in midsummer to start this process.

ANSWERS TO POST-HEARING QUESTIONS

Responses by Rita R. Colwell, Director, National Science Foundation

Questions submitted by Chairman Sherwood Boehlert

Q1. In your testimony to the Committee, you said that cyber security researchers will be told about National Science Foundation (NSF) funding opportunities for centers, like the competitions for Science and Technology Center grants. However, the Cyber Security Research and Development Act *authorizes a program specifically for Computer and Network Security Research Centers. Will NSF run competitions specifically targeted at "Cyber Security Centers," as required by the Act?*

A1. NSF is currently preparing a program solicitation entitled Cyber Trust; we expect that it will be released toward the end of summer, 2003. The Cyber Trust announcement will solicit proposals describing a range of types, including individual investigator, small group and center-scale projects. Thus, cyber security centers will be targeted in this competition. It is NSF's intent to continue integrating center-scale projects into its existing research and education portfolio of activities at a rate that will nurture and sustain the emerging cyber security community in academe.

Awards made in FY 2004 as a result of the Cyber Trust competition will complement awards in the agency's current cyber security portfolio. As the Committee may be aware, NSF is already funding center-scale cyber security projects. For example:

An Industry/University Cooperative Research Center (I/UCRC) on Cyber Protection is currently being supported by an NSF planning grant. Building on a strong partnership between Iowa State University, Mississippi State University and the University of Kansas, as well as key industry partners including EDS, MPI Software Technology, and Amerlnd, this Center is planning to provide one of the first facilities dedicated to creating a simulated Internet for the purpose of researching, designing, and testing cyber defense mechanisms. By recreating critical components of the infrastructure, end-users and developers will be able to test security configurations and help researchers from a broad range of disciplines examine the policy, business, systems, and economic implications of cyber security innovations.

The Georgia Institute of Technology's Center for Experimental Research on Computer Systems has two primary intellectual thrusts that examine systems survivability and security issues. The first deals with the development of a secure distributed software infrastructure. The second thrust deals with adaptive management in distributed systems with a goal of tolerating failures, attacks, or performance overloads while maximizing system performance. This center works closely with the Georgia Tech Information Security Center (GTISC), supporting many of the faculty in GTISC.

Although the merit review process is not yet complete for the FY 2003 ITR competition, it is increasingly likely that several center-scale awards will be made in the area of cyber security. If interested, we would be pleased to share these awards with the Committee after they are completed.

We plan to bring the leaders of these and future center-scale operations in the cyber security area together on a regular basis and to publicize them as a group. NSF's Cyber Trust portfolio will include both the centers of excellence, as authorized by the Act, and smaller-scale projects, including single investigator projects. At NSF we have learned that a variety of coordinated funding approaches is most effective in building a strong, coherent research and education community.

Q2. The Cyber Security Research and Development Act *authorizes NSF to run a broad, cyber security grants program for individual investigators and small groups of investigators. You testified about ongoing work in this area and about how cyber security research funding at NSF has increased from $15 million in fiscal year 2002 to $30 million in fiscal year 2003. What is the schedule for awarding the new grants to be made from the fiscal year 2003 funding and how will proposals be solicited? Will there be a competition run specifically in cyber security, or will the cyber security proposals be solicited and evaluated as part of a more general Information Technology Research or Cyber Infrastructure solicitation?*

A2. NSF's FY 2003 competitions are drawing to a close at this time. Consequently, the agency expects to make many new awards between now and the end of the fiscal year.

During FY 2003, the agency ran several competitions that specifically targeted cyber security; these included the Trusted Computing program and the Data and Applications Security program. These two competitions yielded over 100 proposals. The proposals received have now completed the merit review process and NSF expects to make between 30 and 40 new awards before the end of this fiscal year.

In addition, the agency also emphasized the growing importance of cyber security in a number of other FY 2003 solicitations and program announcements, including the Information Technology Research (ITR) solicitation, the Embedded and Hybrid Systems (EHS) program announcement, the Networking Research Testbeds (NRT) program announcement and the NSF Middleware Initiative. Response to these solicitations has been strong in the area of cyber security. If interested, we would be pleased to share these awards with the Committee after they are completed.

Q3. The Cyber Security Research and Development Act *emphasizes the importance of workforce development, and the Committee believes that it is important to train skilled professionals to execute information technology security in the private sector and at government agencies, as well as scientists and engineers to perform cyber security research and development. What do you see as particular workforce needs in cyber security?*

A3. In order to determine the workforce needs to meet the cyber security demands of government and industry, NSF has held and will continue to hold discussions with the higher education establishment, and government and industry IT leaders.

In June 2002 the American Association of Community Colleges (AACC) hosted an NSF supported workshop on cyber security education. This workshop examined the role of the community colleges in the preparation of cyber security professionals. As a result of this workshop, NSF has included cyber security education as a main component of the Advanced Technology Education (ATE) program. Through this program, NSF will be funding two projects related to cyber security, one Center of Excellence in Cyber Security Education as well as providing planning grants for two more Centers.

NSF and NIST are planning an invitational workshop of academic, industry, and government leaders to help assess the needs and identify the strategies necessary to prepare a world-class cyber security workforce. In order to facilitate educational innovation in cyber security, design concepts for new cyber security-related curricula will be devised. Implementation strategies will be discussed to determine the best way to deliver cyber security education to a broad audience.

The workshop will focus its efforts on strategies for workforce investments in cyber security at the undergraduate and doctoral levels. It will also examine implementation strategies to support faculty traineeships in cyber security enabling recent Ph.D. graduates and current IT faculty to pursue academic careers in cyber security.

Q4. The Cyber Security Research and Development Act *authorizes NSF to provide funding for several activities designed to build this nation's capacity for cyber security education, both of operational cyber security professionals and of future cyber security researchers. What steps has NSF taken to execute these programs, specifically:*

Q4a. Have programs been started to provide grants to institutions of higher education to establish or improve undergraduate and Master's degree programs in computer and network security and to increase the number of students in these programs?

A4a. NSF has several programs that seek to establish or improve undergraduate degree programs in computer and network security, and to increase the number of students in these programs.

Based on the recommendations of the AACC workshop, NSF has included security education as a major component of the Advanced Technology Education (ATE) program. Through this program, NSF is funding two cyber security projects and a Center of Excellence in Cyber Security Education as well as providing planning grants for two Centers.

The Center of Excellence in Cyber Security NSF expects to fund in the next two months is a consortium of eight institutions of higher learning (two universities, five community colleges and one technical college) based in the Midwest. The Center will be funded to develop and implement degree programs in IT Security and Data Assurance technologies at the certificate, Associate's and Bachelor's level. The Center will also undertake a comprehensive outreach and support program to increase the number of students from under-represented groups in IT professions. In addition, Train-the-Trainer summer workshops will be developed for faculty from both two-

and four-year institutions throughout the region. This project has been approved for funding but has not yet been announced to the winners.

The NSF-CompTIA Cyber Security Fast Track Training and Certification Program was a initiated this year as a supplemental award to an existing grant. This supplemental award extends the mission of the National Workforce Center for Emerging Technologies (NWCET) to include the Computing Technology Industry Association's (CompTIA) Security+ certification program for cyber security instructors. The supplemental training program will train and certify 80 faculty from 60 community colleges in a four month period. Participating faculty will produce best practices documentation once they have begun instructing students. This documentation will be disseminated to other faculty via the web.

The Federal Cyber Service: Scholarships for Service (SFS) program is specifically designed to address cyber security education issues. Though it preceded the Act, it does address the law's intentions for capacity building and increased student involvement in cyber security through awards to some of the country's leading academic institutions. Since the inception of the program in mid-2001, SFS has made 19 scholarship awards and 35 capacity building awards for a total of about $52.9 million. As a result of this investment, the Federal Government will have recruitment access to the pool of 200 students currently supported at the 19 scholarship institutions. By the end of FY 2004, NSF expects the pool of students to grow to 350. These individuals will all have degrees, BS, MS, or Ph.D.s in cyber security-related fields. All participating institutions have been designated as Centers of Academic Excellence in Information Assurance Education (CAE/IAE) by the National Security Agency or equivalent. Four new schools have just been accorded Center status and their students will enter the program starting this fall.

Q4b. Have programs been started to provide grants to institutions of higher education to establish traineeship programs for graduate students in computer and network security research and to enable these students to pursue academic careers in cyber security after they graduate?

A4b. NSF's primary support of graduate students in the cyber security arena is through research assistantship support in cyber security research and education grants. The increasing number of awards made in this area will support as many as several hundred graduate students in computer and network security in FY'03. It is expected that a significant percentage of these students will pursue academic careers upon graduation with the doctoral degree.

In addition to support through research assistantships, graduate students can also be supported through traineeships and fellowships awards via programs such as the Integrative Graduate Education and Research Training (IGERT) and the Graduate Research Fellowships programs. NSF will continue to encourage the submission of cyber security traineeship and fellowship proposals through these programs, and will fund leading projects as they emerge. However the agency anticipates that as for other fields of science, graduate student support will mainly be provided through research assistantships.

SFS institutions are supporting graduate students who are uniquely qualified to enter academia as the next generation of cyber security faculty members. The program has recently been expanded to include active Ph.D. students. Plans are under development to increase both the number of yearly graduates and the overall capacity of the national higher education enterprise to produce the most qualified graduates and potential new faculty members in the field of cyber security. At the same time, the capacity building awards under SFS include activities that support the development of faculty members with expertise in the area of Information Assurance.

Q5. How does NSF work with other agencies that have cyber security research and development programs?

Q5a. Do you coordinate overall federal goals with the other agencies, and if so, can you describe some of the technical milestones or goals in workforce development?

A5a. NSF coordinates its investments in cyber security workforce development with other agencies in the following ways:

The NSF Scholarships for Service program has helped the Federal Government achieve several milestones that are key to cyber security. Through the Federal Cyberservice Initiative, the Federal Government has increased access to talented cyber security students prior to graduation. NSF has coordinated with the National Security Agency (NSA) to make capacity building awards to qualified institutions that wish to achieve certification as NSA Cyber Security Centers of Excellence.

Awardees funded by NSF, NSA and the Department of Defense will come together at the 2003 Cyber Service/Cyber Corps Student Symposium. The Symposium, to be held at Carnegie Mellon University's Center for Computer and Communications Security, will allow students to network across programs, as well as with their faculty mentors and senior Government officials. This coordinated symposium in which the students take center-stage is an example of the success that federal workforce development programs in cyber security are enjoying.

NSF is sponsoring a conference focused on cyber security education to be held on June 26–28, 2003. The third annual World Conference on Information Security Education (WISE3) will be held at the Naval Post Graduate School. The conference brings together leaders in computer security education from around the globe. The theme for the conference is "Teaching the Role of Information Assurance in Critical Infrastructure Protection."

In conjunction with WISE3, the Workshop on Education in Computer Security (WECS) will be held in the three days prior (also at the Naval Postgraduate School). WECS is an opportunity for educators to learn about fundamentals and recent advances in information assurance and computer security, and to improve their instructional capabilities in these areas. This annual forum allows instructors to share best practices and is a significant achievement in building the capacity of the Nation's cyber security education enterprise.

Q5b. Two interagency groups were discussed at the hearing: the Infosec Research Council (IRC) and the High Confidence Software and Systems group within the Networking and Information Technology Research and Development Interagency Working Group. How are these two groups related?

A5b. The Infosec Research Council (IRC) is an effective knowledge sharing body. Though it has no formal charter, the group has served as an important technical coordinating organization. Agency representatives use this as a forum to discuss security implementations and development activities that they are pursuing, which may have synergies with other agencies. This kind of informal coordination leads to joint-funded projects and helps to avoid duplication of effort in security development and implementation programs.

The High Confidence Software & Systems (HCSS) Program Component Area (PCA) of the NITRD–IWG concentrates on Research and Development of critical technologies that are needed to enable computer systems to achieve high levels of availability, reliability, safety, security, survivability, protection and restorability of information services. The members of this subgroup take a long-term view. Integrating the high-confidence attributes that are essential to secure software and systems requires formal scientific design principles, large-scale testing and new diagnostic and forensic tools. The HCSS informs development of the Administration's budget in this PCA.

Though the two groups have a different mandates, NSF staff are active in both and are working to find synergies along the path from research to implementation.

Q5c. Do the groups divide up tasks among various agencies? Do they monitor progress in cyber security research and development at the agencies?

A5c. Interagency collaboration is well established in the area of cyber security. Program Officers involved in these interagency working groups share programmatic information and cooperate in jointly funded projects.

In addition to the committees that regularly meet to exchange information and coordinate efforts discussed above, the federal cyber security enterprise sponsors workshops and meetings with the research and education community. One example of the cooperative effort in place is the NSF PI meeting to be held in August 2003. This meeting, held in cooperation with the Department of Homeland Security (DHS) and the National Institute of Standards and Technology (NIST), will be open to all federal personnel with an interest in cyber security. This kind of interagency information sharing is common and ensures that Program Officers are cognizant of the full federal portfolio of cyber security activity. It allows them to monitor progress made by other federal agencies and leverage it to their specific needs.

Q5d. You testified that the High Confidence Software and Systems group is working to define the federal portfolio of cyber security research and development and will identify gaps. When will that effort be complete? What follow-up actions will NSF and the other agencies in the group take?

A5d. The HCSS group, which is co-chaired by an NSF Program Officer, is approaching cyber security in the federal portfolio as an ongoing program. This work has already begun, and though the work will never be complete (cyber security will be a dynamic, changing research subject for the foreseeable future) that organization will

have a consolidated portfolio statement that includes new programs to fill gaps in the current portfolio by the end of the fiscal year.

The agenda will be organized around three interdependent topic areas: near-term reduced vulnerability, next-generation embedded security, and interoperable migration strategies. NSF will seek to increase funding, basing our priorities on the portfolio items that the group identifies. NSF will then look for opportunities to share funding with the other agencies involved in HCSS, CIIP, and IRC.

ANSWERS TO POST-HEARING QUESTIONS

Responses by Arden L. Bement, Jr., Director, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce

Questions submitted by Chairman Sherwood Boehlert

Q1. The National Institute of Standards and Technology (NIST) has not yet begun the grants to institutions of higher education that are partnering with companies on cyber security research and development or the re-training fellowships to increase the cyber security workforce, both of which are authorized by the Cyber Security Research and Development Act. *How much funding would NIST need to implement these programs? Will NIST request these funds for fiscal year 2005?*

A1. NIST has provided twelve cyber security research grants in the past two years: one to the Critical Infrastructure Protection Project; nine to various recipients under the NIST 2001 Critical Infrastructure Protection Grants Program; and two to the Institute for Information Infrastructure Protection (I3P) at Dartmouth College's Institute for Security and Technology Studies, as described below. Note that, in addition, related awards have been made under the NIST Advanced Technology Program and Small Business Innovative Research program.

Critical Infrastructure Protection Project (CIP Project)

The CIP Project is a joint effort of George Mason University and James Madison University to develop a nationally recognized program that fully integrates the disciplines of law, policy, and technology for enhancing the security of cyber networks and supporting the Nation's critical infrastructures. The consideration of all three disciplines—law, policy, and technology—is what makes the CIP Project unique. The CEP Project is funded by a NIST FY 2002 grant of $6.5 million. We expect to provide another $6.5 million in FY03 to fund this activity.

The CIP Project's research uniquely and innovatively aligns scholarly research with national goals and objectives. Current projects include the following:

Economic Incentives for Cyber Security: Working closely with Nobel Laureate Vernon Smith, the CEP Project is developing software to conduct replicable human use experiments to study how individuals create markets to share risk through self-insuring cyber networks, secondary insurance markets, contracting, and standards development. There are no similar products available for our nation's critical infrastructure owners.

Securing the Internet Infrastructure: The CIP Project is developing a comprehensive "map" of our nation's telecommunications infrastructure and examining how connectivity and performance are affected by removal of critical cities (nodes) resulting from physical attacks on key infrastructure facilities. Presently, critical infrastructures owners do not have access to such a map for security planning or disaster mitigation.

Cyber Attacker Digital Fingerprinting: The CIP Project is developing methods to identify cyber attackers based on characteristics discovered during and after their attacks using data mining tools and techniques. Additional research will examine the complex intellectual property and privacy implications of this developing technology.

Network Security Risk Assessment Model (NSRAM): The CIP Project is creating a tool (the NSRAMT) that will model, detect, and assess network vulnerabilities to facilitate enhanced risk quantification, intrusion detection, and network security. The NSRAMT improves upon existing tools by incorporating the time dimension into the assessment of cyber vulnerabilities.

NIST Critical Infrastructure Protection Grants Program

In September 2001, NIST awarded $5M to nine grant recipients under the FY 2001 Critical Infrastructure Protection Grants Program (CIPGP) to improve the robustness, resilience, and security information in all the critical infrastructures. Under the competitive grant application process, we received 133 proposals requesting roughly $73M from applicants in both industry and academia. We selected proposals in intrusion detection, telecommunications, wireless security, electric power infrastructure, and compiler security.

Funded research addresses a variety of topics to include tools and methods for analyzing security and detecting attacks due to vulnerabilities introduced by merging of data networks (i.e., the Internet) and voice networks (i.e., the public switched telephone network). Other topics addressed are attack detection for wireless and

converged networks, security controls for protecting the North American power grid, and methods for evaluating intrusion detection systems.

While results are still preliminary from the Grants program and some projects will not be completed due to a discontinuation of program funding, important developments were made in wireless security, converged data/IP networks, and electric power infrastructure security. Additional information is available via http://csrc.nist.gov/grants/index.html

Institute for Information Infrastructure Protection (I3P)

The Institute for Information Infrastructure Protection (I3P) at Dartmouth College's Institute for Security and Technology Studies is a consortium of twenty-three academic and not-for-profit research organizations focused on cyber security and information infrastructure protection research and development (R&D). The I3P helps protect the information infrastructure of the United States by developing a comprehensive, prioritized R&D Agenda for cyber security and promoting collaboration and information sharing among academia, industry, and government. NIST participated in providing input to the I3P's Cyber Security Research and Development Agenda (January 2003) that identified the following as priority research areas:

- Enterprise Security Management;
- Trust Among Distributed Autonomous Parties;
- Discovery and Analysis of Security Properties and Vulnerabilities;
- Secure System and Network Response and Recovery;
- Traceback, Identification, and Forensics;
- Wireless Security;
- Metrics and Models; and
- Law, Policy, and Economic Issues.

Discussion of the I3P's research methodology and details on each of these topics is available in the I3P's R&D Agenda at http://www.thei3p.org/documents/2003 Cyber Security RD Agenda.pdf

The activities of the I3P are supported by NIST grants of $3 million in FY 2001 and $3 million in FY 2002.

While these activities are not specifically identified in the *Cyber Security Research and Development Act,* they demonstrate NIST's commitment to cyber security research. NIST will do its best to fulfill the specific requirements of the *Cyber Security Research and Development Act of 2002* within present resources and through future budget cycles.

Q2. At the hearing, you described the importance of standards for information security. What are some examples of these standards? How will NIST and the Department of Homeland Security (DHS) be working together on such standards? Will NIST and DHS be working together on communications for first responders?

A2. Examples of standards that are important for information security include cryptographic-based standards used for encryption (e.g., Advanced Encryption Standard) and for digital signatures. Although not formal standards, other security specifications are also important, such as recommendations for security settings for specific products and for security features for procured information technology products.

When appropriate, NIST and DHS will be working together on these standards and other cyber security standards and specifications through collaborative research and planning, formal exchange of personal, sharing of information, and joint private sector outreach. All of these activities will be facilitated by the recently signed Memorandum of Understanding between DHS and the Technology Administration (TA) of the Department of Commerce. NIST and DHS will also be working together on cyber security standards and biometrics through the American National Standards Institute—Homeland Security Standards Panel (ANSI–HSSP). The Chief of NIST's Standards Services Division co-chairs the ANSI–HSSP.

NIST will work with DHS to ensure that our work is complementary, while maintaining our necessary independence. Of course, DHS, like all other federal agencies, can take advantage of NIST cyber security guidelines and standards to protect its sensitive information and systems. Additionally, like other federal organizations, NIST will invite DHS to comment and review NIST's draft security standards and guidelines. Our collaboration is furthered by having DHS membership on our Information Security and Privacy Advisory Board.

With regard to first responders communications, NIST and the Department of Homeland Security have already begun to coordinate efforts aimed at improving the

communications capabilities of first responders. NIST's Office of Law Enforcement Standards, in partnership with DHS' Science and Technology Directorate and the National Institute of Justice, will be hosting a Summit on Interoperable Communications for Public Safety at the end of June. The goal of the Summit will be to gather all of the federal and national programs together that are in some way addressing public safety communications and provide an understanding on how the various programs inter-relate, thus facilitating improved information sharing, coordination, and focus in this important area. In addition, NIST has been, and will continue to work closely with DHS' SAFECOM program, to provide scientific, engineering, and standards expertise to the public safety community.

Q3. The Cyber Security Research and Development Act *emphasizes the importance of workforce development, and the Committee believes that it is important to train skilled professionals to execute information technology security in the private sector and at government agencies, as well as scientists and engineers to perform cyber security research and development. What do you see as particular workforce needs in cyber security? What actions is your agency taking or planning to take to provide education and training in the cyber security area?*

A3. Workforce needs in cyber security include skilled researchers in the areas of system vulnerabilities and in security technology, metrology, and testing. A larger and more-skilled workforce in the area of systems operations, specifically experts that can use today's tools and techniques to better secure existing critical systems, is also needed. The range of skills required is discussed in NIST Special Publication 800–16. (See http://csrc.nist.gov/publications/nistpubs/index.html) NIST has a role in providing guidance on training; a draft NIST guideline is currently out for public review. We work with universities (contributor/evaluator for the NSA Centers of Excellence program), with industry certification groups, such as International Information Systems Security Certification Consortia, CompTIA, and SANS, and with the Federal Information Systems Security Educators Association to develop training guidelines.

NIST provides education and training by hosting various security workshops and conferences in the area of cyber security and related fields. For example, we hosted a workshop on advanced public key infrastructure research in April. We are also hosting a workshop on IT security and capital planning in June.

Q4. How does NIST work with other agencies that have cyber security research and development programs?

a. Do you coordinate overall federal goals with the other agencies, and if so, can you describe some of the technical milestones or goals in workforce development?

b. Two interagency groups were discussed at the hearing: the Infosec Research Council (IRC) and the High Confidence Software and Systems group within the Networking and Information Technology Research and Development Interagency Working Group. How are these two groups related? Does NIST participate in both groups?

c. Do the groups divide up tasks among various agencies? Do they monitor progress in cyber security research and development at the agencies?

A4. NIST works with DARPA, NSF, OSTP, OMB, NSA, and a range of other federal and private sector organizations involved in cyber security research. In the specific area of workforce development, NIST participates in the Service for Scholarship program by hiring students and interns. We assist NSA in reviewing their annual applications for their centers of excellence designation. NIST also has been assigned new responsibilities under the *Cyber Security R&D Act* for awarding cyber security fellowships. In addition, our current CIO recently served a two-year tour as Director of the National Coordination Office (NCO) for Information Technology Research and Development, reporting to OSTP. The NCO's work involves twelve federal agencies. The High Confidence Software and Systems (HCSS) Working Group is the most focused on cyber security issues.

NIST participates in both the Infosec Research Council (IRC) and the High Confidence Software and Systems group within the Networking and Information Technology Research and Development Interagency Working Group. The IRC serves to share research priorities and activities, specifically in the area of cyber security. As its charter describes:

> "The INFOSEC Research Council (IRC) consists of U.S. Government sponsors of information security research from the Department of Defense, the Intelligence Community, and Federal Civil Agencies. The IRC provides its member-

ship with a community-wide forum to discuss critical information security issues, convey the research needs of their respective communities, and describe current research initiatives and proposed courses of action for future research investments. By participating in the IRC, sponsors obtain and share valuable information that will help focus their information security research programs, identify high-leverage, high-value research targets of opportunity, and minimize duplication of research. The IRC will be a collective effort for the mutual benefit and collaboration of the participating organizations and is intended to promote intelligent information security research investments. While it is understood that each participating agency will have its own research priorities, it is anticipated that the IRC will be able to identify high priority areas of research to develop a common, shared appreciation of the important and challenging information security problems of the day." (www.infosec-research.org)

The NCO's HCSS Working Group is more broadly focused than just cyber security: (www.itrd.gov)

> The National Coordination Office (NCO) for Information Technology Research and Development (IT R&D) coordinates planning, budget, and assessment activities for the Federal Networking and IT R&D Program. This 12-agency collaborative effort pioneers fundamental advances in the critical technologies of the Nation's information infrastructure, including high performance computing, large-scale networking, and high assurance software and systems design.

The NCO reports to the *White House Office of Science and Technology Policy and the National Science and Technology Council (NSTC).* The NCO works with the participating federal agencies through the NSTC's *Interagency Working Group (IWG)* on IT R&D and six IWG Coordinating Groups to prepare and implement the $2 billion Federal IT R&D budget crosscut. Since no one federal agency cites IT R&D as its primary mission, it is vital for agencies to coordinate, collaborate, and cooperate to help increase the overall effectiveness and productivity of Federal IT R&D. The major research emphases of the IT R&D effort are called Program Component Areas (PCAs).

The High Confidence Software and Systems (HCSS) Program Component Area (PCA) concentrates on Research and Development into critical technologies that are needed to enable computer systems to achieve high levels of availability, reliability, safety, security, survivability, protection and restorability of information services.

Q5. The Cyber Security Research and Development Act *makes the National Science Foundation (NSF) the lead agency for cyber security research and development, as Dr. Colwell testified at the hearing. In what ways are you interacting with NSF as it acts as the lead agency in this area? Does NSF review your budget proposal for programs in this area? Does NSF lead the agencies in a group effort to determine overall cyber security research and development priorities, and if so, how?*

A5. We meet regularly with NSF personnel via the IRC, as described above. NSF does not review NIST budget proposals. In addition, as discussed earlier, NIST's current CIO recently served a two-year tour as Director of the National Coordination Office (NCO) for Information Technology Research and Development, reporting to OSTP. The NCO's work involves twelve federal agencies, including NSF.

Appendix 2:

Additional Material for the Record

INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

Established by the Computer Security Act of 1987
[Amended by the Federal Information Security Management Act of 2002]

April 8, 2003

The Honorable Mitchell E. Daniels, Jr.
Director
Office of Management and Budget
17th Street and Pennsylvania Avenue, N.W.
Washington, D.C. 20503

Dear Mr. Daniels:

The Information Security and Privacy Advisory Board is a Federal advisory committee established by the Computer Security Act of 1987, as amended. The law directs the Board to identify emerging managerial, technical, administrative, and physical safeguard issues relative to information security and privacy in government systems. The Board is then to advise, among others, the Director, Office of Management and Budget and the Secretary of Commerce and to report its findings to the Secretary of Commerce, the Office of Management and Budget, the Director of the National Security Agency, and the appropriate committees of the Congress.

At the Board's March meeting, we reviewed and discussed the National Strategy to Secure Cyberspace, issued in February 2003. Our review was preceded by a discussion with David Howe of the President's Critical Infrastructure Protection Board staff at the Board's December 2002 meeting. Mr. Howe briefed us on the process leading to the development of the final Strategy and invited us to submit Board comments. We submitted our comments on December 20, 2002, and are providing you with a copy.

The Board understands that it is the government's intent to treat the Strategy as a living document, that additional development of actions and recommendations will follow, and that the Strategy will evolve. The Board believes the following considerations are important to ensure that the Strategy's objectives are met as government moves forward to implement the document's actions and recommendations.

Implementation of the Strategy can benefit from existing government programs and capabilities. A number of important initiatives are already underway at the Department of Commerce's National Institute of Standards and Technology (NIST) that will provide significant and near-term support for key action and recommendations. For example, with respect to Action/Recommendations 3-1 and 3-3, NIST is already conducting security awareness seminars for the small business community.

Secretariat: National Institute of Standards and Technology
100 Bureau Drive, Stop 8930, Gaithersburg, MD 20899-8930
Telephone: 301/975-3357 *** Fax: 301/926-2733

Additionally, work underway at NIST, primarily in the Information Technology Laboratory, can directly support the Strategy's actions and recommendations. For example, these include commercial product security evaluation and validation, computer security and biometric standards development and testing, and programs to improve software quality. Increased direct funding for NIST programs should be given high priority.

With respect to Action/Recommendation 4-4, the Board questions the value of reviewing lessons-learned from implementation of the Defense Department's July 2002 policy requiring the acquisition of evaluated products. This policy has not been in place long enough to yield significant results. The Board also recommends that the broader review of the National Information Assurance Partnership (NIAP) include private sector participation in the examination.

The Strategy includes many recommendations for actions by the private sector to help secure cyberspace. In most instances the Strategy does not describe what Federal agencies can or should do to help advance such action through mechanisms routinely available to government. These include direct funding, indirect incentives such as creation of joint public-private forums and projects, or the use of existing regulations in support of cyber security.

As observed in the Strategy, a principal mechanism government has to compel action is its own purchasing power. It would be useful to require agencies to report periodically to OMB what they have done or are doing in their own procurement processes to purchase products and services in a fashion that promotes achieving the goals prescribed by the Strategy. Such guidance might be built into OMB's reporting process under the Federal Information Security Management Act (FISMA).

Regulatory authority already available to many agencies (such as FAA, NRC, EPA, DOL, FTC, SEC, FCC, Department of Health and Human Services, Department of the Treasury, and others) can be used to accelerate implementation of specific recommendations and actions made in the Strategy where appropriate. As the Strategy is implemented, it would be useful to ask agencies to report periodically to OMB and DHS what they have done or are doing with their regulatory authority to meet the goals prescribed by the Strategy. Agencies should also be asked to report whether changes to their regulatory authority are warranted to enhance their capabilities in this area.

As examples, compliance with the requirements of the Sarbanes-Oxley Act of 2002 could include the implementation of an effective information security program to help ensure the safeguarding of corporate information assets and the integrity of financial reporting. There are already precedents for this, as Department of Health and Human Services, Federal Energy Regulatory Commission, and the Nuclear Regulatory Commission, among others have sought NIST's advice with respect to information security implementations in support of regulations.

The Strategy raises larger issues arising from the increased policy and operational intersection between public and private sector critical infrastructure protection organizations and systems. Many of the Strategy's actions and recommendations point to a blurring of roles and responsibilities between what had been traditionally seen as national security and non-national security systems.

Recognizing the intent of the Computer Security Act of 1987, as reaffirmed by FISMA, this is an issue that must be addressed more directly. Additionally, the Strategy minimally acknowledges the critical issue of information and citizen privacy and fails to provide specific actions or recommendations. The Board believes this must be addressed as well.

We thank you for your consideration.

Sincerely,

Franklin S. Reeder
Chairman

Enclosure

July 8, 2003

CURRENT ACTIVITIES OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY IN CYBER SECURITY AND RELATED PROGRAMS

1. Cyber Security Research Grants

NIST has provided twelve cyber security research grants in the past two years: one to the Critical Infrastructure Protection Project; nine under the NIST 2001 Critical Infrastructure Protection Grants Program and two to the Institute for Information Infrastructure Protection (I3P) at Dartmouth College's Institute for Security and Technology Studies. Each will be briefly described. Note that, in addition, related awards have been made under the NIST Advanced Technology Program and Small Business Innovative Research program, but for the sake of brevity, they will not be included at this time.

Critical Infrastructure Protection Project (CIP Project)

The CIP Project is a joint effort of George Mason University and James Madison University to develop a nationally recognized program that fully integrates the disciplines of law, policy, and technology for enhancing the security of cyber networks and economic processes supporting the Nation's critical infrastructures. The consideration of all three disciplines—law, policy, and technology—is what makes the CIP Project unique. The CIP Project is funded by a NIST FY 2002 grant of $6.5 million. NIST expects to provide another $6.5 million in FY03 to fund this activity.

The CIP Project's research agenda serves as a unique and innovative approach to aligning scholarly research with national goals and objectives. Current projects include the following:

Economic Incentives for Cyber Security: Working closely with Nobel Laureate Vernon Smith, the CIP Project is developing software to conduct replicable human use experiments to study how individuals create markets to share risk through self-insuring cyber networks, secondary insurance markets, contracting, and standards development. There are no similar products available for our nation's critical infrastructure owners.

Securing the Internet Infrastructure: The CIP Project is developing a comprehensive "map" of our nation's telecommunications infrastructure and examining how connectivity and performance are affected by removal of critical cities (nodes) resulting from physical attacks on key infrastructure facilities. Presently, critical infrastructures owners do not have access to such a map for security planning or disaster mitigation purposes.

Cyber Attacker Digital Fingerprinting: The CIP Project is developing technological methods to identify cyber attackers based on characteristics discovered during and after their attacks using data mining tools and techniques. Additional research will examine the complex intellectual property and privacy implications of this developing technology.

Network Security Risk Assessment Model (NSRAM): The CIP Project is creating a tool (the NSRAMT) that will model, detect, and assess network vulnerabilities in order to facilitate enhanced risk quantification, intrusion detection, and network security. The NSRAMT improves upon existing tools by incorporating the time dimension into the assessment of cyber vulnerabilities.

NIST Critical Infrastructure Protection Grants Program

In September 2001, NIST awarded $5M to nine grant recipients under the FY 2001 Critical Infrastructure Protection Grants Program (CIPGP) to improve the robustness, resilience, and security information in all the critical infrastructures. Under the competitive grant application process, NIST received 133 proposals requesting roughly $73M from applicants in both industry and academia. Proposals selected were in intrusion detection, telecommunications, wireless security, electric power infrastructure, and compiler security.

Funded research addresses a variety of topics to include tools and methods for analyzing security and detecting attacks due to vulnerabilities introduced by merging of data networks (i.e., the Internet) and voice networks (i.e., the public switched telephone network). Other topics addressed are attack detection for wireless and converged networks, the development of security controls for protecting the North American power grid, and methods for evaluating intrusion detection systems.

While results are still preliminary from the Grants program and some projects will not be completed due to a discontinuation of program funding, NIST will still produce important results especially in the wireless area, converged data/IP networks and security of the electric power infrastructure. Additional information is available via http://csrc.nist.gov/grants/index.html

Institute for Information Infrastructure Protection (I3P)

The Institute for Information Infrastructure Protection (I3P) at Dartmouth College's Institute for Security and Technology Studies is a consortium of twenty-three academic and not-for-profit research organizations focused on cyber security and information infrastructure protection research and development (R&D). The UP helps protect the information infrastructure of the United States by developing a comprehensive, prioritized R&D Agenda for cyber security and promoting collaboration and information sharing among academia, industry, and government. NIST participated in providing input to the I3P's Cyber Security Research and Development Agenda (January 2003) that identified the following as priority research areas:

- Enterprise Security Management;
- Trust Among Distributed Autonomous Parties;
- Discovery and Analysis of Security Properties and Vulnerabilities;
- Secure System and Network Response and Recovery;
- Traceback, Identification, and Forensics;
- Wireless Security;
- Metrics and Models; and
- Law, Policy, and Economic Issues.

A substantial discussion about the I3P's research methodology and details on each of these topics is available in the I3P's R&D Agenda at http://www.thei3p.org/documents/2003 Cyber Security RD Agenda.pdf

The activities of the I3P are supported by NIST grants of $3M in FY 2001 and a second $3M in FY 2002. NIST expects to provide a third $3M grant in FY 2003 to I3P.

2. National Research Council Study of Network Vulnerabilities

As called for by CSRDA, NIST is also moving forward with steps to fund, in collaboration with DARPA, a National Research Council study to review the vulnerabilities and inter-dependencies in NIST's critical infrastructure networks and identify appropriate research needs and associated resource requirements. NRC colleagues have already identified a study director and are ready to initiate this study.

3. Security of Supervisory Control and Data Acquisition Systems (SCADA)

SCADA computerized systems play a key role in controlling industrial processes in the food, pharmaceutical, chemical, and oil and gas industries, and other critical sectors of the economy. These systems, typically designed as stand-alone systems, are now often networked and managed via the Internet. This means that they are now vulnerable to the same panoply of security vulnerabilities that confront all other Internet-connected systems. NIST's work in this area is aimed at building more secure industrial control systems to protect against threats by terrorists, hackers, disgruntled employees or anyone else intent on these vitally important elements of the Nation's infrastructure.

For example, in the area of SCADA systems used in electrical power generation and distribution, legacy systems must be retrofitted with security hardware and software. NIST is working with EPRI, the electric power industry's research arm, to identify precisely where weaknesses exist and to develop security requirements for the real-time systems that control the power grid and other critical industrial processes.

In the area of automated building control systems, work is addressing the hardening of a host of complex systems that control lighting, ventilation, fire alarm and other critical systems. NIST is working with industry to develop security enhancements for building control systems and also with the General Services Administration to implement security features in government buildings.

4. Biometrics

The United States visa issuance and border entry-exit systems are required to use biometrics to prevent unauthorized persons from entering the U.S. through nearly 400 air, sea, and land ports of entry. Biometrics are automated methods of recognizing a person based on physical or behavioral characteristics.

In response to mandates in the *USA PATRIOT Act* and the *Enhanced Border Security and Visa Entry Reform Act,* NIST helped develop a report to Congress, submitted jointly by the Departments of Justice and State and NIST, on February 4, 2003, in which NIST recommended that at least two fingerprints and a face image be used as the required biometrics. This recommendation was made as a result of biometric tests that used hundreds of thousands of samples of real-world data ob-

tained from the State Department, the Immigration and Naturalization Service (INS), the Texas Department of Public Safety, and the Federal Bureau of Investigation (FBI).

NIST has also obtained a system that models the FBI's Integrated Automated Fingerprint Identification System (IAFIS) and has tested this system. The results provide accuracy measurements of the FBI fingerprint matching system, which is also mandated in the *PATRIOT Act.* These measurements are crucial for determining how to best perform background checks of foreign nationals applying for visas.

NIST has also been working on standards development for biometrics to provide inter-operability among different biometric vendors. NIST developed and spearheaded the adoption of a standard for inter-operability and exchange of fingerprint and facial image information. This standard is mandatory for data exchange between the FBI and state law enforcement organizations. Working through biometrics standards committees, NIST is developing image-based standards for face, finger, and iris that will lead to inter-operability. NIST is also submitting its biometric evaluation methodology as a testing standard to the International Committee for Information Technology Standards. Finally, NIST's testing results are being used to formulate the U.S. position on biometrics with the International Civil Aviation Organization (ICAO), which establishes international passport standards.

5. Forensics

Law enforcement officials and cyber security experts need to sort through the reams of files on computers in a timely manner to find evidence of terrorist and other criminal activities and to find evidence of cyber security events. Moreover, once digital evidence is uncovered, it is in danger of not being accepted in the U.S. court system. In order to enable the investigation and the subsequent prosecution in court, computer forensics must be based on sound, scientific practices that are produced and validated by neutral third parties.

In response to this need, NIST, working in partnership with the National Institute of Justice, the FBI, the U.S. Secret Service, the U.S. Customs Service, the DOD, and many State and local agencies, has developed two computer forensics products: the National Software Reference Library (NSRL) and the Computer Forensics Tool Testing (CFTT) Program. These products are used daily to help solve thousands of cases, including terrorism investigations.

Besides helping solve crimes, the products also help defend digital evidence that is introduced in court by prosecutors. The first high profile case to address this is the case of alleged terrorist Zacarias Moussaoui. As summarized by CNN, "The (prosecutor's) highly technical report on the computers and e-mail search followed a request by court-appointed defense attorneys assisting Moussaoui that computer evidence be authenticated." The "highly technical report," filed by the Government, relies heavily on NIST and specifically references the CFTT project.

Cyber security experts outside of law enforcement are also using these tools. The MIT computer security researchers who set out to prove that significant confidential information can be found on discarded computers used the NSRL as part of their process. They found over 5000 credit card numbers, medical records and a year of ATM transactions. See http://www.msnbc.com/news/859843.asp?cpl=l

6. Network Security

NIST's efforts in Internet security research are focused on both near-term objectives of expediting significant improvements to the security and integrity of today's Internet technologies, and longer-term objectives such as exploring the use of quantum information theory to develop ultra-secure networking technologies of the future.

Our near-term research is directed at working with industry and other government agencies to improve the inter-operability, scalability and performance of new Internet security systems and to expedite the development of Internet infrastructure protection technologies. NIST staff is actively working with the Internet Engineering Task Force (IETF) to design, develop, standardize and test new protocols that will make authentication, confidentiality and integrity services inherent capabilities of all networks based upon Internet technologies. NIST has taken leadership roles within the IETF in the specification of public key infrastructure, network layer security and key management technologies. Working shoulder to shoulder with industry, NIST is contributing technical specifications, modeling and analysis results, research prototypes and test and measurement tools to the IETF community to expedite the standardization of ubiquitous Internet security services and to foster the rapid development of commercial products.

Another area of focus for the near-term efforts is the research and development of technologies to protect the core infrastructure of Internet. NIST is working with the IETF and other government agencies to devise means to protect the control protocols and infrastructure services that underlie the operation of today's Internet. NIST's research and standardization efforts in this area include: extensions to the Domain Name System (DNS) to add cryptographic authentication to this most basic Internet service, and the design and analysis of protection and restoration mechanisms to improve failure resilience of core switching and routing infrastructures. NIST's future work in this area will focus on improving security and resilience of core Internet routing protocols.

Looking further into the future, NIST sees the potential for new computational paradigms to threaten the mathematical underpinnings of today's cryptographic systems. In response, NIST is conducting research in the use of quantum information theory to devise ultra-secure network technologies that are not dependent upon today's cryptographic techniques. NIST is collaborating with other government agencies in the design and evaluation of quantum information network technologies, ranging from physical devices capable of operating on single photons of a high speed optical link, to next generation quantum key distribution protocols capable of exploiting these physical links to devise provably secure cryptographic techniques.

7. Public Key Infrastructure (PKI)

In the past NIST has done research on PKI, primarily on effective revocation strategies and strategies for building large heterogeneous PKIs; however, today efforts are primarily focused on devising effective assurance tests for PKI components and clients. Assurance testing is an important research topic because assurance tests that are repeatable and meaningful provide a means for vendors to improve the security quality of their products. NIST is attempting to develop specific pass/fail tests and techniques for PKI assurance testing based on specific test requirements, and thus streamlining PKI security testing as compared to ad hoc conventional security assurance evaluation testing that requires a great deal of product-specific design analysis. There has been some success with this in Certificate Issuing and Management Components (CIMC) protection profile, for testing certification authorities, which breaks new ground in several areas. Work is now extending into client testing, which is more challenging and technically complex.

NIST also hosts and cosponsors, along with Internet2, an annual PKI research conference. Recently, informal collaborations were begun with investigators at the Korean Information Security Agency (KISA). We are seeking to invent a secure authenticator for sensitive personal information in PKI certificates to enable the subject to authenticate personal information if he or she chooses to divulge it.

8. Quantum Information Systems and Quantum Cryptography

NIST is working on a scalable quantum information network test-bed for research in quantum computing and cryptography. While current cryptosystems are extremely hard to break, quantum cryptography has the potential to provide truly unbreakable codes. A quantum information network is built to exploit the laws of quantum mechanics. Present day engineering of computational systems (e.g., clock speed for a processor, maximum size of memory) and implementation of algorithms (including cryptographic algorithms) are limited by the laws of classical mechanics. The results provided by quantum mechanics point out the potential for capabilities for computing and communication beyond that theoretically possible with the known laws of classical mechanics. This is the reason that quantum computation and quantum communication have become prime areas of research for applications for quantum mechanics.

NIST seeks to develop an extensible quantum information testbed and the scalable component technology essential to the practical realization of a quantum communication network. Quantum cryptographic systems are the first products of quantum computing research to advance to the commercial stage, with two products currently on the market. This market is expected to continue to grow, producing products for both government and commercial use. The testbed will demonstrate quantum communication and quantum cryptographic key distribution with high data rate. This testbed, once developed, will provide a measurement and standards infrastructure that will be open to the scientific community and will enable wide-ranging experiments on both the physical- and network-layer aspects of a quantum communication system. The infrastructure will be used to provide calibration, testing, and development facilities.

Quantum cryptography offers several advantages over traditional methods, including stronger security, eavesdropping detection, and the ability to generate and distribute large amounts of keying material more efficiently than conventional key dis-

tribution infrastructures. NIST has developed a hybrid authentication protocol for quantum networks, combining conventional and quantum methods. Authentication is critical for commercially viable quantum key distribution. In addition, this research has led to the discovery of serious vulnerabilities in many proposed quantum cryptographic protocols. Lessons learned from this research will assist quantum protocol developers in improving security, and provide the basis for incorporating quantum cryptographic module testing into the NIST Cryptographic Module Validation Program for the FIPS 140–2 standard.

9. Wireless Mobile Device Security

With the trend toward a highly mobile workforce, the acquisition of handheld devices such as Personal Digital Assistants (PDAs) is growing at an ever-increasing rate. These devices are relatively inexpensive productivity tools and are quickly becoming a necessity in today's business environment. Most handheld devices can be configured to send and receive electronic mail and browse the Internet. However, as handheld devices increasingly retain sensitive information or provide the means to obtain such information wirelessly, they must be protected.

NIST's efforts to date have focused on improving several aspects of security: user authentication, policy enforcement, and wireless communications. For user authentication NIST has developed a framework for multi-mode authentication that allows more than one authentication mechanism to contribute to the verification of a user's identity. For example, a biometric, such as voice input, may be required in combination with a security token, such as a smart card, before a user is permitted to access the contents of a device. In addition, NIST has invented a visual means of authentication that not only is easier than passwords for users to authenticate, but also significantly more powerful, and has contributed updates to an open source code initiative that allow smart cards to be used on certain handheld devices.

For policy enforcement, NIST has developed a system that requires users to present a policy certificate to a device, as a means of moving from a restricted processing environment to one in which the privileges accorded a user via the policy certificate are enabled. Policy rules govern such things as application usage, file access, and communications interfaces, including wireless communications. This mechanism allows organization policy controls to be asserted on handheld devices, which typically are at the fringes of an organization's influence, and was designed to tie in with emerging Public Key Infrastructures.

For wireless communications, NIST has developed a highly-regarded publication on Wireless Network Security, aimed at reducing the risks associated with 802.11 wireless local area networks and Bluetooth wireless networks that are commonly used with handheld devices. In the six months since its publication, the guideline has been downloaded over 120,000 times by users in over 50 countries.

Additionally, NIST is actively supporting the standards community in moving towards stronger, more robust security by integrating stronger, more secure cryptographic algorithms and their associated modes of operation into the next generation of the relevant standards. Two of the NIST 2001 Critical Information Protection Grants were awarded in the wireless security area to the University of Pittsburgh and the University of Maryland.

The University of Pittsburgh's research is studying interaction between the survivability and security of wireless information architectures. As part of this research, techniques for evaluating the survivability of wireless networks were developed, secure wireless architectures were designed, and strategies for meeting survivability and security requirements were examined. The impact of security services on performance, energy consumption, speed, and bandwidth were also simulated. The researchers demonstrated the interaction of survivability and security and proposed methods for measuring and optimizing both of these requirements. These results are expected to ultimately be applied to the design of critical wireless infrastructures.

The University of Maryland research is focused on a secure wireless testbed. There are several goals of the Secure Wireless LAN/MAN Infrastructure testbed. First, the testbed is testing the secure inter-operation between a multitude of different wireless equipment—both commercial and developmental. Second, the testbed supports research designed to address integration issues arising from the new draft security architecture for IEEE 802.11 (Enhanced Security Network), as well as security and management issues surrounding scalability, naming, and fraud control in wireless metropolitan networks. Finally, the testbed serves as a wireless security training apparatus for students, faculty, and other collaborators

10. Access Control

One of the basic tenets of IT security is controlling access to vital IT resources. NIST has been actively researching for many years more cost-effective and efficient

ways to administer access to critical system resources. In effect, NIST is answering the question "who is allowed to do what?" Access control mechanisms can take on many forms. Recognizing the inadequacies of traditional, labor-intensive, and error-prone approaches to controlling user access to sensitive information and the security benefits that could be gained via breakthroughs in access control technology, a NIST research team created a new approach to controlling user access, called Role-Based Access Control (RBAC). What is most striking about RBAC is its rapid evolution from a theoretical model to commercial implementation and deployment. An independently conducted NIST-sponsored economic impact study, conducted by RTI, estimated that the team's work will soon be used by some 30 millions users for access to sensitive information controlled using this technology. RBAC's productivity advantages alone are often sufficient to justify its deployment. An outside study by RTI estimated that RBAC technology saved U.S. industry $671 million, and that NIST was responsible for 44 percent of the savings giving the taxpayer a 10,900 percent return on investment.

11. Security Guidelines and Standards

NIST continues to develop standards and guidelines in support of its federal responsibilities. Many of these are also used, on a voluntary basis, by organizations in the private sector. Hundreds of thousands of copies of NIST guidelines have been downloaded from the NIST Computer Security Resource Center. For example, over 400,000 copies of NIST's Contingency Planning Guide for Information Technology have been downloaded since its publication less than a year ago. In 2002–2003, NIST published the following security guidelines:

- Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme;
- Federal S/MIME V3 Client Profile;
- Wireless Network Security: 802.11, Bluetooth, and Handheld Devices;
- Security Guide for Interconnecting Information Technology Systems;
- Security for Telecommuting and Broadband Communications;
- Guidelines on Electronic Mail Security;
- Guidelines on Securing Public Web Servers;
- Systems Administration Guidance for Windows 2000 Professional;
- Guidelines on Firewalls and Firewall Policy;
- Procedures for Handling Security Patches;
- Contingency Planning Guide for Information Technology Systems; and
- Risk Management Guide for Information Technology Systems.

See http://csrc.nist.gov/publications/nistpubs/index.html

NIST has also published the following draft guidelines for review by federal departments and agencies as well as other interested organizations and individuals concerning:

- Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems;
- Building an Information Technology Security Awareness and Training Program;
- Recommendation on Key Establishment Schemes;
- Recommendation on Key Management;
- Security Metrics Guide for Information Technology Systems;
- Recommendation for Block Cipher Modes of Operation: the RMAC Authentication Mode;
- Guide to Selecting IT Security Products;
- Guide to IT Security Services;
- Security Considerations in Federal Information Technology Procurements; and
- Guideline on Network Security Testing.

See http://csrc.nist.gov/publications/drafts.html

In addition, numerous NIST Information Technology Laboratory (ITL) Bulletins have been issued during the last year to provide guidance to agencies and others on a broad list of topics.

See http://www.itl.nist.gov/lab/bulletns/cslbull1.htm

NIST has also completed the Keyed-Hash Message Authentication Code as Federal Information Processing Standard (FIPS) 198 and provided three new secure hashing codes in the enhanced FIPS 180–2. These new enhanced secure hashing codes are used to help users create more secure digital signatures. While on the subject of cryptography, late in 2001, Secretary Evans approved the Advanced Encryption Standard (or AES) as a federal security standard and it is being actively adopted by voluntary standards bodies and implemented by vendors. In fact, over 70 commercial implementations of the AES have already been validated though NIST's Cryptographic Module Validation Program. See http://csrc.nist.gov/publications/fips/index.html and http://csrc.nist.gov/cryptval/aes/aesval.html

12. Reducing Vulnerabilities Through Security Testing

Both research and security testing can help reduce vulnerabilities in the commercial IT products used to support the Nation's critical infrastructures.

Research on identifying and correcting information technology vulnerabilities is urgently needed. When new technologies are identified that could potentially influence customers' security practices, NIST researches the technologies, their potential vulnerabilities and also work to find ways to apply new technologies in a secure manner. The solutions that NIST develops are made available to both public and private users. Some examples are methods for authorization management and policy management, ways to compensate for deficiencies in current wireless security standards, and ways to implement cryptography. Research helps us find more cost-effective ways to implement and address security requirements.

Security testing complements security standards by providing consumers with confidence that security standards and specifications are correctly implemented in the products that they buy. Implementing cryptography correctly and securely can be complicated. However, unless it is correctly implemented, it may provide no protection. Therefore, in conjunction with the Government of Canada's Communication Security Establishment, NIST operates the Cryptographic Module Validation Program, which helps ensure correct and secure implementation of NIST's cryptographic standards. The Cryptographic Module Validation Program has now validated over 500 modules with another 100 or more expected within the next year. This successful program utilizes private-sector accredited laboratories to conduct security conformance testing of cryptographic modules against the cryptographic federal standards NIST develops and maintains. The testing by the laboratories and NIST's work with Canada involves access to unclassified public algorithms and test suites, and not to any Federal Government operational cryptographic keys or classified information. Besides many organizations in the financial sector, two major U.S. corporations, Boeing and VISA, see such value to the benefits of the testing program that they now require CMVP-validated cryptographic modules to protect their sensitive information. The Government of the United Kingdom has also officially recognized CMVP-validated modules for use in their agencies.

To give a sense of the quality improvement that the program achieves, consider that statistics from NIST's testing laboratories show that 48 percent of the modules brought in for voluntary testing had security flaws that were corrected during testing. In other words, without NIST's program, the Federal Government would have had only a 50/50 chance of buying correctly implemented cryptography!

In addition, in recent years NIST has worked to develop the "Common Criteria" (ISO/IEC 15408), which can be used to specify security requirements. These requirements are then used by private-sector laboratories, accredited by NIST, for the voluntary evaluation of commercial products needed for the protection of government systems and networks. This work is undertaken in cooperation with the Defense Department's National Security Agency in our National Information Assurance Partnership (NIAP). You may be aware that the *National Strategy to Secure Cyberspace* calls for a review of the NIAP. Staff discussions have begun with NSA to identify ways that might improve the process, through research, process changes, and to understand the resources needed for NIAP to fully succeed.

13. Security Awareness and Outreach

Timely, relevant, and easily accessible information to raise awareness about the risks, vulnerabilities and requirements for protection of information systems is urgently needed. This is particularly true for new and rapidly emerging technologies, which are being delivered with such alacrity by industry. NIST also hosts and sponsors information sharing among security educators, the Federal Computer Security Program Managers' Forum, and industry. NIST actively supports information sharing through conferences, workshops, web pages, publications, and bulletins. Finally, NIST also has a guideline available to assist agencies with their training activities

and is an active supporter of the Federal Information Systems Security Educators' Association.

NIST sponsors the web-based Computer Security Resource Center (CSRC) to provide a wide-range of security materials and information to the community and link to the Federal Computer Incident Response Center at DHS and other emergency response centers. CSRC now has over 20 million "hits" annually. On CSRC, one of the most popular resources is the NIST-developed web-based tool known as ICAT that allows users to identify (and then fix) known vulnerabilities for their specific software. ICAT provides links to vendor sites at which the users can obtain patches to fix these vulnerabilities. This is important because many computer break-ins exploit well known vulnerabilities. Over 5500 vulnerabilities are now catalogued in this NIST on-line database that receives over 200,000 hits per month. See http://icat.nist.gov/icat.cfm

14. Security Assessment Guideline and Automated Security Self-Evaluation Tool (ASSET)

The Chief Information Officers Council and NIST developed a security assessment Framework to assist agencies with a very high level review of their security status. The Framework established the groundwork for standardizing on five levels of security and defined criteria agencies could use to determine if the levels were adequately implemented. By using the Framework levels, an agency can prioritize agency efforts as well as evaluate progress. Subsequently, NIST issued a more detailed security questionnaire that most agencies used in 2001 to conduct their program and system reviews. Last year, in cooperation with OMB, a PC-based automated version of the security questionnaire was developed and made available for use by agencies in 2002 to collect this information for annual agency security reporting to OMB.

15. Federal Agency Security Practices Website

NIST recently inaugurated the Federal Agency Security Practices (FASP) website (http://csrc.nist.gov/fasp/), building upon past successful work of the Federal CIO Council's Best Security Practices pilot effort to identify, evaluate, and disseminate best practices for CIP and security. NIST was asked to undertake the transition of this pilot effort to an operational program. As a result, NIST developed the FASP site, which contains agency policies, procedures and practices; the CIO pilot best practices; and, a Frequently-Asked-Questions section. Agencies are encouraged to share their IT security information and IT security practices and submit them for posting on the FASP site. Over 80 practices are now available via the site. Some practices have been modified so as not to identify the specific submitting agencies.

In accordance with tasking to NIST under FISMA, discussions are now underway to develop a similar web-based service to share security practices from private-sector organizations.

16. IT Product Security Configuration Checklists

The CSRDA tasked NIST with developing IT product security checklists that provide settings and option selections that minimize the security risks associated with each computer hardware or software system that is, or is likely to become, widely used within the Federal Government. In response, there are plans to hold a public workshop to focus on developing a standardized checklist template to structure configuration and related information. Vendors, agencies, and other reputable sources can use the template to construct and submit checklists that will populate a NIST public web-based repository. It should be noted that because of vendors' unique expertise, experience, and understanding of the security of their products, voluntary participation by vendors in this effort will be particularly sought and valued. The workshop will also serve to publicize NIST's plans to obtain checklists and make them available via the CSRC website. NIST will also be crafting ground rules for the selection and rejection of submitted checklists. Discussions have already taken place with representatives of DISA, NSA, NASA, and GAO regarding initial plans and to gain their valuable feedback. NIST hopes to hold the next checklists public workshop later this summer and unveil this new service by the end of the year.

Public Law 107–305
107th Congress

An Act

To authorize funding for computer and network security research and development and research fellowship programs, and for other purposes.

Nov. 27, 2002
[H.R. 3394]

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

Cyber Security Research and Development Act.
Communications and telecommunications.

SECTION 1. SHORT TITLE.

This Act may be cited as the "Cyber Security Research and Development Act".

SEC. 2. FINDINGS.

The Congress finds the following:

(1) Revolutionary advancements in computing and communications technology have interconnected government, commercial, scientific, and educational infrastructures—including critical infrastructures for electric power, natural gas and petroleum production and distribution, telecommunications, transportation, water supply, banking and finance, and emergency and government services—in a vast, interdependent physical and electronic network.

(2) Exponential increases in interconnectivity have facilitated enhanced communications, economic growth, and the delivery of services critical to the public welfare, but have also increased the consequences of temporary or prolonged failure.

(3) A Department of Defense Joint Task Force concluded after a 1997 United States information warfare exercise that the results "clearly demonstrated our lack of preparation for a coordinated cyber and physical attack on our critical military and civilian infrastructure".

(4) Computer security technology and systems implementation lack—

(A) sufficient long term research funding;

(B) adequate coordination across Federal and State government agencies and among government, academia, and industry; and

(C) sufficient numbers of outstanding researchers in the field.

(5) Accordingly, Federal investment in computer and network security research and development must be significantly increased to—

(A) improve vulnerability assessment and technological and systems solutions;

(B) expand and improve the pool of information security professionals, including researchers, in the United States workforce; and

(C) better coordinate information sharing and collaboration among industry, government, and academic research projects.

(6) While African-Americans, Hispanics, and Native Americans constitute 25 percent of the total United States workforce and 30 percent of the college-age population, members of these minorities comprise less than 7 percent of the United States computer and information science workforce.

15 USC 7402.

SEC. 3. DEFINITIONS.

In this Act:

(1) DIRECTOR.—The term "Director" means the Director of the National Science Foundation.

(2) INSTITUTION OF HIGHER EDUCATION.—The term "institution of higher education" has the meaning given that term in section 101(a) of the Higher Education Act of 1965 (20 U.S.C. 1001(a)).

15 USC 7403.

SEC. 4. NATIONAL SCIENCE FOUNDATION RESEARCH.

(a) COMPUTER AND NETWORK SECURITY RESEARCH GRANTS.—

(1) IN GENERAL.—The Director shall award grants for basic research on innovative approaches to the structure of computer and network hardware and software that are aimed at enhancing computer security. Research areas may include—

(A) authentication, cryptography, and other secure data communications technology;

(B) computer forensics and intrusion detection;

(C) reliability of computer and network applications, middleware, operating systems, control systems, and communications infrastructure;

(D) privacy and confidentiality;

(E) network security architecture, including tools for security administration and analysis;

(F) emerging threats;

(G) vulnerability assessments and techniques for quantifying risk;

(H) remote access and wireless security; and

(I) enhancement of law enforcement ability to detect, investigate, and prosecute cyber-crimes, including those that involve piracy of intellectual property.

(2) MERIT REVIEW; COMPETITION.—Grants shall be awarded under this section on a merit-reviewed competitive basis.

(3) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the National Science Foundation to carry out this subsection—

(A) $35,000,000 for fiscal year 2003;

(B) $40,000,000 for fiscal year 2004;

(C) $46,000,000 for fiscal year 2005;

(D) $52,000,000 for fiscal year 2006; and

(E) $60,000,000 for fiscal year 2007.

(b) COMPUTER AND NETWORK SECURITY RESEARCH CENTERS.—

(1) IN GENERAL.—The Director shall award multiyear grants, subject to the availability of appropriations, to institutions of higher education, nonprofit research institutions, or

consortia thereof to establish multidisciplinary Centers for Computer and Network Security Research. Institutions of higher education, nonprofit research institutions, or consortia thereof receiving such grants may partner with 1 or more government laboratories or for-profit institutions, or other institutions of higher education or nonprofit research institutions.

(2) MERIT REVIEW; COMPETITION.—Grants shall be awarded under this subsection on a merit-reviewed competitive basis.

(3) PURPOSE.—The purpose of the Centers shall be to generate innovative approaches to computer and network security by conducting cutting-edge, multidisciplinary research in computer and network security, including the research areas described in subsection (a)(1).

(4) APPLICATIONS.—An institution of higher education, nonprofit research institution, or consortia thereof seeking funding under this subsection shall submit an application to the Director at such time, in such manner, and containing such information as the Director may require. The application shall include, at a minimum, a description of—

(A) the research projects that will be undertaken by the Center and the contributions of each of the participating entities;

(B) how the Center will promote active collaboration among scientists and engineers from different disciplines, such as computer scientists, engineers, mathematicians, and social science researchers;

(C) how the Center will contribute to increasing the number and quality of computer and network security researchers and other professionals, including individuals from groups historically underrepresented in these fields; and

(D) how the center will disseminate research results quickly and widely to improve cyber security in information technology networks, products, and services.

(5) CRITERIA.—In evaluating the applications submitted under paragraph (4), the Director shall consider, at a minimum—

(A) the ability of the applicant to generate innovative approaches to computer and network security and effectively carry out the research program;

(B) the experience of the applicant in conducting research on computer and network security and the capacity of the applicant to foster new multidisciplinary collaborations;

(C) the capacity of the applicant to attract and provide adequate support for a diverse group of undergraduate and graduate students and postdoctoral fellows to pursue computer and network security research; and

(D) the extent to which the applicant will partner with government laboratories, for-profit entities, other institutions of higher education, or nonprofit research institutions, and the role the partners will play in the research undertaken by the Center.

(6) ANNUAL MEETING.—The Director shall convene an annual meeting of the Centers in order to foster collaboration and communication between Center participants.

(7) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated for the National Science Foundation to carry out this subsection—

(A) $12,000,000 for fiscal year 2003;
(B) $24,000,000 for fiscal year 2004;
(C) $36,000,000 for fiscal year 2005;
(D) $36,000,000 for fiscal year 2006; and
(E) $36,000,000 for fiscal year 2007.

15 USC 7404.

SEC. 5. NATIONAL SCIENCE FOUNDATION COMPUTER AND NETWORK SECURITY PROGRAMS.

(a) COMPUTER AND NETWORK SECURITY CAPACITY BUILDING GRANTS.—

(1) IN GENERAL.—The Director shall establish a program to award grants to institutions of higher education (or consortia thereof) to establish or improve undergraduate and master's degree programs in computer and network security, to increase the number of students, including the number of students from groups historically underrepresented in these fields, who pursue undergraduate or master's degrees in fields related to computer and network security, and to provide students with experience in government or industry related to their computer and network security studies.

(2) MERIT REVIEW.—Grants shall be awarded under this subsection on a merit-reviewed competitive basis.

(3) USE OF FUNDS.—Grants awarded under this subsection shall be used for activities that enhance the ability of an institution of higher education (or consortium thereof) to provide high-quality undergraduate and master's degree programs in computer and network security and to recruit and retain increased numbers of students to such programs. Activities may include—

(A) revising curriculum to better prepare undergraduate and master's degree students for careers in computer and network security;

(B) establishing degree and certificate programs in computer and network security;

(C) creating opportunities for undergraduate students to participate in computer and network security research projects;

(D) acquiring equipment necessary for student instruction in computer and network security, including the installation of testbed networks for student use;

(E) providing opportunities for faculty to work with local or Federal Government agencies, private industry, nonprofit research institutions, or other academic institutions to develop new expertise or to formulate new research directions in computer and network security;

(F) establishing collaborations with other academic institutions or academic departments that seek to establish, expand, or enhance programs in computer and network security;

(G) establishing student internships in computer and network security at government agencies or in private industry;

(H) establishing collaborations with other academic institutions to establish or enhance a web-based collection

of computer and network security courseware and laboratory exercises for sharing with other institutions of higher education, including community colleges;

(I) establishing or enhancing bridge programs in computer and network security between community colleges and universities; and

(J) any other activities the Director determines will accomplish the goals of this subsection.

(4) SELECTION PROCESS.—

(A) APPLICATION.—An institution of higher education (or a consortium thereof) seeking funding under this subsection shall submit an application to the Director at such time, in such manner, and containing such information as the Director may require. The application shall include, at a minimum—

(i) a description of the applicant's computer and network security research and instructional capacity, and in the case of an application from a consortium of institutions of higher education, a description of the role that each member will play in implementing the proposal;

(ii) a comprehensive plan by which the institution or consortium will build instructional capacity in computer and information security;

(iii) a description of relevant collaborations with government agencies or private industry that inform the instructional program in computer and network security;

(iv) a survey of the applicant's historic student enrollment and placement data in fields related to computer and network security and a study of potential enrollment and placement for students enrolled in the proposed computer and network security program; and

(v) a plan to evaluate the success of the proposed computer and network security program, including post-graduation assessment of graduate school and job placement and retention rates as well as the relevance of the instructional program to graduate study and to the workplace.

(B) AWARDS.—(i) The Director shall ensure, to the extent practicable, that grants are awarded under this subsection in a wide range of geographic areas and categories of institutions of higher education, including minority serving institutions.

(ii) The Director shall award grants under this subsection for a period not to exceed 5 years.

(5) ASSESSMENT REQUIRED.—The Director shall evaluate the program established under this subsection no later than 6 years after the establishment of the program. At a minimum, the Director shall evaluate the extent to which the program achieved its objectives of increasing the quality and quantity of students, including students from groups historically underrepresented in computer and network security related disciplines, pursuing undergraduate or master's degrees in computer and network security. Deadline.

(6) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the National Science Foundation to carry out this subsection—

(A) $15,000,000 for fiscal year 2003;
(B) $20,000,000 for fiscal year 2004;
(C) $20,000,000 for fiscal year 2005;
(D) $20,000,000 for fiscal year 2006; and
(E) $20,000,000 for fiscal year 2007.

(b) SCIENTIFIC AND ADVANCED TECHNOLOGY ACT OF 1992.—

(1) GRANTS.—The Director shall provide grants under the Scientific and Advanced Technology Act of 1992 (42 U.S.C. 1862i) for the purposes of section 3(a) and (b) of that Act, except that the activities supported pursuant to this subsection shall be limited to improving education in fields related to computer and network security.

(2) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the National Science Foundation to carry out this subsection—

(A) $1,000,000 for fiscal year 2003;
(B) $1,250,000 for fiscal year 2004;
(C) $1,250,000 for fiscal year 2005;
(D) $1,250,000 for fiscal year 2006; and
(E) $1,250,000 for fiscal year 2007.

(c) GRADUATE TRAINEESHIPS IN COMPUTER AND NETWORK SECURITY RESEARCH.—

(1) IN GENERAL.—The Director shall establish a program to award grants to institutions of higher education to establish traineeship programs for graduate students who pursue computer and network security research leading to a doctorate degree by providing funding and other assistance, and by providing graduate students with research experience in government or industry related to the students' computer and network security studies.

(2) MERIT REVIEW.—Grants shall be provided under this subsection on a merit-reviewed competitive basis.

(3) USE OF FUNDS.—An institution of higher education shall use grant funds for the purposes of—

(A) providing traineeships to students who are citizens, nationals, or lawfully admitted permanent resident aliens of the United States and are pursuing research in computer or network security leading to a doctorate degree;

(B) paying tuition and fees for students receiving traineeships under subparagraph (A);

(C) establishing scientific internship programs for students receiving traineeships under subparagraph (A) in computer and network security at for-profit institutions, nonprofit research institutions, or government laboratories; and

(D) other costs associated with the administration of the program.

(4) TRAINEESHIP AMOUNT.—Traineeships provided under paragraph (3)(A) shall be in the amount of $25,000 per year, or the level of the National Science Foundation Graduate Research Fellowships, whichever is greater, for up to 3 years.

(5) SELECTION PROCESS.—An institution of higher education seeking funding under this subsection shall submit an application to the Director at such time, in such manner, and containing such information as the Director may require. The application shall include, at a minimum, a description of—

(A) the instructional program and research opportunities in computer and network security available to graduate students at the applicant's institution; and

(B) the internship program to be established, including the opportunities that will be made available to students for internships at for-profit institutions, nonprofit research institutions, and government laboratories.

(6) REVIEW OF APPLICATIONS.—In evaluating the applications submitted under paragraph (5), the Director shall consider—

(A) the ability of the applicant to effectively carry out the proposed program;

(B) the quality of the applicant's existing research and education programs;

(C) the likelihood that the program will recruit increased numbers of students, including students from groups historically underrepresented in computer and network security related disciplines, to pursue and earn doctorate degrees in computer and network security;

(D) the nature and quality of the internship program established through collaborations with government laboratories, nonprofit research institutions, and for-profit institutions;

(E) the integration of internship opportunities into graduate students' research; and

(F) the relevance of the proposed program to current and future computer and network security needs.

(7) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the National Science Foundation to carry out this subsection—

(A) $10,000,000 for fiscal year 2003;

(B) $20,000,000 for fiscal year 2004;

(C) $20,000,000 for fiscal year 2005;

(D) $20,000,000 for fiscal year 2006; and

(E) $20,000,000 for fiscal year 2007.

(d) GRADUATE RESEARCH FELLOWSHIPS PROGRAM SUPPORT.—Computer and network security shall be included among the fields of specialization supported by the National Science Foundation's Graduate Research Fellowships program under section 10 of the National Science Foundation Act of 1950 (42 U.S.C. 1869).

(e) CYBER SECURITY FACULTY DEVELOPMENT TRAINEESHIP PROGRAM.—

(1) IN GENERAL.—The Director shall establish a program to award grants to institutions of higher education to establish traineeship programs to enable graduate students to pursue academic careers in cyber security upon completion of doctoral degrees.

(2) MERIT REVIEW; COMPETITION.—Grants shall be awarded under this section on a merit-reviewed competitive basis.

(3) APPLICATION.—Each institution of higher education desiring to receive a grant under this subsection shall submit

an application to the Director at such time, in such manner, and containing such information as the Director shall require.

(4) USE OF FUNDS.—Funds received by an institution of higher education under this paragraph shall—

(A) be made available to individuals on a merit-reviewed competitive basis and in accordance with the requirements established in paragraph (7);

(B) be in an amount that is sufficient to cover annual tuition and fees for doctoral study at an institution of higher education for the duration of the graduate traineeship, and shall include, in addition, an annual living stipend of $25,000; and

(C) be provided to individuals for a duration of no more than 5 years, the specific duration of each graduate traineeship to be determined by the institution of higher education, on a case-by-case basis.

(5) REPAYMENT.—Each graduate traineeship shall—

(A) subject to paragraph (5)(B), be subject to full repayment upon completion of the doctoral degree according to a repayment schedule established and administered by the institution of higher education;

(B) be forgiven at the rate of 20 percent of the total amount of the graduate traineeship assistance received under this section for each academic year that a recipient is employed as a full-time faculty member at an institution of higher education for a period not to exceed 5 years; and

(C) be monitored by the institution of higher education receiving a grant under this subsection to ensure compliance with this subsection.

(6) EXCEPTIONS.—The Director may provide for the partial or total waiver or suspension of any service obligation or payment by an individual under this section whenever compliance by the individual is impossible or would involve extreme hardship to the individual, or if enforcement of such obligation with respect to the individual would be unconscionable.

(7) ELIGIBILITY.—To be eligible to receive a graduate traineeship under this section, an individual shall—

(A) be a citizen, national, or lawfully admitted permanent resident alien of the United States; and

(B) demonstrate a commitment to a career in higher education.

(8) CONSIDERATION.—In making selections for graduate traineeships under this paragraph, an institution receiving a grant under this subsection shall consider, to the extent possible, a diverse pool of applicants whose interests are of an interdisciplinary nature, encompassing the social scientific as well as the technical dimensions of cyber security.

(9) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the National Science Foundation to carry out this paragraph $5,000,000 for each of fiscal years 2003 through 2007.

15 USC 7405.

SEC. 6. CONSULTATION.

In carrying out sections 4 and 5, the Director shall consult with other Federal agencies.

SEC. 7. FOSTERING RESEARCH AND EDUCATION IN COMPUTER AND NETWORK SECURITY.

Section 3(a) of the National Science Foundation Act of 1950 (42 U.S.C. 1862(a)) is amended—

(1) by striking "and" at the end of paragraph (6);

(2) by striking "Congress." in paragraph (7) and inserting "Congress ; and"; and

(3) by adding at the end the following:

"(8) to take a leading role in fostering and supporting research and education activities to improve the security of networked information systems.".

SEC. 8. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY PROGRAMS. 15 USC 7406.

(a) RESEARCH PROGRAM.—The National Institute of Standards and Technology Act (15 U.S.C. 271 et seq.) is amended—

(1) by moving section 22 to the end of the Act and redesignating it as section 32; and 15 USC 278h, 278q.

(2) by inserting after section 21 the following new section:

"SEC. 22. RESEARCH PROGRAM ON SECURITY OF COMPUTER SYSTEMS 15 USC 278h.

"(a) ESTABLISHMENT.—The Director shall establish a program of assistance to institutions of higher education that enter into partnerships with for-profit entities to support research to improve the security of computer systems. The partnerships may also include government laboratories and nonprofit research institutions. The program shall—

"(1) include multidisciplinary, long-term research;

"(2) include research directed toward addressing needs identified through the activities of the Computer System Security and Privacy Advisory Board under section 20(f); and

"(3) promote the development of a robust research community working at the leading edge of knowledge in subject areas relevant to the security of computer systems by providing support for graduate students, post-doctoral researchers, and senior researchers.

"(b) FELLOWSHIPS.—

"(1) POST-DOCTORAL RESEARCH FELLOWSHIPS.—The Director is authorized to establish a program to award post-doctoral research fellowships to individuals who are citizens, nationals, or lawfully admitted permanent resident aliens of the United States and are seeking research positions at institutions, including the Institute, engaged in research activities related to the security of computer systems, including the research areas described in section 4(a)(1) of the Cyber Security Research and Development Act.

"(2) SENIOR RESEARCH FELLOWSHIPS.—The Director is authorized to establish a program to award senior research fellowships to individuals seeking research positions at institutions, including the Institute, engaged in research activities related to the security of computer systems, including the research areas described in section 4(a)(1) of the Cyber Security Research and Development Act. Senior research fellowships shall be made available for established researchers at institutions of higher education who seek to change research fields and pursue studies related to the security of computer systems.

"(3) ELIGIBILITY.—

"(A) IN GENERAL.—To be eligible for an award under this subsection, an individual shall submit an application to the Director at such time, in such manner, and containing such information as the Director may require.

"(B) STIPENDS.—Under this subsection, the Director is authorized to provide stipends for post-doctoral research fellowships at the level of the Institute's Post Doctoral Research Fellowship Program and senior research fellowships at levels consistent with support for a faculty member in a sabbatical position.

"(c) AWARDS; APPLICATIONS.—

"(1) IN GENERAL.—The Director is authorized to award grants or cooperative agreements to institutions of higher education to carry out the program established under subsection (a). No funds made available under this section shall be made available directly to any for-profit partners.

"(2) ELIGIBILITY.—To be eligible for an award under this section, an institution of higher education shall submit an application to the Director at such time, in such manner, and containing such information as the Director may require. The application shall include, at a minimum, a description of—

"(A) the number of graduate students anticipated to participate in the research project and the level of support to be provided to each;

"(B) the number of post-doctoral research positions included under the research project and the level of support to be provided to each;

"(C) the number of individuals, if any, intending to change research fields and pursue studies related to the security of computer systems to be included under the research project and the level of support to be provided to each; and

"(D) how the for-profit entities, nonprofit research institutions, and any other partners will participate in developing and carrying out the research and education agenda of the partnership.

"(d) PROGRAM OPERATION.—

"(1) MANAGEMENT.—The program established under subsection (a) shall be managed by individuals who shall have both expertise in research related to the security of computer systems and knowledge of the vulnerabilities of existing computer systems. The Director shall designate such individuals as program managers.

"(2) MANAGERS MAY BE EMPLOYEES.—Program managers designated under paragraph (1) may be new or existing employees of the Institute or individuals on assignment at the Institute under the Intergovernmental Personnel Act of 1970, except that individuals on assignment at the Institute under the Intergovernmental Personnel Act of 1970 shall not directly manage such employees.

"(3) MANAGER RESPONSIBILITY.—Program managers designated under paragraph (1) shall be responsible for—

"(A) establishing and publicizing the broad research goals for the program;

"(B) soliciting applications for specific research projects to address the goals developed under subparagraph (A);

"(C) selecting research projects for support under the program from among applications submitted to the Institute, following consideration of—

"(i) the novelty and scientific and technical merit of the proposed projects;

"(ii) the demonstrated capabilities of the individual or individuals submitting the applications to successfully carry out the proposed research;

"(iii) the impact the proposed projects will have on increasing the number of computer security researchers;

"(iv) the nature of the participation by for-profit entities and the extent to which the proposed projects address the concerns of industry; and

"(v) other criteria determined by the Director, based on information specified for inclusion in applications under subsection (c); and

"(D) monitoring the progress of research projects supported under the program.

"(4) REPORTS.—The Director shall report to the Senate Committee on Commerce, Science, and Transportation and the House of Representatives Committee on Science annually on the use and responsibility of individuals on assignment at the Institute under the Intergovernmental Personnel Act of 1970 who are performing duties under subsection (d).

"(e) REVIEW OF PROGRAM.—

"(1) PERIODIC REVIEW.—The Director shall periodically review the portfolio of research awards monitored by each program manager designated in accordance with subsection (d). In conducting those reviews, the Director shall seek the advice of the Computer System Security and Privacy Advisory Board, established under section 21, on the appropriateness of the research goals and on the quality and utility of research projects managed by program managers in accordance with subsection (d).

"(2) COMPREHENSIVE 5-YEAR REVIEW.—The Director shall also contract with the National Research Council for a comprehensive review of the program established under subsection (a) during the 5th year of the program. Such review shall include an assessment of the scientific quality of the research conducted, the relevance of the research results obtained to the goals of the program established under subsection (d)(3)(A), and the progress of the program in promoting the development of a substantial academic research community working at the leading edge of knowledge in the field. The Director shall submit to Congress a report on the results of the review under this paragraph no later than 6 years after the initiation of the program.

Reports. Deadline.

"(f) DEFINITIONS.—In this section:

"(1) COMPUTER SYSTEM.—The term 'computer system' has the meaning given that term in section 20(d)(1).

"(2) INSTITUTION OF HIGHER EDUCATION.—The term 'institution of higher education' has the meaning given that term in section 101(a) of the Higher Education Act of 1965 (20 U.S.C. 1001(a)).".

(b) AMENDMENT OF COMPUTER SYSTEM DEFINITION.—Section 20(d)(1)(B)(i) of National Institute of Standards and Technology Act (15 U.S.C. 278g–3(d)(1)(B)(i)) is amended to read as follows:

"(i) computers and computer networks;".

(c) CHECKLISTS FOR GOVERNMENT SYSTEMS.—

(1) IN GENERAL.—The Director of the National Institute of Standards and Technology shall develop, and revise as necessary, a checklist setting forth settings and option selections that minimize the security risks associated with each computer hardware or software system that is, or is likely to become, widely used within the Federal Government.

(2) PRIORITIES FOR DEVELOPMENT; EXCLUDED SYSTEMS.—The Director of the National Institute of Standards and Technology may establish priorities for the development of checklists under this paragraph on the basis of the security risks associated with the use of the system, the number of agencies that use a particular system, the usefulness of the checklist to Federal agencies that are users or potential users of the system, or such other factors as the Director determines to be appropriate. The Director of the National Institute of Standards and Technology may exclude from the application of paragraph (1) any computer hardware or software system for which the Director of the National Institute of Standards and Technology determines that the development of a checklist is inappropriate because of the infrequency of use of the system, the obsolescence of the system, or the inutility or impracticability of developing a checklist for the system.

(3) DISSEMINATION OF CHECKLISTS.—The Director of the National Institute of Standards and Technology shall make any checklist developed under this paragraph for any computer hardware or software system available to each Federal agency that is a user or potential user of the system.

(4) AGENCY USE REQUIREMENTS.—The development of a checklist under paragraph (1) for a computer hardware or software system does not—

(A) require any Federal agency to select the specific settings or options recommended by the checklist for the system;

(B) establish conditions or prerequisites for Federal agency procurement or deployment of any such system;

(C) represent an endorsement of any such system by the Director of the National Institute of Standards and Technology; nor

(D) preclude any Federal agency from procuring or deploying other computer hardware or software systems for which no such checklist has been developed.

(d) FEDERAL AGENCY INFORMATION SECURITY PROGRAMS.—

(1) IN GENERAL.—In developing the agencywide information security program required by section 3534(b) of title 44, United States Code, an agency that deploys a computer hardware or software system for which the Director of the National Institute of Standards and Technology has developed a checklist under subsection (c) of this section—

(A) shall include in that program an explanation of how the agency has considered such checklist in deploying that system; and

(B) may treat the explanation as if it were a portion of the agency's annual performance plan properly classified under criteria established by an Executive Order (within the meaning of section 1115(d) of title 31, United States Code).

(2) LIMITATION.—Paragraph (1) does not apply to any computer hardware or software system for which the National Institute of Standards and Technology does not have responsibility under section 20(a)(3) of the National Institute of Standards and Technology Act (15 U.S.C.278g–3(a)(3)).

SEC. 9. COMPUTER SECURITY REVIEW, PUBLIC MEETINGS, AND INFORMATION.

Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) is amended by adding at the end the following new subsection:

"(e) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the Secretary $1,060,000 for fiscal year 2003 and $1,090,000 for fiscal year 2004 to enable the Computer System Security and Privacy Advisory Board, established by section 21, to identify emerging issues, including research needs, related to computer security, privacy, and cryptography and, as appropriate, to convene public meetings on those subjects, receive presentations, and publish reports, digests, and summaries for public distribution on those subjects.".

SEC. 10. INTRAMURAL SECURITY RESEARCH.

Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3), as amended by this Act, is further amended by redesignating subsection (e) as subsection (f), and by inserting after subsection (d) the following:

"(e) INTRAMURAL SECURITY RESEARCH.—As part of the research activities conducted in accordance with subsection (b)(4), the Institute shall—

"(1) conduct a research program to address emerging technologies associated with assembling a networked computer system from components while ensuring it maintains desired security properties;

"(2) carry out research associated with improving the security of real-time computing and communications systems for use in process control; and

"(3) carry out multidisciplinary, long-term, high-risk research on ways to improve the security of computer systems.".

SEC. 11. AUTHORIZATION OF APPROPRIATIONS. 15 USC 7407.

There are authorized to be appropriated to the Secretary of Commerce for the National Institute of Standards and Technology—

(1) for activities under section 22 of the National Institute of Standards and Technology Act, as added by section 8 of this Act—

(A) $25,000,000 for fiscal year 2003;
(B) $40,000,000 for fiscal year 2004;
(C) $55,000,000 for fiscal year 2005;
(D) $70,000,000 for fiscal year 2006;
(E) $85,000,000 for fiscal year 2007; and

(2) for activities under section 20(f) of the National Institute of Standards and Technology Act, as added by section 10 of this Act—

(A) $6,000,000 for fiscal year 2003;
(B) $6,200,000 for fiscal year 2004;
(C) $6,400,000 for fiscal year 2005;
(D) $6,600,000 for fiscal year 2006; and
(E) $6,800,000 for fiscal year 2007.

15 USC 7408.

SEC. 12. NATIONAL ACADEMY OF SCIENCES STUDY ON COMPUTER AND NETWORK SECURITY IN CRITICAL INFRASTRUCTURES.

Deadline.
Contracts.

(a) STUDY.—Not later than 3 months after the date of the enactment of this Act, the Director of the National Institute of Standards and Technology shall enter into an arrangement with the National Research Council of the National Academy of Sciences to conduct a study of the vulnerabilities of the Nation's network infrastructure and make recommendations for appropriate improvements. The National Research Council shall—

(1) review existing studies and associated data on the architectural, hardware, and software vulnerabilities and interdependencies in United States critical infrastructure networks;

(2) identify and assess gaps in technical capability for robust critical infrastructure network security and make recommendations for research priorities and resource requirements; and

(3) review any and all other essential elements of computer and network security, including security of industrial process controls, to be determined in the conduct of the study.

Deadline.

(b) REPORT.—The Director of the National Institute of Standards and Technology shall transmit a report containing the results of the study and recommendations required by subsection (a) to the Senate Committee on Commerce, Science, and Transportation and the House of Representatives Committee on Science not later than 21 months after the date of enactment of this Act.

(c) SECURITY.—The Director of the National Institute of Standards and Technology shall ensure that no information that is classified is included in any publicly released version of the report required by this section.

(d) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the Secretary of Commerce for the National Institute of Standards and Technology for the purposes of carrying out this section, $700,000.

15 USC 7409.

SEC. 13. COORDINATION OF FEDERAL CYBER SECURITY RESEARCH AND DEVELOPMENT

The Director of the National Science Foundation and the Director of the National Institute of Standards and Technology shall coordinate the research programs authorized by this Act or pursuant to amendments made by this Act. The Director of the Office of Science and Technology Policy shall work with the Director of the National Science Foundation and the Director of the National Institute of Standards and Technology to ensure that programs authorized by this Act or pursuant to amendments made by this Act are taken into account in any government-wide cyber security research effort.

SEC. 14. OFFICE OF SPACE COMMERCIALIZATION.

Section 8(a) of the Technology Administration Act of 1998 (15 U.S.C. 1511e(a)) is amended by inserting "the Technology Administration of" after "within".

SEC. 15. TECHNICAL CORRECTION OF NATIONAL CONSTRUCTION SAFETY TEAM ACT. 15 USC 7301.

Section 2(c)(1)(d) of the National Construction Safety Team Act is amended by striking "section 8;" and inserting "section 7;".

SEC. 16. GRANT ELIGIBILITY REQUIREMENTS AND COMPLIANCE WITH IMMIGRATION LAWS. 15 USC 7410.

(a) IMMIGRATION STATUS.—No grant or fellowship may be awarded under this Act, directly or indirectly, to any individual who is in violation of the terms of his or her status as a nonimmigrant under section 101(a)(15)(F), (M), or (J) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(15)(F), (M), or (J)).

(b) ALIENS FROM CERTAIN COUNTRIES.—No grant or fellowship may be awarded under this Act, directly or indirectly, to any alien from a country that is a state sponsor of international terrorism, as defined under section 306(b) of the Enhanced Border Security and VISA Entry Reform Act (8 U.S.C. 1735(b)), unless the Secretary of State determines, in consultation with the Attorney General and the heads of other appropriate agencies, that such alien does not pose a threat to the safety or national security of the United States.

(c) NON-COMPLYING INSTITUTIONS.—No grant or fellowship may be awarded under this Act, directly or indirectly, to any institution of higher education or non-profit institution (or consortia thereof) that has—

(1) materially failed to comply with the recordkeeping and reporting requirements to receive nonimmigrant students or exchange visitor program participants under section 101(a)(15)(F), (M), or (J) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(15)(F), (M), or (J)), or section 641 of the Illegal Immigration Reform and Responsibility Act of 1996 (8 U.S.C. 1372), as required by section 502 of the Enhanced Border Security and VISA Entry Reform Act (8 U.S.C. 1762); or

(2) been suspended or terminated pursuant to section 502(c) of the Enhanced Border Security and VISA Entry Reform Act (8 U.S.C 1762(c)).

SEC. 17. REPORT ON GRANT AND FELLOWSHIP PROGRAMS. 15 USC 7411.

Within 24 months after the date of enactment of this Act, the Director, in consultation with the Assistant to the President for National Security Affairs, shall submit to Congress a report reviewing this Act to ensure that the programs and fellowships are being awarded under this Act to individuals and institutions of higher education who are in compliance with the Immigration

and Nationality Act (8 U.S.C. 1101 et seq.) in order to protect our national security.

Approved November 27, 2002.

LEGISLATIVE HISTORY—H.R. 3394 (S. 2182):

HOUSE REPORTS: No. 107–355, Pt. 1 (Comm. on Science).
SENATE REPORTS: No. 107–239 accompanyinig S. 2182 (Comm. on Commerce, Science, and Transportation).
CONGRESSIONAL RECORD, Vol. 148 (2002):
Feb. 7, considered and passed House.
Oct. 16, considered and passed Senate, amended, in lieu of S. 2182.
Nov. 12, House concurred in Senate amendment.

○