AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

THE FUTURE OF COMPUTER SCIENCE RESEARCH IN THE U.S.

HEARING

BEFORE THE

COMMITTEE ON SCIENCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

MAY 12, 2005

Serial No. 109–14

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

20–999PS WASHINGTON : 2005

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*

RALPH M. HALL, Texas
LAMAR S. SMITH, Texas
CURT WELDON, Pennsylvania
DANA ROHRABACHER, California
KEN CALVERT, California
ROSCOE G. BARTLETT, Maryland
VERNON J. EHLERS, Michigan
GIL GUTKNECHT, Minnesota
FRANK D. LUCAS, Oklahoma
JUDY BIGGERT, Illinois
WAYNE T. GILCHREST, Maryland
W. TODD AKIN, Missouri
TIMOTHY V. JOHNSON, Illinois
J. RANDY FORBES, Virginia
JO BONNER, Alabama
TOM FEENEY, Florida
BOB INGLIS, South Carolina
DAVE G. REICHERT, Washington
MICHAEL E. SODREL, Indiana
JOHN J.H. "JOE" SCHWARZ, Michigan
MICHAEL T. MCCAUL, Texas
VACANCY
VACANCY

BART GORDON, Tennessee
JERRY F. COSTELLO, Illinois
EDDIE BERNICE JOHNSON, Texas
LYNN C. WOOLSEY, California
DARLENE HOOLEY, Oregon
MARK UDALL, Colorado
DAVID WU, Oregon
MICHAEL M. HONDA, California
BRAD MILLER, North Carolina
LINCOLN DAVIS, Tennessee
RUSS CARNAHAN, Missouri
DANIEL LIPINSKI, Illinois
SHEILA JACKSON LEE, Texas
BRAD SHERMAN, California
BRIAN BAIRD, Washington
JIM MATHESON, Utah
JIM COSTA, California
AL GREEN, Texas
CHARLIE MELANCON, Louisiana
VACANCY

CONTENTS

May 12, 2005

	Page
Witness List	2
Hearing Charter	3

Opening Statements

Statement by Representative Sherwood L. Boehlert, Chairman, Committee on Science, U.S. House of Representatives	18
Written Statement	19
Statement by Representative Lincoln Davis, Member, Committee on Science, U.S. House of Representatives	20
Written Statement	21
Prepared Statement by Representative Jerry F. Costello, Member, Committee on Science, U.S. House of Representatives	22
Prepared Statement by Representative Eddie Bernice Johnson, Member, Committee on Science, U.S. House of Representatives	23
Prepared Statement by Representative Russ Carnahan, Member, Committee on Science, U.S. House of Representatives	23
Prepared Statement by Representative Sheila Jackson Lee, Member, Committee on Science, U.S. House of Representatives	24

Witnesses:

Dr. John H. Marburger, III, Director, Office of Science and Technology Policy, The White Housest	
Oral Statement	25
Written Statement	27
Biography	31
Dr. Anthony J. Tether, Director, Defense Advanced Research Projects Agency	
Oral Statement	32
Written Statement	38
Biography	56
Dr. William A. Wulf, President, National Academy of Engineering	
Oral Statement	56
Written Statement	59
Biography	63
Financial Disclosure	65
Dr. F. Thomson Leighton, Chief Scientist and Co-founder, Akamai Technologies	
Oral Statement	67
Written Statement	68
Biography	76
Discussion	76

Appendix 1: Answers to Post-Hearing Questions

Dr. John H. Marburger, III, Director, Office of Science and Technology Policy, The White House	98
Dr. Anthony J. Tether, Director, Defense Advanced Research Projects Agency	103
Dr. William A. Wulf, President, National Academy of Engineering	106

Page

Dr. F. Thomson Leighton, Chief Scientist and Co-founder, Akamai Technologies 114

Appendix 2: Additional Material for the Record

Joint Statement of the Computing Research Community 120

THE FUTURE OF COMPUTER SCIENCE RESEARCH IN THE U.S.

THURSDAY, MAY 12, 2005

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

The Committee met, pursuant to call, at 10:10 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

The Future of Computer Science Research in the U.S.

Thursday, May 12, 2005
10:00 a.m. – 12:00 p.m.
2318 Rayburn House Office Building (WEBCAST)

Witness List

Dr. John H. Marburger III
Director, Office of Science and Technology Policy
The White House

Dr. Anthony J. Tether
Director
Defense Advanced Research Projects Agency

Dr. Wm. A. Wulf
President
National Academy of Engineering

Dr. Tom Leighton
Chief Scientist and Co-Founder
Akamai Technologies

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

The Future of Computer Science Research in the U.S.

THURSDAY, MAY 12, 2005
10:00 A.M.—12:00 P.M.
2318 RAYBURN HOUSE OFFICE BUILDING

1. Purpose

On Thursday, May 12, 2005, the House Science Committee will hold a hearing to examine the state of computer science research in the United States and the evolution of federal support for this field. Specifically, the hearing will examine the controversy surrounding the apparent shift away from basic research in overall federal support for computer science and the impact of the shift on federal agencies, academia and industry.

2. Witnesses

Dr. John H. Marburger, III is Director of the Office of Science and Technology Policy (OSTP), the White House science office. Prior to joining OSTP, Dr. Marburger served as President of the State University of New York at Stony Brook and as Director of the Brookhaven National Laboratory.

Dr. Anthony J. Tether is the Director of the Defense Advanced Research Projects Agency (DARPA). Prior to his appointment as Director of DARPA in 2001, Dr. Tether served as Chief Executive Officer of The Sequoia Group and of Dynamics Technology Inc.

Dr. William A. Wulf is President of the National Academy of Engineering. He is on leave from the University of Virginia, Charlottesville, where he is a University Professor and AT&T Professor of Engineering and Applied Sciences. His research focuses on computer architecture and computer security. He served as Assistant Director for Computer and Information Science and Engineering at the National Science Foundation from 1988 to 1990.

Dr. Tom Leighton is Chief Scientist and co-founder of Akamai Technologies. His expertise is in algorithms for network applications, which he used to develop a solution to freeing up Internet congestion. In addition to his position at Akamai, he is a Professor of Applied Mathematics at the Massachusetts Institute of Technology. He is currently a member of the President's Information Technology Advisory Committee (PITAC) and served as Chairman of the Committee's Subcommittee on Cyber Security.

3. Brief Overview

- Federal support for information technology research has been a key to the development of the information technology industry. The 2003 National Academy of Sciences report *Innovation in Information Technology* lists 19 areas in which federally sponsored fundamental research underpinned the innovations that eventually became multi-billion-dollar information technology industries. Examples include the Internet and the World Wide Web, parallel and relational databases, data mining, and speech recognition.
- Academic computer science research has direct relevance to the information technology industry. University research in computer science is funded by a number of agencies within the Federal Government, but the largest contributors are the Defense Advanced Research Projects Agency (DARPA) and the National Science Foundation (NSF), which together accounted for about 85 percent of the roughly $1.1 billion of federal funding for research performed at universities and colleges in mathematics and computer sciences in fiscal year 2004 (FY04).
- Recently, many computer science researchers have become concerned about an apparent trend at DARPA toward reducing the percentage of DARPA's

computer science research portfolio dedicated to long-term fundamental research. DARPA's withdrawal may have contributed to increased proposal pressures on NSF, which has experienced a doubling of applications for funding relating to computer science over the last four years, causing application approval rates to plummet.

- DARPA and NSF programs are complementary, but have many significant differences. While both agencies award grants competitively, DARPA has its program managers select the awardees, while NSF uses a peer-review process. Peer review allows a wider range of views to be considered, but also tends to be more conservative. DARPA awards also tend to be targeted to a more specific end-product even though that product may be many years away. The general view in the computer science field is that both agencies need to support fundamental research to allow for a balanced national portfolio. A sense of the relative strengths of the two agencies can be seen in the development of the Internet. DARPA-sponsored research led to the initial forerunner of the Internet, known as ARPANET. NSF funding led to the expansion of networks (initially for university use) and to the development of the World Wide Web.
- In March 2005, the President's Information Technology Advisory Committee (PITAC) released a report entitled *Cyber Security: A Crisis of Prioritization.* In it, the Committee describes the importance of federally supported research in cyber security and recommends additional federal investment at several agencies (including NSF and DARPA) to develop the next generation of cyber security technologies and increase the size of the cyber security research community. The PITAC report also recommends strengthening cyber security technology transfer efforts and improving interagency coordination of cyber security research programs.
- The Science Committee has been a leader in pushing for increased research in cyber security through, for example, passage in 2002 of the *Cyber Security Research and Development Act* (P.L. 107–305), which authorized $903 million over five years for cyber security research and fellowship programs at NSF and at the National Institute of Standards and Technology. In FY05, NSF cyber security programs are funded at about $82 million, $46 million below the level authorized in the Act.

4. Overarching Questions

- What effects are shifts in federal support for computer science—e.g., shifts in the balance between short- and long-term research, shifts in the roles of different agencies—having on academic and industrial computer science research and development? What impacts will these changes have on the future of the U.S. information technology industry and on innovation in this field?
- Are the Federal Government's current priorities related to computer science research appropriate? If not, how should they be changed?
- What should the Federal Government be doing to implement the recommendations of the recent President's Information Technology Advisory Committee (PITAC) report on cyber security?

5. Background

Federal Support for Information Technology Research

Many of the technologies that enabled electronic commerce to take off in the 1990s are based on research initially conducted at universities and funded by DARPA and NSF. The 2003 National Academy of Sciences (NAS) report *Innovation in Information Technology* lists 19 areas in which federally sponsored fundamental research underpinned the innovations that eventually became multi-billion dollar information technology industries.[1] Examples relating to e-commerce include web browsers, search engines, cryptography methods that allow secure credit card transactions, databases to manage information and transactions, and the protocols and hardware underlying the Internet itself. Often, the unanticipated results of such research are as important as the anticipated results. For example, the early research that led to e-mail and instant messaging technologies was originally done in the 1960s as part of a project examining how to share expensive computing resources among multiple simultaneous and interacting users.

[1] Computer Science and Telecommunications Board, National Academies, *Innovation in Information Technology,* National Academy Press (2003), pages 6–7.

These innovations have helped create an information technology sector that is credited for nearly 30 percent of real growth in the U.S. gross domestic product from 1994 to 2000 and that currently accounts for 29 percent of all U.S. exports.[2] The military also depends heavily on the information technology sector's commercial-off-the-shelf products to meet its critical information technology needs.

Since the pace of change in information technology products is so rapid, companies' main competitive advantage often comes from being first to market with a particular product or feature. If the U.S. research community isn't producing the ideas, or if the ideas are classified, it is less likely that U.S. companies will be the first to benefit from the research results.

Academic research also contributes to the training of the information technology workforce. Research grants support graduate students, and undergraduate and graduate computer science and engineering programs at universities produce the software developers and testers, hardware designers, and other personnel that power the computing and communications industries and the industries that depend on information technologies. (For example, automotive and manufacturing companies rely on modeling and simulation for product development and production management, and the financial services sectors utilize information technology for modeling markets and securing financial transactions.)

Agencies That Support Academic Computer Science Research

University research in computer science is funded by a number of agencies within the Federal Government but the largest contributors are DARPA and NSF, which together accounted for about 85 percent of the roughly $1.1 billion of federal funding for research performed at universities and colleges in mathematics and computer sciences in FY04. Other agencies that contribute in this area include the National Institutes of Health, the National Aeronautics and Space Administration, the Department of Energy, and the research agencies of the Armed Forces. Coordination among the agencies primarily occurs through working groups organized under the multi-agency National Information Technology Research and Development Program (NITRD), which operates under the auspices of the White House Office of Science and Technology Policy.

Defense Advanced Research Projects Agency

DARPA's mission is to ensure that the U.S. military remains, over the long-run, at the cutting edge of technology. DARPA conducts its mission by sponsoring revolutionary, high-payoff research that bridges the gap between fundamental discoveries and their military use. (The research it sponsors tends to be more revolutionary and more targeted than the research funded by NSF.) DARPA does not conduct any research itself; it sponsors research in academia and industry. DARPA's programs are organized around strategic thrusts in areas of importance to national security, and projects are sought out and selected by program managers. These program managers usually come to DARPA on leave from technical positions in the private sector, other government agencies, or academia and usually stay at DARPA for about four to six years. DARPA program managers are encouraged to pursue high-risk technical ideas and have the authority to quickly make decisions about starting, continuing, or stopping research projects.

DARPA played a key role in the birth and maturation of computer science as a field and the development of many of the important sub-specialties. As described by the NAS report, DARPA helped start many of today's university computer science programs by funding large-scale university centers of excellence early in the history of the computer science field.

DARPA supported research that produced advances in areas as diverse as computer graphics, artificial intelligence, networking, and computer architecture.[3] A recent Defense Science Board report also describes the unique role DARPA has played. DARPA program managers have encouraged simultaneous yet competing work by industrial and university researchers on the technological barriers to new computing capabilities and has also funded university researchers to produce convincing prototypes of revolutionary concepts.[4]

However, in the past five years, the computer science research community in both academia and industry has raised concerns that DARPA has been narrowing its focus. The community believes DARPA has been moving away from investing in

[2] Data from the Information Technology Industry Council, *http://www.itic.org/sections/Economy.html.*

[3] Computer Science and Telecommunications Board, National Academies, *Innovation in Information Technology,* National Academy Press (2003), pages 23–25.

[4] Report of the Defense Science Board Task Force on High Performance Microchip Supply, February 2005, page 87.

longer-term basic research in favor of increased funding for development of specific technologies for the armed forces' more immediate defensive and offensive needs. They believe that this change in focus is evident in a number of ways—a reduction of funding for university research in computer science, an increase in classification of research programs and restriction on participation of non-citizens, and reviews of whether to continue funding individual research projects at 12- to 18-month intervals, which is short for fundamental research.[5,6] These concerns recently received public airing in an article on the front page of the business section of the *New York Times* (Attachment A) and an editorial in *Science* magazine (Attachment B).

The way DARPA categorizes its research makes it difficult to get a complete picture of the trends in its computer science research. DARPA's budget requests, relevant appropriations language, and project portfolio management are organized in a constantly changing array of "program elements" rather than by field. However, in response to a Congressional request for historical data on DARPA funding for computer science and the amount of that funding given to universities, DARPA reviewed individual projects from the recent past to determine which could be classified as computer science research. The data was provided for FY01 through FY04 (Table 1) and showed that while overall computer science funding grew slightly (from $546 million in FY01 to $583 million in FY04), funding awarded to universities for computer science research declined each year in that period, going from $214 million in FY01 to $123 million in FY04 (a drop of 43 percent).

Table 1: DARPA funding for computer science research, overall and at universities (dollars in millions).

	FY01	FY02	FY03	FY04
Total DARPA Funding	1,884	2,260	2,655	2,815
Total DARPA Computer Science Funding	546	571	613	583
Amount of Computer Science Funding Awarded to Universities	214	207	173	123

Source: DARPA communication to Senate Armed Services Committee Staff
Note: Data was only provided for these four years.

Another source of information on the changing role of DARPA in supporting university computer science research is data gathered by the Computing Research Association. These data show that at leading university computer science departments, both the dollar amount of funding received from DARPA, and the percent of their funding from DARPA dropped sharply between FY99 and FY04. The percentage of their funding from DARPA in FY04 was roughly half of what it was in FY99.

DARPA has cited several factors that have contributed to this decline in its funding for university computer science research. First, much more DARPA computing research is classified, and universities generally do not perform classified research. The impact of increased classification has been particularly noticeable in the area of information assurance (also known as cyber security) for which the unclassified budget dropped by 50 percent between FY01 and FY04, leading to a drop in university funding from $20 million to $4 million. Second is the congressional termination[7] in FY04 of DARPA's program on asymmetric threats, which included approximately $11 million in university funding.

The third and perhaps most critical explanation for why DARPA's funding for university computer science research has declined is that work in many ongoing programs has progressed from the research phase to the product development and construction phase. For example, DARPA notes that work on high-performance computing has moved from research on how to design new computers to product development, leading funding to shift from universities to industry. Similarly, work in intelligent software has gone beyond the fundamental research stage, leading DARPA funding in that area for universities to decline from about $28 million in FY01 to

[5] "An Endless Frontier Postponed," by Edward D. Lazowska and David A. Patterson, *Science* Magazine, Volume 308, May 6, 2005, page 757.

[6] Report of the Defense Science Board Task Force on High Performance Microchip Supply, February 2005, page 88.

[7] DARPA's work on asymmetric threats was terminated as part of congressional elimination of DARPA's larger Terrorism Information Awareness program (also known as Total Information Awareness) in FY04 due to congressional concerns about the appropriateness of the overall program goals.

about $8 million in FY04. But computer scientists argue that, while work has progressed in these programs, there is basic research to be pursued in other, new areas.

Finally, DARPA may be feeling increasing pressure from the Department of Defense and the individual armed services to more quickly develop new technologies that can be deployed to meet current and near-term needs. DARPA has always played a critical role in the development of technologies for the armed forces. Examples of current DARPA programs with important short-term impacts include the Marine Airborne Retransmission System program, which helps extend the range of tactical radios and is expected to be deployed with the Marine Corps in Iraq very soon, and work on operating systems for unmanned combat air vehicles.

DARPA has always carried out a mix of nearer- and longer-term work and the question is whether the current balance is appropriate. Academic and some industry researchers fear that the balance is now shifting too much in the direction of nearer-term work, which will deprive the U.S. industry (and military) of ideas that could be helpful in the future. For example, research is needed on how to integrate nanotechnology and biotechnology with information technology systems.

National Science Foundation

Like DARPA, NSF performs no research itself. At NSF, projects are selected for funding through a competitive, peer review process, in which NSF brings together panels of experts in a given field to review proposals anonymously. Researchers can send project proposals to NSF either in response to agency-issued requests for proposals in specific areas or as unsolicited proposals.

Computer science research at NSF is conducted almost entirely in the Computer and Information Sciences and Engineering Directorate (CISE), although the directorate funding is not entirely devoted to computer science research. Relevant CISE activities include support for investigator-initiated research in all areas of computer and information science and engineering; development and maintenance of cutting-edge national computing and information infrastructure for research and education in many fields; and support for the education and training of the next generation of computer scientists and engineers.

In the five years between FY00 and FY04, the number of proposals received at CISE annually has more than doubled (Table 2). While funding has also increased, it has not kept pace with increasing proposal pressure and the rising costs of doing research. As a result, the success rate for proposals dropped to 16 percent, which is the lowest of any NSF directorate. During the same time period, the percentage of federal funding for research performed at universities and colleges in mathematics and computer sciences that was provided by NSF grew from 55 percent to 65 percent.[8]

Table 2: Proposal Pressure within the NSF Computer and Information Sciences and Engineering directorate

	FY00	FY01	FY02	FY03	FY04
NSF Total Funding ($ in millions)	$3948	$4454	$4789	$5308	$5652
CISE Total Funding ($ in millions)	$389	$478	$515	$589	$605
Number of Proposals to CISE	3,022	3,866	4,540	5,612	6,496
Number of Grants Awarded by CISE	931	923	1,093	1,231	1,064
CISE Success Rate	31%	24%	24%	22%	16%
Overall NSF Success Rate	33%	31%	30%	27%	24%

Note 1: Statistics are for "competitively reviewed" proposals and awards (i.e. proposal actions for research, education, and training grants processed through NSF's merit review system each year). Funding for second-year and later increments for continuing grants are not included.

Note 2: Over this same period, the average grant size in CISE increased from $153,840 in FY00 to $175,692 in FY04, and the number of senior personnel supported doubled, rising from 1,985 to 3,908.

Source: *Report to the National Science Board on the National Science Foundation's Merit Review Process: Fiscal Year 2004*, NSB-05-12, March 2005, pages 29 and 31.

A number of factors have contributed to this rise in proposal pressure and the drop in success rate. One is the growing number of computer science faculty looking to the Federal Government for research support. From the 1999–2000 academic year to the 2003–2004 academic year, the number of faculty in the top 24 U.S. computer

[8] *Federal Funds for Research and Development: Fiscal Years 2002, 2003, and 2004; Federal Funds for Research and Development: Fiscal Years 2001, 2002, and 2003;* and *Federal Funds for Research and Development: Fiscal Years 2000, 2001, and 2002.* All compiled by the NSF Division of Science Resources Statistics.

science departments increased by 27 percent (nearly 300 new faculty), and similar growth patterns were seen in the total number of faculty at all computer science departments.[9] Another factor is the growth of interest in the types of computer science-related programs funded by CISE. As researchers from other disciplines have discovered the value of information technology in tackling outstanding questions in their fields, scientists in physics, oceanography, biology, and many other areas have begun to seek funding from CISE. Finally, while the number of proposals was rising, CISE was also making a concerted effort to increase grant size in order to enhance researchers' productivity and improve opportunities for training students. While this strategy was consistent with recommendations made by PITAC and overall NSF goals, it also limited CISE's ability to increase the number of grants awarded.

Given the multitude of factors that have contributed to the increase in proposals submitted to CISE, it is difficult to determine how much of this change is due to researchers shifting their focus to NSF from DARPA because of the increasing difficulty of getting DARPA grants.

How DARPA and NSF Complement Each Other

Both DARPA and NSF have played a critical role in the development of computer science. NSF programs are generally driven by researchers' proposals and peer review while DARPA's investments are generally driven by the priorities set out by program managers who try to push the research envelope to meet particular military and national needs. NSF support is essential to the ongoing research and education work of a broad computer science community; DARPA work is essential to pulling that community into specific, newer areas. Both agencies have funded work that has led to technological leaps in information technology.

The Science Committee has been reviewing the relationship between the two agencies for some time. For example, on May 14, 2003, the Science Committee held a hearing to examine federal cyber security R&D activities. At the hearing, Dr. Tether, the Director of DARPA, in response to a question about whether the Federal Government was giving sufficient priority to the needs of cyber security, answered that DARPA is "more idea limited right now than we are funding limited," and indicated that DARPA relied on NSF to supply ideas. That appeared to be a shift away from DARPA's historic role, in which it funded fundamental research to foster new ideas as well as working to bring ideas to the development stage. Also many computer scientists expressed surprise at the DARPA comment, arguing that numerous ideas for research were going begging for money.

PITAC Report—Cyber Security: A Crisis of Prioritization

On March 18, 2005, the President's Information Technology Advisory Committee (PITAC) released their report *Cyber Security: A Crisis of Prioritization.* (The Executive Summary of the report is Attachment C.) In it, the Committee argues for increased federal funding for cyber security research and emphasizes the important and complementary roles multiple agencies play in ensuring that the next generation of cyber security technologies will be developed and implemented.

Specifically, the report presents four findings and recommendations. The first recommendation is that Congress and the Administration should substantially increase funding for fundamental research in civilian cyber security at a number of agencies, especially NSF, DARPA, and the Department of Homeland Security (DHS). In particular, the report recommends that funding for cyber security research at NSF be increased by $90 million annually.

The second recommendation from the Committee is that the Federal Government increase its support for recruitment and retention of cyber security researchers and students at research universities, with a goal of at least doubling the size of the civilian cyber security fundamental research community by the end of the decade. In particular, the report recommends increased, stable funding for research, recruitment of people from other fields into cyber security, and increased emphasis on the importance of unclassified cyber security research.

The third recommendation from the Committee is that, because current cyber security technology transfer efforts are not adequate to move the results of federal research investments into civilian sector best practices and products, the Federal Government should strengthen its cyber security technology transfer partnership with the private sector. Examples of what the Federal Government could do include: placing greater emphasis on the development of metrics, models, data sets, and testbeds so that new products and best practices could be evaluated; and encouraging feder-

[9] Annual Taulbee Surveys from the Computing Research Association. Available on line at *http://www.cra.org/statistics/*.

ally supported graduate students and postdoctoral researchers to gain experience in industry as researchers, interns, or consultants.

The final recommendation from the Committee is that the Federal Government should improve coordination and oversight of federal cyber security R&D to increase the focus and efficiency of the programs. Currently several interagency groups focus on, or include cyber security research in their missions, but there is not a single group with primary responsibility. The Committee recommends that the Interagency Working Group on Critical Information Infrastructure Protection become the focal point for coordinating federal cyber security R&D efforts. One task for a strengthened version of this working group would be to systematically collect data on federal cyber security R&D efforts.

6. Witness Questions

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

Questions for Dr. John Marburger:

- What are the Administration's highest priorities in computer science research? How and why have these priorities—and overall federal support for computer science research—changed in the last five years?
- What are the relative roles of the National Science Foundation and the Defense Advanced Research Projects Agency in supporting computer science research? How and why have these roles been changing?
- What is the Administration's response to the recent President's Information Technology Advisory Committee (PITAC) report on cyber security?

Questions for Dr. Anthony Tether:

- How does the Defense Advanced Research Projects Agency's (DARPA's) support for computer science research relate to its overall mission?
- What are DARPA's highest priorities in computer science research?
- How do you determine the balance between short- and long-term research programs? How does DARPA utilize academic and industrial researchers for computer science projects? Has the balance between short- and long-term research and between academic and industrial researchers within DARPA's computer science research portfolio changed in the last five years? If so, why?
- What is DARPA's response to the recent President's Information Technology Advisory Committee (PITAC) report on cyber security?

Questions for Dr. Wm. Wulf:

- What effects are shifts in federal support for computer science—e.g., shifts in the balance between short- and long-term research, shifts in the roles of different agencies—having on academic and industrial computer science research? What effects are changes in that research likely to have on the future of the U.S. information technology industry and on innovation in this field?
- Are the Federal Government's current priorities related to computer science research appropriate? If not, how should they be changed?
- What are your views on the recent President's Information Technology Advisory Committee (PITAC) report on cyber security? What should the Federal Government be doing to implement the recommendations of this report? Should PITAC be renewed when its current term expires on June 1?

Questions for Dr. Tom Leighton:

- Please explain the findings and recommendations of the recent President's Information Technology Advisory Committee (PITAC) report on *Cyber Security: A Crisis of Prioritization.*
- What role does cyber security research conducted at universities play in the development of cyber security tools and the implementation of good cyber security practices by U.S. companies?
- How have the composition and activities of the cyber security research community changed in recent years? How has federal support for cyber security research changed in recent years?

Attachment A

PENTAGON REDIRECTS ITS RESEARCH DOLLARS

NEW YORK TIMES, APRIL 2, 2005, PAGE C1

BY JOHN MARKOFF

SAN FRANCISCO, April 1—The Defense Advanced Research Projects Agency at the Pentagon—which has long underwritten open-ended "blue sky" research by the Nation's best computer scientists—is sharply cutting such spending at universities, researchers say, in favor of financing more classified work and narrowly defined projects that promise a more immediate payoff.

Hundreds of research projects supported by the agency, known as DARPA, have paid off handsomely in recent decades, leading not only to new weapons, but to commercial technologies from the personal computer to the Internet. The agency has devoted hundreds of millions of dollars to basic software research, too, including work that led to such recent advances as the Web search technologies that Google and others have introduced.

The shift away from basic research is alarming many leading computer scientists and electrical engineers, who warn that there will be long-term consequences for the Nation's economy. They are accusing the Pentagon of reining in an agency that has played a crucial role in fostering America's lead in computer and communications technologies.

"I'm worried and depressed," said David Patterson, a computer scientist at the University of California, Berkeley who is President of the Association of Computing Machinery, an industry and academic trade group. "I think there will be great technologies that won't be there down the road when we need them."

University researchers, usually reluctant to speak out, have started quietly challenging the agency's new approach. They assert that DARPA has shifted a lot more work in recent years to military contractors, adopted a focus on short-term projects while cutting support for basic research, classified formerly open projects as secret and placed new restrictions on sharing information.

This week, in responding to a query from the staff of the Senate Armed Services Committee, DARPA officials acknowledged for the first time a shift in focus. They revealed that within a relatively steady budget for computer science research that rose slightly from $546 million in 2001 to $583 million last year, the portion going to university researchers has fallen from $214 million to $123 million.

The agency cited a number of reasons for the decline: increased reliance on corporate research; a need for more classified projects since 9/11; Congress's decision to end controversial projects like Total Information Awareness because of privacy fears; and the shift of some basic research to advanced weapons systems development.

In Silicon Valley, executives are also starting to worry about the consequences of DARPA's stinting on basic research in computer science.

"This has been a phenomenal system for harnessing intellectual horsepower for the country," said David L. Tennenhouse, a former DARPA official who is now Director of Research for Intel. "We should be careful how we tinker with it."

University scientists assert that the changes go even further than what DARPA has disclosed. As financing has dipped, the remaining research grants come with yet more restrictions, they say, often tightly linked to specific "deliverables" that discourage exploration and serendipitous discoveries.

Many grants also limit the use of graduate students to those who hold American citizenship, a rule that hits hard in computer science, where many researchers are foreign.

The shift at DARPA has been noted not just by those researchers directly involved in computing technologies, but by those in other fields supported by the agency.

"I can see they are after deliverables, but the unfortunate thing is that basic research gets squeezed out in the process," said Wolfgang Porod, Director of the Center for Nano Science and Technology at the University of Notre Dame.

The concerns are highlighted in a report on the state of the Nation's cyber security that was released with little fanfare in March by the President's Information Technology Advisory Committee. DARPA has long focused on long-term basic research projects with time horizons that exceed five years, the report notes, but by last year, very little of DARPA's financing was being directed toward fundamental research in the field.

"Virtually every aspect of information technology upon which we rely today bears the stamp of federally sponsored university research," said Ed Lazowska, a computer scientist at the University of Washington and co-chairman of the advisory

panel. "The Federal Government is walking away from this role, killing the goose that laid the golden egg."

As a result of the new restrictions, a number of computer scientists said they had chosen not to work with DARPA any longer. Last year, the agency offered to support research by Leonard Kleinrock, a computer scientist at the University of California, Los Angeles who was one of the small group of researchers who developed the Arpanet, the 1960's predecessor to today's Internet.

Dr. Kleinrock said that he decided that he was not interested in the project when he learned that the agency was insisting that he employ only graduate assistants with American citizenship.

DARPA officials, who declined repeated requests for interviews, disputed the university researchers. The agency, which responded only in writing to questions, contended that the criticisms leveled by the advisory committee and other researchers were not accurate and that it had always supported a mix of longer- and shorter-term research.

"The key is a focus on high-risk, high-payoff research," Jan Walker, a DARPA spokeswoman, stated in an e-mail message. Given the threat from terrorism and the demands on troops in Iraq, she wrote, DARPA is rightly devoting more attention to "quick reaction" projects that draw on the fruits of earlier science and technology to produce useful prototypes as soon as possible.

The Pentagon shift has put added pressure on the other federal agencies that support basic information technology research.

At the Directorate for Computer and Information Science and Engineering of the National Science Foundation, the number of research proposals has soared from 2,000 in 1999 to 6,500 last year. Peter A. Freeman, its director, said that the sharp rise was partly attributable to declines in Pentagon support.

"DARPA has moved away from direct funding to universities," Mr. Freeman said. "Even when they do directly fund, some of the conditions and constraints seem to be pretty onerous. There is no question that the community doesn't like what the head of DARPA has been doing, but he has his reasons and his prerogatives."

The transformation of DARPA has been led by Anthony J. Tether, a Stanford-educated electrical engineer who has had a long career moving between executive positions at military contractors and the Pentagon.

Last year, Dr. Tether's new approach led to a series of cutbacks at a number of computer science departments. Program financing for a DARPA project known as Network Embedded Sensor Technology—intended to develop networks of sensors that could potentially be deployed on battlefields to locate and track enemy tanks and soldiers—has been cut back or ended on as many as five university campuses and shifted instead to traditional military contractors.

"The network has now become as vital as the weapons themselves," Dr. Tether said in an appearance before the advisory committee last year, testifying that secrecy had become more essential for a significant part of the agency's work.

That has created problems for university researchers. Several scientists have been instructed, for example, to remove previously published results from Web sites. And at U.C.L.A. and Berkeley, DARPA officials tried to classify software research done under a contract that specified that the results would be distributed under so-called open-source licensing terms.

"We were requested to remove all publicly accessible pointers to software developed under the program," said Deborah Estrin, Director of Embedded Network Sensing at U.C.L.A. "This is the first time in 15 years that I have no DARPA funding."

At Berkeley, Edward A. Lee, who was recently named Chairman of the Computer Science Department, agreed not to publish a final report at DARPA's request, even though he told officials the data had already become widely available.

Despite the complaints, some pioneering researchers support the changes being driven by Dr. Tether and say they are necessary to prepare the Nation for a long battle against elusive enemies.

"There are pressures and demands on DARPA to be relevant," said Robert Kahn, a former DARPA administrator who is now President of the Corporation for National Research Initiatives in Reston, Va. "People think it should stay the same, but times have changed."

Still, a number of top scientists argue that the Pentagon's shift in priorities could not have come at a worse time. Most American companies have largely ended basic research and have begun to outsource product research and development extensively even as investments in Asia and Europe are rising quickly.

And many computer scientists dispute DARPA's reasoning that fighting wars demands a shift away from basic research. During the Vietnam War, they say, DARPA kept its commitment to open-ended computer research, supporting things like a lab-

oratory in the hills behind Stanford University dedicated to the far-out idea of building computing machines to mimic human capabilities.

John McCarthy founded the Stanford artificial research lab in 1964, helping to turn it into a wellspring for some of Silicon Valley's most important companies, from Xerox Parc to Apple to Intel.

"American leadership in computer science and in applications has benefited more from the longer-term work," Mr. McCarthy said, "than from the deliverables."

Attachment B

EDITORIAL: AN ENDLESS FRONTIER POSTPONED

SCIENCE MAGAZINE, VOLUME 308, MAY 6, 2005, PAGE 757

BY EDWARD D. LAZOWSKA AND DAVID A. PATTERSON

Next month, U.S. scientists Vinton G. Cerf and Robert E. Kahn will receive computing's highest prize, the A.M. Turing Award, from the Association for Computing Machinery. Their Transmission Control Protocol (TCP), created in 1973, became the language of the Internet. Twenty years later, the Mosaic Web browser gave the Internet its public face. TCP and Mosaic illustrate the nature of computer science research, combining a quest for fundamental understanding with considerations of use. They also illustrate the essential role of government-sponsored university-based research in producing the ideas and people that drive innovation in information technology (IT).

Recent changes in the U.S. funding landscape have put this innovation pipeline at risk. The Defense Advanced Research Projects Agency (DARPA) funded TCP. The shock of the Soviet satellite Sputnik in 1957 led to the creation of the agency, which was charged with preventing future technological surprises. From its inception, DARPA funded long-term non-classified IT research in academia, even during several wars, to leverage all the best minds. Much of this research was dual-use, with the results ultimately advancing military systems and spurring the IT industry.

U.S. IT research grew largely under DARPA and the National Science Foundation (NSF). NSF relied on peer review, whereas DARPA bet on vision and reputation, complementary approaches that served the Nation well. Over the past four decades, the resulting research has laid the foundation for the modern microprocessor, the Internet, the graphical user interface, and single-user workstations. It has also launched new fields such as computational science. Virtually every aspect of IT that we rely on today bears the stamp of federally sponsored research. A 2003 National Academies study provided 19 examples where such work ultimately led to billion-dollar industries, an economic benefit that reaffirms science advisor Vannevar Bush's 1945 vision in *Science: The Endless Frontier.*

However, in the past three years, DARPA funding for IT research at universities has dropped by nearly half. Policy changes at the agency, including increased classification of research programs, increased restrictions on the participation of noncitizens, and "go/no-go" reviews applied to research at 12- to 18-month intervals, discourage participation by university researchers and signal a shift from pushing the leading edge to "bridging the gap" between fundamental research and deployable technologies. In essence, NSF is now relied on to support the long-term research needed to advance the IT field.

Other agencies have not stepped in. The Defense Science Board noted in a recent look at microchip research at the Department of Defense (DOD): "[DARPA's] withdrawal has created a vacuum. . .. The problem, for DOD, the IT industry, and the Nation as a whole, is that no effective leadership structure has been substituted." The Department of Homeland Security, according to a recent report from the President's Information Technology Advisory Committee, spends less than two percent of its Science and Technology budget on cyber security, and only a small fraction of that on research. NASA is downsizing computational science, and IT research budgets at the Department of Energy and the National Institutes of Health are slated for cuts in the president's fiscal year 2006 budget.

These changes, combined with the growth of the discipline, have placed a significant burden on NSF, which is now showing the strain. Last year, NSF supported 86 percent of federal obligations for fundamental research in IT at academic institutions. The funding rate for competitive awards in the IT sector fell to 16 percent, the lowest of any directorate. Such low success rates are harmful to the discipline and, ultimately, to the Nation.*

At a time when global competitors are gaining the capacity and commitment to challenge U.S. high-tech leadership, this changed landscape threatens to derail the extraordinarily productive interplay of academia, government, and industry in IT. Given the importance of IT in enabling the new economy and in opening new areas of scientific discovery, we simply cannot afford to cede leadership. Where will the next generation of ground-breaking innovations in IT arise? Where will the Turing Awardees 30 years hence reside? Given current trends, the answers to both questions will likely be, "not in the United States."

About the Authors: Edward D. Lazowska holds the Bill & Melinda Gates Chair in Computer Science & Engineering at the University of Washington. David A. Patterson holds the E.H. and M.E. Pardee Chair of Computer Science at the University

of California, Berkeley, and is president of the Association for Computing Machinery. Both are members of the National Academy of Engineering and the President's Information Technology Advisory Committee, and past chairs of the Computing Research Association.

*The House Science Committee will consider these issues at a 12 May hearing on "The Future of Computer Science Research in the U.S." See *http://www.cra.org/research.*

Attachment C

CYBER SECURITY: A CRISIS OF PRIORITIZATION

REPORT TO THE PRESIDENT FROM THE PRESIDENT'S INFORMATION TECHNOLOGY ADVISORY COMMITTEE

RELEASED MARCH 2005

EXECUTIVE SUMMARY

The information technology (IT) infrastructure of the United States, which is now vital for communication, commerce, and control of our physical infrastructure, is highly vulnerable to terrorist and criminal attacks. The private sector has an important role in securing the Nation's IT infrastructure by deploying sound security products and adopting good security practices. But the Federal Government also has a key role to play by supporting the discovery and development of cyber security technologies that underpin these products and practices. The PITAC finds that the Federal Government needs to fundamentally improve its approach to cyber security to fulfill its responsibilities in this regard.

Background

The Nation's IT infrastructure has undergone a dramatic transformation over the last decade. Explosive growth in the use of networks to connect various IT systems has made it relatively easy to obtain information, to communicate, and to control these systems across great distances. Because of the tremendous productivity gains and new capabilities enabled by these networked systems, they have been incorporated into a vast number of civilian applications, including education, commerce, science and engineering, and entertainment. They have also been incorporated into virtually every sector of the Nation's critical infrastructure—including communications, utilities, finance, transportation, law enforcement, and defense. Indeed, these sectors are now critically reliant on the underlying IT infrastructure.

At the same time, this revolution in connectivity has also increased the potential of those who would do harm, giving them the capability to do so from afar while armed with only a computer and the knowledge needed to identify and exploit vulnerabilities. Today, it is possible for a malicious agent to penetrate millions of computers around the world in a matter of minutes, exploiting those machines to attack the Nation's critical infrastructure, penetrate sensitive systems, or steal valuable data. The growth in the number of attacks matches the tremendous growth in connectivity, and dealing with these attacks now costs the Nation billions of dollars annually. Moreover, we are rapidly losing ground to those who do harm, as is indicated by the steadily mounting numbers of compromised networks and resulting financial losses.

Beyond economic repercussions, the risks to our nation's security are clear. In addition to the potential for attacks on critical targets within our borders, our national defense systems are at risk as well, because the military increasingly relies on ubiquitous communication and the networks that support it. The Global Information Grid (GIG), which is projected to cost as much as $100 billion and is intended to improve military communications by linking weapons, intelligence, and military personnel to each other, represents one such critical network. Since military networks interconnect with those in the civilian sector or use similar hardware or software, they are susceptible to any vulnerability in these other networks or technologies. Thus cyber security in the civilian and military sectors is intrinsically linked.

Although the large costs associated with cyber insecurity have only recently become manifest, the Nation's cyber security problems have been building for many years and will plague us for many years to come. They derive from a decades-long failure to develop the security protocols and practices needed to protect the Nation's IT infrastructure, and to adequately train and grow the numbers of experts needed to employ those mechanisms effectively. The short-term patches and fixes that are deployed today can be useful in response to isolated vulnerabilities, but they do not adequately address the core problems. Rather, fundamental, long-term research is required to develop entirely new approaches to cyber security. It is imperative that we take action before the situation worsens and the cost of inaction becomes even greater.

Summary of Findings and Recommendations

The PITAC's recommendations on cyber security, and the findings upon which those recommendations are based, are summarized below.

Issue 1: Federal Funding Levels for Fundamental Research in Civilian Cyber Security

Long-term, fundamental research in cyber security requires a significant investment by the Federal Government because market forces direct private sector investment away from research and toward the application of existing technologies to develop marketable products. However, federal funding for cyber security research has shifted from long-term, fundamental research toward shorter-term research and development, and from civilian research toward military and intelligence applications. Research in these domains is often classified and the results are thus unavailable for use in securing civilian IT infrastructure and commercial off-the-shelf (COTS) products in widespread use by both government and the civilian sector. These changes have been particularly dramatic at the Defense Advanced Research Projects Agency (DARPA) and the National Security Agency (NSA); other agencies, such as the National Science Foundation (NSF) and the Department of Homeland Security (DHS), have not stepped in to fill the gaps that have been created. As a result, investment in fundamental research in civilian cyber security is decreasing at the time when it is most desperately needed.

The PITAC finds that the Federal R&D budget provides inadequate funding for fundamental research in civilian cyber security, and recommends that the NSF budget in this area be increased by $90 million annually. Funding for fundamental research in civilian cyber security should also be substantially increased at other agencies, most notably DHS and DARPA. Funding should be allocated so that at least the ten specific areas listed in the "Cyber Security Research Priorities" section beginning on page 37 of Chapter 4 are appropriately addressed. Further increases in funding may be necessary depending on the Nation's future cyber security posture.

Issue 2: The Cyber Security Fundamental Research Community

Improving the Nation's cyber security posture requires highly trained people to develop, deploy, and incorporate new cyber security products and practices. The number of such highly trained people in the U.S. is too small given the magnitude of the challenge. At U.S. academic institutions today, the PITAC estimates, there are fewer than 250 active cyber security or cyber assurance specialists, many of whom lack either formal training or extensive professional experience in the field. In part, this situation exists because cyber security has historically been the focus of a small segment of the computer science and engineering research community. The situation has been exacerbated by the insufficient and unstable funding levels for long-term, civilian cyber security research, which universities depend upon to attract and retain faculty.

The PITAC finds that the Nation's cyber security research community is too small to adequately support the cyber security research and education programs necessary to protect the United States. The PITAC recommends that the Federal Government intensify its efforts to promote recruitment and retention of cyber security researchers and students at research universities, with a goal of at least doubling the size of the civilian cyber security fundamental research community by the end of the decade. In particular, the Federal Government should increase and stabilize funding for fundamental research in civilian cyber security, and should support programs that enable researchers to move into cyber security research from other fields.

Issue 3: Translating Research into Effective Cyber Security for the Nation

Technology transfer enables the results of federally supported R&D to be incorporated into products that are available for general use. There has been a long and successful history of federally funded IT R&D being transferred into products and best practices that are widely adopted in the private sector, in many cases spawning entirely new billion-dollar industries. Technology transfer has been particularly challenging in the area of cyber security, however, because the value of a good cyber security product to the consumer lies in the reduced incidence of successful attacks—a factor difficult to quantify in the short-term as a return on investment.

The PITAC finds that current cyber security technology transfer efforts are not adequate to successfully transition federal research investments into civilian sector best practices and products. As a result, the PITAC recommends that the Federal Government strengthen its cyber security technology transfer partnership with the private sector. Specifically, the Federal Government should place greater emphasis on the development of metrics, models, data sets, and testbeds so that new products and best practices can be evaluated; jointly sponsor with the private sector an annual interagency conference at which new cyber security R&D results are showcased; fund technology transfer efforts (in cooperation with industry) by researchers who have developed promising ideas or technologies; and encourage federally supported graduate students and postdoctoral researchers to gain experience in industry as researchers, interns, or consultants.

Issue 4: Coordination and Oversight for Federal Cyber Security R&D

One of the key problems with the Federal Government's current approach to cyber security is that the government-wide coordination of cyber security R&D is ineffective. Research agendas and programs are not systematically coordinated across agencies and, as a result, misconceptions among agencies regarding each others' programs and responsibilities have been allowed to develop, causing important priorities to be overlooked. In the absence of coordination, individual agencies focus on their individual missions and can lose sight of overarching national needs. Initiatives to strengthen and enlarge the cyber security research community and efforts to implement the results of R&D would be more effective and efficient with significantly stronger coordination across the Federal Government.

The PITAC finds that the overall federal cyber security R&D effort is currently unfocused and inefficient because of inadequate coordination and oversight. To remedy this situation, PITAC recommends that the Interagency Working Group on Critical Information Infrastructure Protection (CIIP) become the focal point for coordinating federal cyber security R&D efforts. This working group should be strengthened and integrated under the Networking and Information Technology Research and Development (NITRD) Program.

Chairman BOEHLERT. I want to welcome everyone here this morning to this extraordinarily important hearing. We are here to examine the state of federal computer science funding. That may sound like an arcane and even dreary subject, but what is at stake is nothing less than our nation's future prosperity and security.

That is not an exaggeration. Information technology advances are responsible for our productivity and economic health, and information technology undergirds and facilitates just about every personal and commercial activity we undertake these days. Information technology provides not just a web, it is the warp and woof of our society.

And it is too easy to take something that has become so basic and so omnipresent for granted. But we didn't get to where we are today by accident and indirection. We are the world leader in information technology, in part, because of strategic investments the Federal Government began making decades ago. And we will only remain the world leader if we continue to make the right investments.

Let me say parenthetically, I have just come from a press conference with Chairman Wolf, one of the cardinals on the Appropriations Committee, and Dr. Ehlers of our own committee, and John Engler, former Secretary and Governor and now head of NAM [National Association of Manufacturers], and a host of others to reveal to the world that we are planning a conference on innovation later this year, and there is $1 million in the appropriations bill that we just passed last week. And Chairman Wolf, as he opened up the conference, said that he just is amazed at the interest in the subject matter. And he pointed out that last year, he was invited to a conference on innovation and technology out in his district, and it was the night of the World Series, and he said that he didn't think there would be many people there, because of what was happening up in Boston. But to his surprise, there was an overflow crowd. Then he introduced me, and I said, "In your crowd, we are all Yankee fans." That is supposed to be funny. Everybody else laughed.

I think there is a broad consensus, at least in theory, about what the Federal Government needs to be doing. We need to continue to follow our recipe for success. That means we need a balanced portfolio that includes significant funding for long-term, fundamental computer science research, much of it at universities, the kind of research that has brought us the Internet and the World Wide Web.

And as this committee has said repeatedly, some of that long-term research needs to be focused on cyber security, because we are not going to protect our information technology in today's world through a hodgepodge of patches and existing know-how.

I don't think anyone disagrees with those statements. The question is whether current federal funding is in line with the theoretical consensus. And despite some rather defensive testimony we will hear today, one has to conclude that the answer to that question is "no."

Current federal funding is not properly balanced. It does not adequately continue our historic commitment to longer-range, more

basic research in computer science, and it does not focus sufficiently on cyber security.

We cannot have a situation where university researchers can point to sharp declines in DARPA funding, reviews of research results that reflect telescoped time horizons, and increased classification. We can not have a situation where the rates of proposal approvals at the National Science Foundation drop by half in just a few years. We can't have a situation where a Presidential Advisory Council declares that our information technology infrastructure is "highly vulnerable" and that there is "relatively little support for fundamental research to address the larger security vulnerabilities." That is not just us saying that. That is the Presidential Advisory Council. We can not have a situation where a Pentagon Advisory Board similarly expresses deep concern over the lack of long-term computing research.

This is not a matter of questioning the budget—the policy or budget of any single agency. This is a matter of having a critical, high-profile national need that is not being addressed by an overall coordinated federal policy or by overall federal spending.

I know we are operating in a time of major fiscal constraints. I know we have a war on. But I think Dr. Wulf makes an important point in his testimony when he notes that if we had similarly narrowed our focus during the Vietnam War, we probably wouldn't have the Internet or the other computing technology we take for granted today. And incidentally, the technology that was the leading reason for why we had such a successful '90s, year after year of record growth and profits, and the economy was stimulated and moving along and all based, essentially, on our investment in information technology.

So I hope we can have a robust and open discussion today about what specifically we can all do to ensure that we have a more balanced, better focused computer science portfolio that will, among other things, enhance funding of cyber security research. The status quo is simply unacceptable.

This committee has long been a leader in pushing the Federal Government to move ahead in computer science, whether that meant helping to create NSF's supercomputer centers or passing the *Cyber Security Research and Development Act.*

I know that all of our witnesses today care about these issues just as much as we do, and indeed spend far more of their time working on them. Together, we need to come up with a plan to get us back on a path that has brought us the information technology on which we have become utterly reliant.

Mr. Davis.

[The prepared statement of Chairman Boehlert follows:]

PREPARED STATEMENT OF CHAIRMAN SHERWOOD L. BOEHLERT

I want to welcome everyone here this morning to this extraordinarily important hearing. We're here to examine the state of federal computer science funding. That may sound like an arcane and even dreary subject, but what's at stake is nothing less than our nation's future prosperity and security.

That's not an exaggeration. Information technology advances are responsible for our productivity and economic health, and information technology undergirds and facilitates just about every personal and commercial activity we undertake these days. Information technology provides not just a web, it is the warp and woof of our society.

And it is too easy to take something that has become so basic and so omnipresent for granted. But we didn't get to where we are today by accident and indirection. We are the world leader in information technology, in part, because of strategic investments the Federal Government began making decades ago. And we will only remain the world leader if we continue to make the right investments.

In theory at least, I think there's a broad consensus about what the Federal Government needs to be doing. We need to continue to follow our recipe for success. That means we need a balanced portfolio that includes significant funding for long-term, fundamental computer science research, much of it at universities—the kind of research that has brought us the Internet and the World Wide Web.

And as this committee has said repeatedly, some of that long-term research needs to be focused on cyber security because we're not going to protect our information technology in today's world through a hodge-podge of patches and existing know-how.

I don't think anyone disagrees with those statements. The question is whether current federal funding is in line with the theoretical consensus. And despite some rather defensive testimony we'll hear today, one has to conclude that the answer is "no."

Current federal funding is not properly balanced. It does not adequately continue our historic commitment to longer-range, more basic research in computer science, and it does not focus sufficiently on cyber security.

We cannot have a situation where university researchers can point to sharp declines in DARPA funding, reviews of research results that reflect telescoped time horizons, and increased classification. We cannot have a situation where proposal approval rates at the National Science Foundation (NSF) drop by half in just a few years. We cannot have a situation where a Presidential advisory council declares that our information technology infrastructure is "highly vulnerable" and that there is "relatively little support for fundamental research to address the larger security vulnerabilities." We cannot have a situation where a Pentagon advisory board similarly expresses deep concern over the lack of long-term computing research.

This is not a matter of questioning the policy or budget of any single agency. This is a matter of having a critical, high-profile national need that is not being addressed by an overall, coordinated federal policy or by overall federal spending.

I know we are operating in a time of major fiscal constraints. I know we have a war on. But I think Dr. Wulf makes an important point in his testimony when he notes that if we had similarly narrowed our focus during the Vietnam War, we probably wouldn't have the Internet or the other computing technology we take for granted today.

So I hope we can have a robust and open discussion today about what specifically we can all do to ensure that we have a more balanced, better focused computer science portfolio that will, among other things, enhance funding of cyber security research. The status quo is simply unacceptable.

This committee has long been a leader in pushing the Federal Government to move ahead in computer science, whether that meant helping to create NSF's supercomputer centers or passing the *Cyber Security Research and Development Act.* I know that all our witnesses today care about these issues just as much as we do—and indeed spend far more of their time working on them.

Together, we need to come up with a plan to get us back on a path that has brought us the information technology on which we have become utterly reliant.

Mr. Davis.

Mr. DAVIS. Chairman Boehlert, thanks for calling the hearings today to review the state of computer science research in our country. It certainly is an important occasion and something that we have needed for some time, and I applaud you and your efforts in bringing together the panel that we have today that will be giving testimony.

This subject, certainly, is an important one. I would like to point at a chart that has appeared in several reports, and which Dr. Wulf includes in his testimony.

[Chart.]

This chart is from a 1995 National Academy of Sciences report on the value of the federal, multi-agency High Performance Computing and Communications programs, which this committee helped establish in 1991.

This chart traces the intertwined government and private sector research efforts that ultimately led to the development of the information technology industry, such as the Internet, graphic user interfaces, and relational databases. This chart reminds us that computer science research has resulted in substantial payoffs for our economy and our country.

Research investments require patience and long-term vision in order to gain these particular payoffs. The chart shows that it takes as much as 15 years or more for early research investments to bear fruits and turn into a billion-dollar commercial market.

Years ago, this Science Committee recognized the importance of sustained and coordinated federal support for research to advance these technologies. This Science Committee also recognized the importance of support for basic research in computer science that fuels these advances in technology.

Chairman Boehlert, I am pleased that this hearing has been called to inquire about the current state of the health for federal support for fundamental, long-term research in computer science. We have heard the concerns from the research community that agency roles in support of computing science research are changing and that these changes have led to declining funding for fundamental, university-based research.

The changes appear to be driven by DARPA's move toward more applied, results-driven research. We will have the opportunity to discuss this today with the DARPA Director, and I would like to welcome Dr. Tether to the hearing today. I look forward to your testimony, and for additional funding in the future.

Also today, we will look at cyber security research; research that keeps the Internet and our computers safe.

The President's Information Technology Advisory Committee has recently released a critique of cyber security research. This critique raises a number of concerns and makes several recommendations.

I am pleased to have Dr. Marburger here today to give the Administration's response to this report. I would also like to hear the Administration's views on the current priorities, agency roles, and funding support levels for basic computer science research.

As stated earlier, the subject of this hearing demands our attention because of the impact of information technology on the Nation, now and in the future.

We can't afford to squander our technological edge in a field that will only grow more in importance.

Mr. Chairman, I want to join you in welcoming our distinguished guests, and I certainly look forward with much anticipation to the discussion to follow.

[The prepared statement of Mr. Davis follows:]

PREPARED STATEMENT OF REPRESENTATIVE LINCOLN DAVIS

Mr. Chairman, thank you for calling this hearing to review the state of computer science research in the U.S.

This subject is an important one. I would like to point out a chart that has appeared in several reports, and which Dr. Wulf includes in his testimony. The chart is from a 1995 National Academy of Sciences report on the value of the federal, multi-agency High-Performance Computing and Communications program, which this committee helped establish in 1991.

This chart traces the intertwined government and private sector research efforts that ultimately led to the development of the information technology industry—such as the Internet, graphic user interfaces, and relational databases.

This chart reminds us that computer science research has resulted in substantial payoffs for our economy. Research investments require patience and long-term vision in order to gain these payoffs. The chart shows that it can take 15 years or more for early research investments to bear fruit and turn into a billion dollar commercial market.

Years ago, the Science Committee recognized the importance of sustained and coordinated federal support for research to advance these technologies. The Science Committee also recognized the importance of support for basic research in computer science that fuels these advances in technology.

Mr. Chairman, I am pleased that this hearing has been called to inquire about the current state of health for federal support for fundamental, long-term research in computer science.

We have heard concerns from the research community that agency roles in support of computer science research are changing, and that these changes have led to declining funding for fundamental, university-based research.

The changes appear to be driven by DARPA's move toward more "applied," results-driven research. We will have the opportunity to discuss this today with the DARPA Director, and I would like to welcome Dr. Tether to the hearing.

Also today, we will look at cyber security research. Research that keeps the Internet and our computers safe.

The President's Information Technology Advisory Committee has recently released a critique of cyber security research. That critique raises a number of concerns and makes several recommendations.

I am pleased to have Dr. Marburger here today to give the Administration's response to this report. I would also like to hear the Administration's views on the current priorities, agency roles, and funding support levels for basic computer science research.

As I said earlier, the subject of this hearing demands our attention because of the impact of information technology on the Nation, now and in the future.

We cannot afford to squander our technological edge in a field that will only grow in importance.

Mr. Chairman, I want to join you in welcoming our distinguished witnesses, and I look forward to our discussion.

Chairman BOEHLERT. Thank you very much, Mr. Davis.

[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 review the current state and future prospects for computer science research in the U.S., with a focus on federal agency roles and responsibilities. In addition, today's hearing will examine the findings and recommendations of the President's Information Technology Advisory Committee (PITAC) report on cyber security research.

Basic research in computer science has changed. As a result, opportunities for advancements in information technologies have been delayed, due to a drop in funding. I am concerned that the long-term impact of inadequate support for such research could harm the economy and have adverse consequences for national defense. Defense Advanced Research Projects Agency (DARPA) has been the lead sponsor of basic research in computer science to assess advances in information technology. Over the past few years, DARPA appears to have shifted its primary focus and objective. Between fiscal year 2001 and fiscal year 2004, DARPA support for university-based, non-classified research dropped by over 40 percent, from $214 million to $123 million. This had a significant impact on the university research community. Consequently, the National Science Foundation (NSF) was deferred to as the principal federal sponsor of basic research in computer science. Although NSF received a large increase in research funding requests, its success rate began to decline from 31 percent in 1999 to 16 percent in 2004. I am interested in learning what efforts are being made by the Administration to adjust and rebalance research support for non-classified, long-term computer science research as DARPA moves toward support for classified, near-term research.

Secondly, the Committee will review the findings and recommendations of the recent PITAC cyber security report. It is my understanding that the report finds a serious under-investment in cyber security research. The recommended funding in-

crease was for $90 million per year at NSF and significant increases for non-classified research at DARPA and DHS. Additionally, the report suggested that the focus on short-term, military classified, and academic research are below critical mass. Therefore, it is important to determine if increased funding for academic cyber security research would automatically increase the size and vitality of the research community.

I welcome the panel of witnesses and look forward to hearing their testimony today.

[The prepared statement of Ms. Johnson follows:]

PREPARED STATEMENT OF REPRESENTATIVE EDDIE BERNICE JOHNSON

Thank you Chairman Boehlert and Ranking Member Gordon for calling this very important hearing. I also wish to thank our expert witnesses for agreeing to testify today.

The purpose of the hearing is to review the current state and future prospects for computer science research in the U.S., with a focus on federal agency roles and responsibilities.

We all agree that a skilled workforce is the essential fuel to propel the economy and ensure a high quality of life. The success of our nation's economy depends on us producing a scientifically literate workforce.

Unfortunately, the budget submitted to us from the administration could possibly put us at risk of reversing all the wonderful computer science research programs that drove the our economy to the greatness we witnessed in the 1990's.

In the past, the Defense Advanced Research Projects Agency has poured billions of dollars into universities to pay for fundamental research of what would become the building blocks of computing, Internet and countless other high-tech endeavors.

But while DARPA spending on basic computer science research has risen from $546 million in fiscal 2001 to $583 million, the cut of it going toward to academic institutions has fallen from $214 million to $123 million during the same period.

Researchers say the shift already is affecting other research agencies such as the NSF, which has seen its own budget increases slow down in recent years.

DARPA's funding shift comes at a time when foreign governments are boosting their basic research efforts and as U.S. companies have cut back theirs. In fact, many U.S. companies partner with universities, which in part rely on government funding and which produce the scientists who eventually might create new companies or work in a corporate lab.

We cannot hope to educate tomorrow's employees and managers without more basic research into what works in the classroom. Our technology-based society is under constant change and additional research will help us master these changes.

That being said, I hope our witnesses can help us today by providing light on how we can maintain our status in the worldwide technology industry with our government support or lack there of computer science research.

[The prepared statement of Mr. Carnahan follows:]

PREPARED STATEMENT OF REPRESENTATIVE RUSS CARNAHAN

Mr. Chairman and Mr. Ranking Member, thank you for hosting this important hearing.

I represent the third district of Missouri, home to both Washington University of St. Louis and the University of Missouri at St. Louis. Both of these institutions are a great resource to our country, excelling in computer science research, and have received millions of dollars worth of funding through NSF's computer science awards. I am proud of the work being done within my congressional district and beyond.

NSF and DARPA house enormously important programs. In fact, they have been the driving force behind the Federal Government's role and our nation's role in the computer science field. If we wish to maintain our global role in this field we need to assess whether or not our priorities and allocated resources for NSF and DARPA are appropriate.

I welcome our witnesses to our committee today and look forward to hearing their testimony. Thank you.

[The prepared statement of Ms. Jackson Lee follows:]

PREPARED STATEMENT OF REPRESENTATIVE SHEILA JACKSON LEE

Chairman Boehlert, Ranking Member Gordon,

I want to thank you for organizing this important hearing to discuss the future of computer science research in the United States. Unfortunately, it seems we once again have to discuss a vital area in science that is receiving less federal funding than it needs. Computer Sciences must be made central to research at academic institutions for the long term well-being of our nation.

Mr. Chairman, I could understand that maybe thirty years ago we would not comprehend the need to fund computer science research. It's been a recent phenomenon in computer science when the home computer and the Internet came to change the face of our nation and indeed the world. It seems now that almost every child born learns to type on a keyboard and surf the web before they even learn how to ride a bicycle. Such is the new age we live in, computers are not only essential to our livelihoods, but in fact they have become completely ingrained in our day-to-day tasks. For example, it is not impossible now to buy a car that not only has a computerized system in it, but one that can give you pinpoint directions, play music beamed from a satellite and give you updated stock quotes and sports scores. The point is that maybe thirty years ago we could plead ignorance to the possibilities of computer science; perhaps it all seemed a bit far fetched. But the fact today is that we can not plead ignorance to the power of computer science and our dependence on this research is only going to grow larger not smaller as time goes on and I believe our nation would be at a great disadvantage to fall behind in this vital research.

I am troubled to learn that the Defense Advanced Research Projects Agency (DARPA) is now scaling back its computer science research from long-term, non-classified research to classified research to meet near-term defense requirements. Between FY 2001 and FY 2004, DARPA support for university-based, non-classified research dropped by over 40 percent, from $214 million to $123 million. Meanwhile, it seems the entire burden of computer science research is being put on NSF. In fact, last year NSF supported 86 percent of federal obligations for fundamental research in IT at academic institutions. At the same time that NSF has seen a large increase in research funding requests, it has also seen an accompanying decline in proposal success rate from 31 percent to 16 percent. For cyber security research proposals, the success rate for FY 2004 was a measly eight percent. The United States of America cannot stand for mediocrity in the critical area of computer science.

Computer science research is not only essential for our economic and technological development, but it is indeed essential for our national security. The amount of information that travels through the Internet and cyberspace on a daily basis is astounding. Because so much information travels through cyberspace it increases our vulnerability. As I said, our dependence on computers is only going to grow larger as time goes on; therefore we need to work now to close all the security gaps before our reliance on technology can be used against us. Less than two months ago, the President's Information Technology Advisory Committee (PITAC) released their report *Cyber Security: A Crisis of Prioritization.* Among the recommendations they made is that Congress and the Administration should substantially increase funding for fundamental research in civilian cyber security at a number of agencies, especially NSF, DARPA, and the Department of Homeland Security (DHS). In particular, the report recommends that funding for cyber security research at NSF be increased by $90 million annually. I have been in full support of these cyber security initiatives, both here in the Science Committee as well as in the Homeland Security Committee, where I am a Member. This kind of Homeland Security can not wait another day; any delay we take now will be a huge risk for our security in the future.

While I am unsatisfied by the status of computer science research being conducted on the federal level, I am also disturbed by the lack of female and minority representation in the field of computer science. The statistics show that women and minorities are not being proportionally represented in academia when it comes to computer science. In 2003, women represented barely over 20 percent of the computer science doctoral degrees granted. The same statistics show that in 2003 the White population made up about 70 percent of the doctoral degrees granted to U.S. citizens and permanent residents. At the same time, Asian/Pacific Islanders made up about 20 percent of the doctoral degrees granted, but Blacks, Hispanics and American Indian/Native Alaskans made up less than five percent of the doctoral degrees granted. These statistics are very discouraging and show that we are not reaching out to our entire population. Indeed, the problem starts in the classroom, where many under-privileged youth do not have nearly the same access to computers and the

Internet. If they don't have this background at an early age, its not surprising that they don't pursue the field in higher education and later in life.

We simply can not allow our nation to fall behind in computer science. We must utilize our entire population including women, minorities and the under-privileged. Our discoveries of the last few decades have changed the face of the world, but we must continue down this path if we are to prosper for the future.

Thank you.

Chairman BOEHLERT. And what a distinguished panel it is, all veterans, appearing before this committee. So you know how we work, we are not going to be arbitrary with the clock, but when you see the red light go on, if you would begin to summarize where you are, and then that will allow us more time for questions.

We have before us Dr. John H. Marburger, III, Director of the Office of Science and Technology Policy, The White House. Dr. Marburger, it is good to have you here. Dr. Anthony J. Tether, Director, Defense Advanced Research Projects Agency. Dr. Tether—and incidentally, you should know that within the past two weeks, I have had occasion on two separate—in two separate instances to speak with Secretary Rumsfeld and General Myers, and in both instances, I expressed to him my apprehensive and concern about the BRAC list tomorrow. The rumor mill suggests that there might be undue cuts in the laboratory complexes under DOD, and that would be very shortsighted indeed. I hope you guys share my concern about that. And hope the rumor mill is wrong. And invariably, it is wrong, but let us hope it springs eternal.

We have Dr. William Wulf, President, National Academy of Engineering who is so helpful as a resource to this committee. And Dr. Wulf, it is good to see you back.

And Dr. Tom Leighton, Chief Scientist and Co-founder of Akamai Technologies.

Gentlemen, it is a pleasure to have you here.

Dr. Marburger, you are first up.

STATEMENT OF DR. JOHN H. MARBURGER, III, DIRECTOR, OFFICE OF SCIENCE AND TECHNOLOGY POLICY, THE WHITE HOUSE

Dr. MARBURGER. Thank you very much, Mr. Chairman. I am pleased to have this opportunity to talk about federal support for computer science research in the United States, and I want to begin by saying that federally-sponsored R&D in networking and information technologies is an Administration priority. These technologies support advances in every area of science and engineering and generate further new capabilities that fuel our economy.

The Administration recognizes the importance of these fields and highlights the multi-agency Networking and Information Technology Research and Development Program, which I am going to refer to as NITRD in my oral testimony, as an R&D priority in the President's budget.

The 9/11 terrorist attacks and the war against terrorism have influenced our current thinking about these fields. Networking and information technology R&D investments for national defense, national security, and homeland security have received high priority in Administration actions. So this work is classified, for obvious reasons.

These new demands, however, have not affected our commitment to the central role of the NITRD program in filling the pipeline of skilled people and innovative ideas we need for national security, economic competitiveness, and scientific leadership in the future.

The 2006 budget proposal of $2.2 billion for the NITRD program raises the Administration's cumulative five-year investment in this activity over the $10 billion mark to $10.4 billion. Despite significant program redirections, the NITRD budget basically holds steady in the President's fiscal year 2006 budget.

This Administration supports breadth and diversity in the NITRD programs, which we view as an important strength. Especially at a time of budget constraints, NITRD's multi-agency collaborative approach strongly supports spending efficiency by leveraging each agency's expertise, minimizing duplicative efforts and enabling results that no single agency could achieve.

As this committee knows, we did act to address concern about one NITRD program area. My office chartered the High End Computing Revitalization Task Force in 2003 to provide a new vision for this increasingly important sector of information technology. The Task Force produced an excellent report, and the Administration strongly encourages this long-term revitalization effort.

The report defined a roadmap that identifies key research challenges in hardware, software, and systems technologies. Federal supercomputing capabilities clearly are critical to our national defense and national security missions as well as for leading-edge scientific research and more broadly for economic innovation and U.S. leadership in science and technology.

One of the first developments to emerge from the Task Force activity is a new multi-agency program, the High End Computing University Research Activity, supported by DARPA, DOE, NSA, and NSF that funds university-based R&D in high-end applications and system software. This program was launched quickly in fiscal year 2004, resulting in 34 grants with total funding of $27.3 million over three years.

Information security and assurance and the management of large data flows are two important priorities for this program and are further described in my written testimony. I won't say more about them here.

But regarding these priorities, in March 2004, my office asked the President's Information Technology Advisory Council to undertake an examination of the federal role in cyber security R&D and PITAC, which is the acronym for that council, responded with a useful report.

We began to respond to the report's findings and recommendations as soon as we heard about them; we did not wait until the report appeared. As soon as we were aware of some of their concerns, we did begin to act. We agree with PITAC that improved coordination of federal cyber security R&D activities can increase the efficiency and effectiveness of the government's investment in this area. My office is facilitating the report's recommendation to integrate the National Science and Technology Council's Interagency Working Group on Critical Information Infrastructure Protection R&D with the NITRD program.

And also before PITAC's final report was released, that program, Critical Information Infrastructure Protection, had begun the process of defining our top cyber security R&D needs and mapping these against current activities. We take very seriously the vulnerabilities in critical U.S. infrastructures pointed to by the report and continue to evaluate PITAC's recommendations regarding other steps that can be taken to enhance the effectiveness of federal efforts in cyber security.

For several years, the National Science Foundation, the agency with the broadest science portfolio, has been the lead agency in the NITRD program. My written testimony includes much more detail on their programs, but over the past five years, NSF's NITRD budget has risen nearly 25 percent, from $643 million in fiscal year 2002 to $803 million in fiscal year 2006.

Over the same period, DARPA's much smaller NITRD program budget has declined 33 percent from $263 million in 2002 to $176 million in 2006, reflecting their priority changes. Dr. Tether will provide more detail on these changes in his testimony, but I want to emphasize that computer science has developed very significantly since DARPA provided early stimulation to this field. And its current breadth justifies a new pattern of funding within DOD and among agencies in general.

In this connection, the President's fiscal year 2006 budget request tasks the National Coordination Office for NITRD and the NITRD agencies to commission a study by the National Academies that identifies important scientific questions and technical problems for which an extraordinary advancement in our understanding is difficult or impossible without leading-edge computing capabilities.

I want to thank the Committee for its attention to this important subject, and I will be happy to answer additional questions.

[The prepared statement of Dr. Marburger follows:]

PREPARED STATEMENT OF JOHN H. MARBURGER, III

Chairman Boehlert, Ranking Minority Member Gordon, and Members of the Committee. I am pleased to appear before you today to discuss the critical role of computer science research in the Federal Government's research and development (R&D) investment portfolio. As ever, I much appreciate the effective ongoing interactions between our office and your committee, which I believe ultimately benefit the Nation's science and technology enterprise.

Federal R&D in networking and information technologies has been and continues to be one of the Administration's highest R&D priorities. It is our view that these technologies provide a foundation for advances in virtually every other area of science and technology and generate myriad new capabilities and tools that grow our economy and make it more productive. Because of their unique role—as universal enablers for advanced science, engineering, and technology—networking and information technologies constitute a strategic component of the Nation's 21st century infrastructure. The Administration clearly recognizes that, and highlights this area as an R&D priority in the President's budget.

Before I address your specific questions, I would like to lay out what I believe is the broad context for our discussion. When I appeared before you in February to testify about the President's FY 2006 R&D budget, I acknowledged that it was subject to considerable pressure, making it the tightest proposal in nearly two decades. The President is committed to winning the war against terrorism, while moderating the growth in overall spending and cutting the deficit in half as a share of the GDP by 2009. These important goals obviously affect budget choices. So I was pleased to report to you that, despite these pressures, overall funding for Federal R&D increases to a record $132 billion in the President's FY 2006 budget—the highest level

of government support for R&D in the world and a 45 percent increase over FY 2001's total of $91 billion.

Let me also note here my belief that the overall health of U.S. science and technology today is strong. We are spending three times as much as Japan on R&D and half again as much as all the European nations combined. Our FY 2006 R&D budget is three-quarters of a billion dollars higher than our FY 2005 request.

This basically strong and stable environment for U.S. R&D does not obviate the need to assure that we are spending federal research dollars wisely and effectively. That entails planning to establish priorities and shifting funds in an orderly way toward the high-priority programs. Well-designed budgets will therefore inevitably have reductions as well as increases within large clusters of programs such as those in the R&D portfolio. These considerations are especially important during a time of significant fiscal constraints.

Now let me turn to your questions.

The first question asks about Administration priorities and how they have changed in the last five years. Clearly, the Administration's priorities in networking and information technology R&D were dramatically affected by 9/11 and the war against terrorism. Networking and information technology R&D investments for national defense, national security, and homeland security purposes received highest priority. Some of this work is classified for obvious reasons.

The 2006 budget proposal of $2.2 billion for the multi-agency Networking and Information Technology Research and Development (NITRD) Program—the Federal Government's primary vehicle for long-term, fundamental R&D in networking, computing systems, software, and related information technologies—puts the Administration's cumulative five-year investment in the NITRD activity over the $10-billion mark, to $10.4 billion. Despite significant program re-directions, the NITRD budget basically holds steady in the President's FY 2006 Budget.

As our NITRD budgets make clear, this Administration supports the breadth and diversity of the NITRD program's research interests. We view the scope of NITRD activities as one of the program's great strengths—encompassing work to advance high-performance computing and high-speed networking architectures for leading-edge research, to improve the quality and cost-effectiveness of software, to increase the security and reliability of computing and networking infrastructure, and to understand the implications of new technologies for education, workforce development, and social structures. Especially at a time of budget constraints, NITRD's multi-agency collaborative approach strongly supports spending efficiency, by leveraging each agency's expertise, minimizing duplicative efforts, and enabling results—such as prototype all-optical networks—that no single agency could achieve.

We consider all the NITRD activities to be of high priority, for precisely the reason that there is no other broad-based, fundamental IT R&D effort of the kind anywhere in this country. NITRD is a national resource.

We did, as you know, act to address concern about one NITRD domain. When my office chartered the High End Computing Revitalization Task Force (HECRTF) in 2003, it was in the recognition that the Federal R&D effort in high-end computing for vital federal missions was in need of a new vision and fresh approaches. The Task Force produced a first-rate report, which I was delighted to present to your committee on May 10, 2004. The Administration strongly encourages this long-term revitalization effort guided by a roadmap that points to the key research challenges in hardware, software, and systems technologies. Federal supercomputing capabilities clearly are critical for our national defense and national security missions, as well as for leading-edge scientific research, and more broadly for economic innovation and U.S. leadership in science and technology.

It is relevant to your inquiries that one of the first developments to emerge from the Task Force activity is a new multi-agency program, the High End Computing University Research Activity (HEC–URA) supported by the Defense Advanced Research Projects Agency (DARPA), the Department of Energy (DOE), the National Security Agency (NSA), and the National Science Foundation (NSF), that funds university-based R&D in high-end applications and system software. This program was launched quickly in FY 2004, resulting in 34 grants with total funding of $27.3 million over three years.

The high-end computing plan also extends access to the Nation's fastest, most powerful computing platforms to the national research community. The 2005 and 2006 budgets fund investments by the National Aeronautics and Space Administration (NASA) and the DOE Office of Science in advanced supercomputing systems whose management will include time allocations for outside researchers selected on a competitive basis. The concept of "national user facilities," being tested with these first two platforms, will itself have a galvanizing positive effect on the U.S. research community.

Another indication of the Administration's interest in the HEC area is that we have re-chartered NITRD's HEC Coordinating Group as an Interagency Working Group (IWG), calling for agency membership at a higher level of membership with increased agency commitment.

Two important priorities for NITRD are information security and assurance and the management of enormous data flows.

First, assuring the security, safety, and highly dependable performance of systems, networks, and software in critical applications and infrastructures is one of the most significant and difficult challenges in information technology R&D. The technical complexity of these systems continues to grow rapidly in two directions—ever-larger systems of systems involving thousands of processors and ever-smaller embedded systems and networks of embedded systems. NITRD agencies are doing critical work toward next-generation software, system, and network engineering that incorporates high assurance levels from the ground up, and even "self-healing" capabilities.

We currently rely on systems that are fragile, attackable, failure-prone, and often impossible to troubleshoot. The risks of such problems in safety- and life-critical applications are clear. This is an extremely valuable NITRD focus, carried out across several of its major research areas (Large Scale Networking, High Confidence Software and Systems, Human-Computer Interaction and Information Management, and Software Design and Productivity).

Second, advanced technologies are required for dealing with the overwhelming volume of information currently being generated. This NITRD research tackles the subjects of how technologies can help us capture and process information (such as multi-modal language translation and video, sound, and signal recognition), and how technologies can help us integrate and make sense of vast amounts of heterogeneous data in multiple formats (complex data sets). These capabilities are critical not only in military and national security environments but increasingly so in civilian applications such as health care, emergency response, education, and research across the spectrum including in the private sector.

To summarize, the Administration's overall R&D investments clearly have been affected by the Nation's move to a war footing after 9/11. Needs in the national defense, national security, and homeland security arenas have been immediate and great. However, these new demands have not affected our commitment to the central role of the NITRD Program in filling the pipeline of skilled people and innovative ideas we need for national security, economic competitiveness, and scientific leadership in the years to come.

The second question asked about the relative roles of NSF and DARPA and changes to these roles.

NSF has for several years been the lead agency in the NITRD Program. Over the last five years, NSF's NITRD budget has risen nearly 25 percent, from $643 million in FY 2002 to $803 million in FY 2006. Over the same period, DARPA's NITRD budget has declined 33 percent, from $263 million in FY 2002 to $176 million in FY 2006, reflecting priority changes. Dr. Tether will comment in his testimony on the specifics involved.

As the only federal research agency with a broad mission to advance both research and education across the physical and social sciences, mathematics, engineering, and technology, NSF plays a unique and invaluable role in the overall Federal R&D portfolio, and certainly in its NITRD activities. The National Science Foundation funds high-risk, long-term, basic research, and it is the only agency supporting that kind of R&D in all the core areas of the NITRD program. The agency identifies the most promising award candidates through a peer-based merit review process and makes awards to single investigators, teams, and center-scale projects. These grants permit investigators to explore promising new research opportunities as they arise, provide funding for projects exploring large-scale, experimental systems, and help educate future generations of computer scientists and provide workforce preparation for others.

In the national IT R&D community, NSF plays a powerful leadership role, constantly working to identify emerging research needs and innovative directions across the spectrum of networking and computing R&D and then developing programs to encourage fresh thinking among researchers and students at colleges and universities. The NSF leadership has compiled a remarkable track record of timely, successful initiatives to maintain leadership in information technology. Specific examples of initiatives follow:

The five-year Information Technology Research (ITR) program, whose concluding grants were awarded in FY 2004, was a foundation-wide initiative explicitly designed to promote multi-disciplinary research by expanding computer science R&D into new areas. The program's novel requirements—that proposing teams cross dis-

ciplinary boundaries and include computer scientists in proposals addressing multi-disciplinary problems—produced good results, not only for multi-disciplinary inquiry—an increasingly important aspect of research problem solving—but for integration of computer science applications into all NSF's science and engineering directorates.

A recent committee of visitors convened to review ITR found that the program enabled many "best-of-breed ideas" and resulted in significant community building across disciplines.

Beginning in FY 2004, NSF established a cross-cutting emphasis to encourage the study of the vulnerabilities of networked computing systems. Although this has been a longstanding concern of the NITRD agencies, NSF's Cyber Trust program crystallized the need for new approaches to cyber security, and also began addressing the national shortage of IT specialists with cyber security training. With the addition of the Cyber Trust program, funding for cyber security research at NSF has risen from $57 million in FY 2004 to $70 million in the President's 2006 budget. In FY 2005, NSF is also launching a new Science and Technology Center devoted to cyber security R&D, which I describe below.

NSF is also playing a key role in the NITRD high confidence software and systems work that I cited earlier. NSF's Science of Design theme is supporting development of a rigorous scientific base for greatly improved methods and tools for building software-intensive systems; this effort is funded at $10 million in 2005 and 2006. And in 2006, NSF plans to work with other NITRD agencies in a project to develop a prototype real-time embedded operating system.

In its five-year Network Middleware Initiative (NMI), NSF is spurring innovation in another core computer science area—the evolving layer of services that resides between the network and more traditional applications and enables networked computing systems to interact transparently with the network and other networked resources. Middleware is a critical component of scientific computing that NSF has stepped in to improve.

In 2006, NSF will begin a new $10-million program—Broadening Participation in Computing—to increase the number of domestic students receiving degrees in computer science.

It is clear that NSF is steadfastly and imaginatively pursuing its mission in information technology.

The third question concerned the Administration response to the President's Information Technology Advisory Committee (PITAC) report on cyber security.

In March 2004, my office asked PITAC to undertake an examination of the federal role in cyber security R&D so that we could better understand what steps are needed to advance the Administration's priority goals of strengthening national and homeland security. During PITAC's study, we asked for and received support from the Office of Management and Budget in identifying federal agencies' cyber security-related R&D investments, which remain very difficult to pinpoint because cyber security activities are not always clearly delineated or called out within broader programs, and, when they can be identified, it can still be difficult to estimate the extent to which the activities are related to IT and security and research.

OSTP much appreciates the PITAC's review of this extremely important topic. As I told PITAC members at their April 14 meeting, we began to respond to the report's findings and recommendations long before the published report appeared.

We agree with the PITAC that improved coordination of federal cyber security R&D activities is key to increasing the efficiency and effectiveness of the government's investments in this area. I am pleased to report that my office is facilitating one of the report's principal recommendations: integration of the National Science and Technology Council's (NSTC's) Interagency Working Group on Critical Information Infrastructure Protection (CIIP) R&D with the NITRD Program. Under the new structure, the CIIP IWG will have a broader charter integrating it with NITRD and providing for dual reporting to the NSTC's Subcommittees on Infrastructure and on Networking and Information Technology R&D. The results will be better coordination among researchers from diverse Federal IT security communities, higher visibility for this vital area of Federal R&D, and an improved capacity to gauge the progress we are making toward new security technologies for our computing and networking infrastructures.

Also, before PITAC's final report was released, the CIIP had begun the process of defining our top cyber security R&D needs and mapping those against current activities. This is crucial if we are to better address the critically important issue of defining priorities.

I wish to call your attention to a recent NSF announcement to establish in FY 2005 a new Science and Technology Center devoted to cyber security R&D. Led by the University of California, Berkeley, the multi-institutional collaborative effort

will investigate key issues of computer trustworthiness in an era of increasing attacks at all levels on computer systems and information-based technologies.

My office continues to evaluate PITAC's findings and recommendations regarding other specific steps that can be taken to enhance the effectiveness of federal efforts in cyber security. Certainly, the vulnerabilities in critical U.S. infrastructures pointed to by the report need to be taken very seriously.

The future of computer science R&D will be determined in part by our ability to demonstrate its significance convincingly over time. I believe we need better metrics of our R&D accomplishments and new models for analyzing funding for science and technology in general. Our current indicators are based on a data taxonomy that is decades old and does not really represent the way R&D is actually conducted today.

In the NITRD area, we are making a start at improving these measures. The President's FY 2006 Budget tasks the National Coordination Office for IT R&D and the NITRD agencies to commission a study by the National Academies that identifies and categorizes important scientific questions and technological problems for which an extraordinary advancement in our understanding is difficult or impossible without leading-edge computing capabilities.

Thank you for your attention to this important subject. I would be happy to answer additional questions.

BIOGRAPHY FOR JOHN H. MARBURGER, III

John H. Marburger, III, Science Adviser to the President and Director of the Office of Science and Technology Policy, was born on Staten Island, N.Y., grew up in Maryland near Washington D.C. and attended Princeton University (B.A., Physics 1962) and Stanford University (Ph.D., Applied Physics 1967). Before his appointment in the Executive Office of the President, he served as Director of Brookhaven National Laboratory from 1998, and as the third President of the State University of New York at Stony Brook (1980–1994). He came to Long Island in 1980 from the University of Southern California where he had been a Professor of Physics and Electrical Engineering, serving as Physics Department Chairman and Dean of the College of Letters, Arts and Sciences in the 1970's. In the fall of 1994 he returned to the faculty at Stony Brook, teaching and doing research in optical science as a University Professor. Three years later he became President of Brookhaven Science Associates, a partnership between the university and Battelle Memorial Institute that competed for and won the contract to operate Brookhaven National Laboratory.

While at the University of Southern California, Marburger contributed to the rapidly growing field of nonlinear optics, a subject created by the invention of the laser in 1960. He developed theory for various laser phenomena and was a co-founder of the University of Southern California's Center for Laser Studies. His teaching activities included "Frontiers of Electronics," a series of educational programs on CBS television.

Marburger's presidency at Stony Brook coincided with the opening and growth of University Hospital and the development of the biological sciences as a major strength of the university. During the 1980's federally sponsored scientific research at Stony Brook grew to exceed that of any other public university in the northeastern United States.

During his presidency, Marburger served on numerous boards and committees, including chairmanship of the Governor's Commission on the Shoreham Nuclear Power facility, and chairmanship of the 80 campus "Universities Research Association" which operates Fermi National Accelerator Laboratory near Chicago. He served as a trustee of Princeton University and many other organizations. He also chaired the highly successful 1991/92 Long Island United Way campaign.

As a public spirited scientist-administrator, Marburger has served local, State and Federal governments in a variety of capacities. He is credited with bringing an open, reasoned approach to contentious issues where science intersects with the needs and concerns of society. His strong leadership of Brookhaven National Laboratory following a series of environmental and management crises is widely acknowledged to have won back the confidence and support of the community while preserving the Laboratory's record of outstanding science.

Chairman BOEHLERT. Thank you very much, Dr. Marburger.

Dr. Tether.

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

Dr. TETHER. Mr. Chairman, Mr. Davis, Members of the Committee, first of all, I would like to say that we at DARPA support the strong funding of all disciplines and at all levels: undergraduate, high school, and graduate.

Now why do we do that?

Well, at DARPA, our role is really in the multi-disciplinary area. We are a projects agency, and we execute projects, which require multiple disciplines in order to be successful.

I would like to have you bear with me for a second, because I couldn't figure out how to really go through this without using pictures, and so I have slides. Yeah, we are from DARPA. We don't know how to talk without slides.

[Slide.]

So what I would like to do is spend a few moments, with your indulgence, explaining how DARPA operates. Now this is not just my impression of how DARPA operates. When I first came to DARPA, I met with the second DARPA Director, Austin "Cy" Betts, down at Southwest in Texas. Charles Herzfeld was the fourth Director. I have met with George Heilmeier, Bob Cooper, Craig Fields, Larry Lynn, Frank Fernandez, and Johnny Foster, who really wasn't a DARPA Director, but we all felt he was anyway. And I meet with these people constantly, and we go over what DARPA is doing, looking at it from the historical perspective and what we are doing now.

So what I am about to give you is something that if they all were here in this room, they would all agree, "Yes, this describes DARPA."

Next slide.

[Slide.]

Most of all, the DARPA organization is an organization that is very similar to the NSF in the following sense, not in the offices, because they are all program or problem-oriented rather than discipline-oriented, but in that the people are only there three to five years. And so we bring them in from industry, from universities, keep them three to five years, and they go back out to industry and universities. These are not detailees. These are people who had to give up a job to come to DARPA and then leave again. And that is the same thing that happens, quite frankly, at NSF.

Next slide.

[Slide.]

How do we fit? This is really the burning question.

I don't want you to get hung up too much on near, mid, and far. That is a notion of the time distance an idea is from becoming an acquisition program or a product. If you look at the service science and technology, it turns out to be on the near end. Now this is great science and technology. This is science and technology that makes radars more sensitive, jet engines more efficient and so forth and so on, but it is all about things we know about.

Then there are these people here on the far side. These are the people who will come to you and say, "Look, I can create a whole new capability by putting two systems together." The problem is, one system may be an Air Force system and the other may be an

Army system. And for that to get funded, this process is difficult, at best. Or these are the people who come to you and say, "Look, I can create whole new materials. I can move atoms around. I can create materials that we have never thought of before." Or, "I can make titanium be $1 a pound." For these people to get funded, they almost have to be like an electron and tunnel their way across.

DARPA was created by President Eisenhower in 1958 to bridge that gap.

Next slide.

[Slide.]

DARPA was created on the onset of Sputnik when President Eisenhower had his 9/11 Commission and the forensics said there was no reason why the Russians beat us into space. The problem was that the people over here didn't quite have high enough on their priority list the problem of getting a satellite in space, but there were plenty of people out here in the far side who said, "We could have done it. You just had to give us the money." And DARPA was created, not necessarily to create the far side, but to mine that far side worldwide to—no matter where the ideas were coming from, to be that agency which looked at these ideas, decided was it time, was it time to take them from the basic fundamental research to a product.

And that is what we have done, and we have done that extraordinarily well for nearly 50 years.

Now somebody in this room may be thinking, "Well, that was a great story, you know, but have you guys ever really done anything?"

Next slide.

[Slide.]

This is just an example of the things that DARPA has brought this country over the last 50 years by finding somebody on the far side, sometimes bringing that person into DARPA as a program manager, giving them a pot full of money with the express purpose of taking that idea or concept to the near side and get out. That is what we do, and we have done that from Saturn. President Kennedy would not have been as bullish when we said we are going to the Moon in 1969 if he didn't already know that the Saturn Rocket was there to have that possibility. That was DARPA's fifth project when it started.

Mundane things during the Vietnam War like the M–16 rifle was a DARPA program all of the way to Global Hawk, Predator. These are all DARPA programs that were brought to you by doing a multi-disciplinary approach to problems requiring these disciplines that have to be funded.

Next slide.

[Slide.]

By the way, here is the budget. This Administration has treated DARPA extraordinarily well. And Dr. Marburger will confirm that R&D has gone up over the last four years extraordinarily well, and they have treated us really well.

Next slide.

[Slide.]

Where is it going?

Well, in the Department of Defense, we have something called the QDR [Quadrennial Defense Review]. This is the QDR from 2001. We are redoing it again. We are going through that process again.

But next slide.

[Slide.]

This shows you where our money has gone. Leveraging information technology is dramatically increasing. Space has dramatically increased, and this category called "other" is where our 6.1 basic research budget is. DARPA has really a very small 6.1 budget, about $150 million, because we use that money to be able to go to the meetings to find those ideas to see if they are ready. In other words, we are not necessarily the agency that ever really has highly-funded basic research, but we are the agency that goes to take that basic research to the next stage.

Next slide.

[Slide.]

I have heard, reading it in the papers, that we are no longer doing "blue sky research," so I thought I would give you some examples.

Electronics. An atomic clock, I don't know if you have ever seen one, but it is big. We are taking that atomic clock and putting it on a chip. Now why are we interested in doing that? Most of our network systems today all need a common time sync, and they all use GPS. So if somebody jams GPS, we are out of business in the military. We can't afford that. So we are basically creating an atomic clock standard, which will be in your radio.

Diodes, laser diodes, 70 percent efficiency. This is a big deal for anybody who knows what it takes to make a high-powered laser where the problem is getting the heat out to make things small.

Next slide.

[Slide.]

Materials. Morphing aircraft. Titanium. We have a process we are working on right now where we believe we are going to get titanium down to less than $2 a pound. If we can do that, that will dramatically change the way we do business, not only in the United States but in the world if we can get titanium down to the cost of aluminum.

Next slide.

[Slide.]

Bio. We have learned how to, using the mind, control an arm.

Mr. ROHRABACHER. How much is titanium now?

Dr. TETHER. It is anywhere from $16 to $30 a pound.

We have learned how to use the thoughts of the mind to control an arm. We have a process right now where we are going to build a prosthetic that is controlled by the mind. Now this is a lot of technology in that arm. It is a real, true, multi-disciplinary approach. Materials, computer science, all of it is in that arm, but the enabling things, we found out how to basically take the thoughts of the mind and moving an arm and have that happen.

Last slide.

[Slide.]

Computer science. $584 million. You heard about the High Performance Computing Program, but if you really look at it, the only

one that is doing anything is the DARPA program that is really building a computer. And we will have a new high-productivity computer system that will give us, again, a competitive advantage in the world in about 2009 or 2010.

Computer science, in general. We are now focusing in computer science at what would be called cognitive processing, making a computer learn you as opposed to you having to learn the computer. Now why is that a big deal? First of all, for the Department of Defense, it is a big deal, because we can reduce people. Now when Bill Gates a couple years ago was out on the stump trying to gin up support for computer science and kids were asking him questions, and they said, "What's in it?" What is the next biggest thing that we could be in this business? He said that if we can show how to have a computer that learns, that will be worth more than 10 Microsofts. So here we are, developing in computer science an area which is important to the DOD. And if we can do it, it will be an economy that we haven't really heard of before. So we are actually in an area that is new. The people who were in computer science in the '90s have not followed that trend. Well, we are having people working in this program that are really the new people just coming out of schools.

Next slide.

[Slide.]

Okay. Upcoming key events. For those of you that really want to hear about DARPA, we have a symposium in August. It is in Anaheim. It is open to the world, foreigners. Why Anaheim? It is Disneyland. Where else would you have a DARPA conference, right?

Also, we have this thing called the Grand Challenge.

Next slide.

[Slide.]

What is that about?

It is a winner takes-all. The Congress gave us the ability to have prizes. An event that is going to occur on October 8, $2 million in cash. Winner takes-all for an autonomous vehicle to go a hundred or so miles and do it in less than 10 hours.

Next slide.

[Slide.]

What is involved?

Look at this, 195 teams from 36 states, three high schools, 35 universities. Why did we pick this one? Everybody owns a car. Everybody can buy a computer. You can go buy the sensors. The only thing left is you, your intellect. This is the ultimate in a multi-disciplinary approach, but the neat thing here is that we are exciting kids, people who would never work on the DOD problem are working on the DOD problem.

Who are we reaching?

Next slide.

[Slide.]

These kids, this is what it is all about. This is what I worry about constantly. Are we keeping the feed stock? I really worry about this more than I worry about "Is some professor being funded?" We have to make sure that kids really want to be interested in engineering in order to pursue that career.

Chairman BOEHLERT. Is that a question to the Chair? The answer is no.

Dr. TETHER. What? We are not interested?

Chairman BOEHLERT. We are not doing enough.

Dr. TETHER. We are not doing enough. And the Grand Challenge was really set up to really put excitement back into the United States, like it did back in the space race to the moon. And we have done that in a very micro way with this effort here.

Next slide.

[Slide.]

You know, I have heard, "My God, you are really concentrating on Iraq and therefore you are not doing research anymore." Yes, we are putting things in Iraq today, which are saving people's lives. This gun truck is a very simple thing made out of armor. Actually, we are finding out how it has saved people's lives. It is in Iraq now working. All I want to say is that the technology, the heavy lifting to have this over in Iraq was all paid for in the '90s. This is what DARPA typically does. We are way out ahead of the curve. When Iraq occurred and we started to put things into Iraq, we wanted to get what we had before and basically—the amount of money being used to get these in Iraq today is small compared to what it cost to develop in the '90s.

Next slide.

[Slide.]

All right. Let us get down to it.

What happened to university funding, especially computer science?

Next slide.

[Slide.]

Well, when I heard all of the fuss, I thought, "Well, maybe there is something going on." I knew that we at DARPA were not doing anything deliberate. I mean, it wasn't like we were throwing out proposals or refusing to fund people, but there was such a noise that I figured something must be going on.

So I went and gathered some data, and this is the data of selected universities. I left their names off for privacy reasons. This is one particular university that really has been on a downward trend since 1999. By the way, this black line is when I showed up. This blue line, these two dates here, these two costs should be averaged, because this is a program that was one particular contract that was funded late in the fiscal year. So if you look at these lines here, you find that from a university viewpoint, funding from DARPA has been either constant or actually going up a little bit. Now this is everything to universities.

Next slide.

[Slide.]

This is all in my testimony, but this is our average funds to university performers. This is just 2002 to 2004. This is your basic research column. This amount has actually doubled over the last five years. But notice that we at DARPA are funding universities to the tune of $450 million a year. I mean, this doesn't sound to me like an organization that is not friendly to universities. We are putting in 20 percent of our budget. On top of that, I said, "Well, they say we are making them go to industry;" in other words, instead of a

prime becoming a subcontractor. So I had our comptroller, who by now was nuts in trying to get me this data, go look at fiscal year 2003. And it is true, $75 million went to universities through subs. So you could add $75 million to that and say that DARPA funds universities about $525 million a year.

Now computer science. Well, this is from 1994, and it is in 2004 constant dollars. And it is a very interesting up and down. I really haven't figured out why we have these peaks and valleys, but they are really only spread over 10 or 15 percent. Look at the scale on the map. But in general, the funding at DARPA in computer science has been upward with its ups and downs, but it has been upward. (On the other hand, it is true that the funding to universities in this time period has shifted. However, we don't fund things by disciplines, so in order to figure out how much is funded to computer science, we have to almost go program by program, and we have about 500 of them. And again, my comptroller, who by now is ready to quit, went and calculated those numbers.)

But this is—doesn't sound like a place that is anti-university and most certainly not a place that is anti-computer science. But the issue is the university funding.

Next slide.

[Slide.]

Well, where did the money go? I mean, I was as curious as all of you. So I went to the websites of the universities. My God. They aren't funding disciplines anymore. Every website at every university you go to is multi-disciplinary something or another. They are building multi-disciplinary buildings for bio info. And what is happening, that I can tell, is that the universities have discovered that multi-disciplinary efforts are the wave of the future. We agree. We absolutely agree, because that is the approach we have had over 50 years. The problems have changed, the thrusts have changed over 50 years, but our approach always has been a multi-disciplinary approach.

Finally, we believe that individual disciplines need to be funded. Healthy funding of individual disciplines is required to assure that we can do multi-disciplinary work. We can't have a case where we are going to fund a multi-disciplinary team and somebody says, "Well, the physics guy is not available. Well, go get the zoologist." You really need to have the disciplines to do that.

One vehicle is block funding as a vehicle. I am treading on dangerous political grounds with that statement, but all disciplines, however, not just computer science, in order to make sure they are healthy, you might want to say we are going to fund them specifically.

But DOD is doing its part. I want you to understand that we at DOD understand this problem, and we are worried about it. We are really worried about it, not from a single discipline viewpoint. We are worried about it from the feed stock of where the kids are coming into high school going into universities to keep that going. So we are doing our part. We have the National Defense Graduate Fellowship, the SMART program, which Congress established in 2005. We have two interns coming to DARPA. We have Multi-disciplinary University Research Initiatives, or MURIs. And we have something called a Focus Research Center in both microelectronics

and nanotechnology, and we are talking about opening up one in cognitive.

Next slide.

[Slide.]

This is what a focus center program is. It is a joint program between industry and the government. We put $10 million in. Industry puts $10 million in. That $20 million goes to these universities. It is run by universities to work on a rather focused problem. It is where we get our far side to figure out what to do next, and in fact, from this, we have had our microelectronics program basically generating what we want. We are going to open up one in nanotechnology, and quite frankly, we are going to try to open up one in computer science, also in cognitive. I am going to approach Microsoft to see if they would like to join up with us, because I do believe, as Microsoft believes, that the computer science of today and the future is not the computer science of the '90s, but is in a new area called cognitive.

Next slide.

[Slide.]

Thank you very much for your time.

[The prepared statement of Dr. Tether follows:]

PREPARED STATEMENT OF ANTHONY J. TETHER

Mr. Chairman, Members, and staff. I am Tony Tether, the Director of the Defense Advanced Research Projects Agency (DARPA). I am pleased to be here today to talk about research at DARPA.

DARPA Funding for "Blue Sky" Research

Last month, an article appeared in the *New York Times* (April 2, 2005), "Pentagon Redirects Its Research Dollars." The general message in the article is that DARPA has decided to shift away from basic research in favor of financing more classified work and narrowly defined projects that promise a more immediate payoff.

That simply is not correct.

There has been no decision to divert resources, as the article implies. DARPA's commitment to seek new ideas, to include ideas that support research by bringing together new communities of research scientists, is the same as it has been, dating back to the Agency's inception in 1958. You can see from my biography that I was at DARPA nearly 25 years ago, so I speak from years of personal experience.

Rather than go through a blow-by-blow rebuttal of the article, I am providing the Committee with my answers to specific questions from the *Times* reporter (Appendix A) and my response to a question from the Senate Armed Services Committee staff (Appendix B) which was used in the article. I urge you to read this information in order to better assess the claims made in the *New York Times* article itself, which is included in Appendix C for your convenience.

A mistaken impression that readers may get from the *New York Times* article is that DARPA is carelessly eliminating universities from research funding by requiring increased security classification. The case cited by the article is DARPA's Network Embedded Systems Technology (NEST) program. NEST is developing technology for networks of small, low-power sensor nodes that can operate under extreme resource constraints of power, timing, memory, communication, and computation, while simultaneously being highly scalable and robust.

As you will see from Appendix A, NEST started in 2001 and was originally planned to end this fiscal year. DARPA extended the program for one year to focus on military applications of the technology. Contrary to the article, NEST funding to universities for research actually *increased* during the life of the program. From fiscal year FY 2001 through FY 2005, NEST program funding for university research increased from the original plan of $18.8 million to $26.1 million—an increase of $7.3 million, or nearly 40 percent.

In addition, the article implies that DARPA is moving away from long-range "blue sky" research. Let me assure you that also is not the case. Appendix D is a list of representative DARPA research programs that show DARPA is, indeed, funding radical ideas that involve long-range research.

When I first heard about the university funding concerns several months ago, I decided to investigate the claim. One of the first things I did was to determine whether a trend existed in DARPA's university funding over the past several years.

Figure 1, entitled "DARPA funding at selected universities, FY 1999 to FY 2004," shows the results from that investigation. For privacy reasons, I have not identified the universities, but I will provide the Committee the information on request.

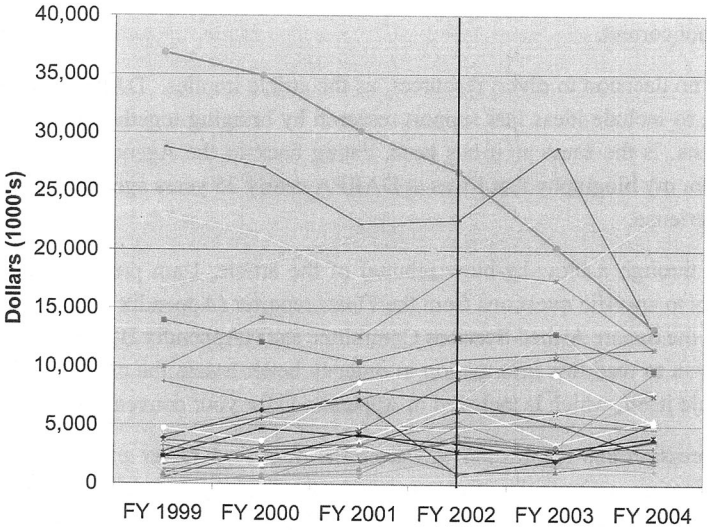


Figure 1: DARPA funding at selected universities, FY 1999 to FY 2004.

The graph shows that funding at individual universities varies over time; from year to year, funding typically goes up and down at any given school. However, with one notable exception,[1] funding varies around a roughly constant level.[2]

The black vertical line in Figure 1 marks the period when I returned to DARPA as Director. Analyzing the data, I could not find any correlation between funding levels and trends since my return to the Agency. Even the university with the large decrease was on this path long before I became Director.

Figures 1 leads to an interesting observation.

The major complaint about reduced university funding seems to be coming from one discipline—computer science. But if DARPA's overall funding of universities is more or less constant, then other disciplines must be the recipients of DARPA's research funding.

The key question becomes, "What other discipline has grown significantly over the past five years at the expense of computer science?"

As part of my investigation, I reviewed several dozen university websites to see if I could determine the new discipline that was on the rise.

The answer is surprising on the one hand and obvious on the other: no *single* discipline has been taking over.

Every university website I visited advertised that they had created centers for multi-disciplinary research and professed that these centers were the harbinger of the future. What must be happening is that, while computer science is always part of the multi-disciplinary efforts, its past dominance and, hence, respective share must be decreasing in relationship to the other disciplines involved in the effort.

---

[1] After I saw the dramatic decrease in the university plotted as the red line, I contacted the president of the university. We are trying to figure out what is going on, and we plan to meet in June.

[2] The peculiar funding profile for the university plotted as the purple line, with a dramatic increase in FY 2003 followed by a sharp decrease in FY 2004, is the result of the timing of one contract; the funding for those two years should be averaged.

In this same vein, last month Dr. Arden Bement, Director of the National Science Foundation, remarked that, "Evolving in concert with the new [scientific] tools are different ways of working within science, such as collaboration across large, multi-disciplinary, often international teams. These new modes of working are essential to meeting the grand scientific challenges of our era—those overarching goals that require a concerted, large-scale effort."[3]

Multi-disciplinary research is the foundation for creating the innovations of the future.

I agree.

In fact, DARPA has been leading that trend for almost 50 years. And we are continuing that tradition.

Let me give you some examples:

Material Science: In the early 1960s, universities had departments in metallurgy, chemistry, physics, mining, and engineering, but there was no "material science" discipline to solve the burgeoning problems of space vehicles, ballistic missile nose cones, and hypervelocity impact.

We needed advanced materials like plastics, composites, thermoelectrics, semiconductors, ceramic windows for high power microwave devices, lightweight armor, and other materials for space applications. All this required multi-disciplinary laboratories to provide the science, technology, and the cadre of "material scientists" to develop the materials the Nation would need for its Defense technologies. DARPA funded the formation and growth of the Interdisciplinary Materials Laboratories through the 1960s. By 1989, there were about 100 materials science departments in U.S. universities—much of this stemming from DARPA's funding of multi-disciplinary university activities.

Computer Science: In the 1960s, there was no "computer science" discipline *per se.* DARPA funded electrical engineering and mathematics ideas, along with ideas from other areas, combined them, and began to focus on the problems and opportunities of human-machine interface and networks. This effort led to the personal computer and the Internet. Today, the multi-disciplinary outcome is what we call "computer science." A recent survey of 335,000 computer science publications[4] shows that DARPA is second only to the National Science Foundation in funding this multi-disciplinary group of researchers.

More recently, DARPA's High Performance Computing Systems (HPCS) program is aimed at filling the gap between today's late-80s high performance computing technology and the quantum/bio-computing systems of the future. HPCS involves new materials, new microelectronics architectures, and revolutionary software engineering-it is a quintessential multi-disciplinary computer program.

Stealth: In the 1970s, DARPA wanted to make an aircraft invisible to radar. To achieve stealthy aircraft such as today's F–117 and B2, DARPA assembled research teams in radar absorbent materials, infrared shielding, heat dissipation, reduced visual signature technology, low-probability-of-intercept radar, active signature cancellation, inlet shielding, exhaust cooling and shaping, and windshield coatings. Physicists, aeronautical engineers, material scientists, and electrical, thermal and structural engineers were brought together to solve the problem. To achieve this, DARPA did not post specific requirements for academic disciplines to be gathered to solve stealth. Instead, we focused on the problem of how to build an airplane not only according to the Navier-Stokes equation, but also according to Maxwell's equations, and then brought together the necessary disciplines to solve the tough technical challenges.

Analog, Optical, and Radio Frequency Electronics: In the 1980s and 1990s, DARPA pioneered advances in digital silicon microelectronics and analog gallium arsenide microwave circuits critical to military information superiority. Since 2000, DARPA has opened a new range of capabilities by leading the development of Integrated Microsystems-complete "platforms on a chip" with the ability to sense, process, and act on data. DARPA programs have driven combinations of electronics, photonics, microelectromechanical systems (MEMS), algorithms, and architectures to give the DOD an unparalleled ability to sense, process, and act on data.

Bio:Info:Micro: A few years ago, we saw opportunity in the convergence of biology, information technology, and microsystems. That led to our current work to combine neuroscience, biology, computers, actuators, sensors, and power systems in a multi-disciplinary program to revolutionize prosthetics. Our goal is to dramatically im-

---

[3] Dr. Arden L. Bement, Jr., "The Shifting Plate Tectonics of Science," American Ceramic Society, Frontiers of Science and Society Rustum Roy Lecture, Baltimore, MD, April 10, 2005

[4] Giles, L. and Councill, I., "Who gets acknowledged: Measuring scientific contributions through automatic acknowledgement indexing," *Proceedings of the National Academy of Sciences* 101, 51 (2004)

prove the quality of life for amputees and allow them to return to a normal life with no limits whatsoever by developing limb prostheses that are fully functional, neurologically controlled limb replacements that have normal sensory abilities.

As I mentioned earlier, Appendix D shows a sample of more than 75 DARPA programs we're working on today. If you look over that list, you can't help but see the tremendous amount of multi-disciplinary work being done to solve Defense technology problems.

Developing completely new multi-disciplinary research is at the heart of many DARPA success stories that are reported often in the press.

DARPA's focus on national security problems and opportunities naturally leads to multi-disciplinary research because most problems or opportunities do not come neatly packaged in disciplines.

We do not emphasize advancing progress in established disciplines. Instead, we bring together teams from diverse institutions and disciplines to solve a particular problem.

This does lead to significant changes in the disciplines and institutions that are involved with DARPA at any given time, but it also results in a great deal of progress.

It is also highly likely that the funding varies considerably for specific established academic disciplines—but these funding variations, like in computer science, are hard to track since DARPA does not specifically fund disciplines, as explained earlier.

Thus, our funding of people, disciplines, universities, and institutions increases and decreases as a result of the constantly changing mix of problems that DARPA is working to solve. The mix does change, but the overall effort is robust.

This change, while occasionally discomforting, is very healthy. It is exactly how problems are solved and ensures DARPA remains open to entirely new ideas. Many, perhaps most, of our solutions are multi-disciplinary and, as you saw above, we even occasionally foster entirely new disciplines this way.

More often than not, revolutionary technological progress—which is distinct from scientific progress—is not a product of continuing, secure funding of established disciplines. Crucial steady progress is made within disciplines, but many would agree that truly major technical revolutions often occur outside or in between disciplines. Real technology breakthroughs come from the multi-disciplinary problem-solving approach that DARPA has been relying on for decades.

DARPA's focus is to agilely pursue national security problems and opportunities.

Funding for the Future

As I think about the issues this committee is dealing with, I have an observation to make.

First, the major complaints about decreased funding seem to be coming from one specific discipline—computer science.

The complaints, I also note, never clearly identify the specific research that is not being done, the problems that are not being solved, or the progress that is impeded as a result of decreased funding in the discipline. The message of the complaints seems to be that the computer science community did good work in the past and, therefore, is entitled to be funded at the levels to which it has become accustomed.

I want to strongly emphasize that I do believe individual research disciplines are important. They provide the scientific foundation for multi-disciplinary research, and they need to be funded at healthy levels to keep the pipeline full and allow for multi-disciplinary work to occur.

However, it may be appropriate to have funding for specific established disciplines such as computer science, and this committee may reach that decision. However once such funding is started, it would be reasonable to expect that other disciplines such as chemistry, physics, and math would expect similar consideration.

But rigidly funding specific, established disciplines would severely limit the flexibility DARPA needs to be successful. DARPA needs the ability to promote multi-disciplinary work to solve important national security problems, to include forming completely new disciplines.

We at DARPA are always interested in hearing about good ideas that we can accelerate into use for our national security no matter where they come from. This is inherently multi-disciplinary work, just as the universities are emphasizing, and we believe it is to the great benefit of our military and nation.

Appendix A

Q and A's Asked by New York Times Reporter Regarding University Interactions with DARPA

1. Is it true that there has been a shift in DARPA funding away from universities during the past two to three years? How significant has the shift been?

A: The claim that DARPA funding has shifted away from universities is incorrect.

However, University funding requires an understanding of how the DOD budgets. There are several Budget Activities ranging from 6.1 to 6.7. Science and Technology (S&T) funding is defined as the 6.1 through 6.3 Budget Activities.

The 6.1 Budget Activity is termed Basic Research and is defined as systematic study directed toward greater knowledge or understanding of the fundamental aspects of phenomena and of observable facts without specific applications in mind. The activity in this account is almost always unclassified and ITAR (International Traffic in Arms Regulations, i.e., export control) restrictions do not apply since specific applications are not in mind. Hence these funds are ideally suited to the operations of universities.

The 6.2 Budget Activity is termed Applied Research and is defined as systematic study to understand the means to meet a recognized and specific need. The activity in this account tends to require classification and/or be subject to ITAR restrictions far more often than 6.1 research. Hence, not all the programs under this account are suitable for universities, or even possible for universities that refuse to do classified research. However universities do submit proposals for programs funded from this account, and receive the largest absolute value of their funding from DARPA from this account. That said, as programs in this account progress, they may require classification and/or have ITAR restrictions, meaning that normal university operating practices make participation in the program less desirable and feasible.

The 6.3 Budget Activity is termed Advanced Technology Development and includes development of subsystems and components and efforts to integrate them into system prototypes for field experiments and/or tests in a simulated environment. This type of work is rarely a good fit with universities. Universities do propose to efforts in this account but the efforts are typically incidental, specific investigations and do not last the duration of the effort.

There has NOT been a shift away from universities. The DARPA 6.1 Basic Research account has increased since 1999 both in absolute terms and as a percentage of the DARPA budget. And, since 1999, the percentage of that 6.1 funding going to universities has also increased.

DARPA 6.1 funding has averaged 8.7 percent of DOD's total 6.1 investment over the last 10 years. DARPA's share of the total 6.1 funding increased noticeably over the past several years. Our 6.1 program was 13.4 percent of the DOD 6.1 program in 2004 and 11.2 percent of the 6.1 total in FY 2005—well above the 10-year average.

Within DARPA's budget, the percentage devoted to 6.1 averaged approximately 4.4 percent over the past 10 years. In this area too, the percentage has been on the rise over this timeframe, and the 6.1 percentage has increased to 5.8 percent of the overall DARPA budget.

In absolute terms, the 6.1 budget has more than tripled, from $54.9 million in FY 1999 to $169.9 million in FY 2005.

The percentage of the DARPA university 6.1 budget in FY 1996–2000 was 52 percent, while the FY 2001–2004 percentage was 59 percent (where FY 2004 stands today). This is in line with the findings of the National Academy of Sciences' *Assessment of Department of Defense Basic Research* study published in 2005 that 60 percent of DOD's overall 6.1 program went to universities.

2. What is the reason for the shift? What are the DARPA priorities and have they changed significantly?

A: The only shift since 1999 in our basic research has been towards MORE funding and MORE funding at universities.

DARPA currently has eight strategic thrusts (see list below) chosen based on a strategic assessment of national security threats and technological opportunities facing the U.S.:

- Detection, precision identification, tracking, and destruction of elusive targets
- Location and characterization of underground structures

- Networked manned and unmanned systems
- Robust, secure self-forming tactical networks
- Cognitive computing
- Assured use of space
- Bio-revolution
- Urban area operations

In addition to these eight strategic thrusts, DARPA's research also emphasizes core technology areas that are independent of current strategic circumstances, but important to future technical opportunities and successes.

These core technology foundations are the investments in fundamentally new technologies, particularly at the component level, that historically have been the technological feedstock enabling quantum leaps in U.S. military capabilities. Core investment areas include: materials, microsystems, information technology and other technologies and sciences, including in recent years biology and mathematics.

Many of DARPA's university performers are funded to develop breakthroughs in the core technology investment areas. However, many universities are also funded to achieve technological breakthroughs in the eight strategic thrust areas.

Details on these thrusts are provided in the DARPA document "Bridging the Gap" which can be downloaded from our website *www.darpa.mil.*

3. Does DARPA publicly break out the university component of its funding?

A: Yes, the following provides average funding for the past three fiscal years:

FY02 to FY04	Avg. $ univ. performers*	Avg. overall DARPA $	Univ. percentage
6.1 Basic Research	$90.1M	$150.3M	60%
6.2 Applied Research	$270.4M	$1,128M	24%
6.3 Adv Tech Devel	$92.3M	$1,076.3M	8.6%
Total	$452.8M	$2,354.3M	19.2%

*This is funding that goes directly to a university and does not count the funding that goes to universities through subcontracts to industry.

Universities receive a significant percentage of dollars from DARPA. In fact, the table shows that universities receive nearly four times more of their dollars from DARPA's 6.2 and 6.3 accounts, even though the research funded in these accounts is less suited to universities' operational practices.

4. A number of university researchers have told me that the DARPA Network Embedded Systems Technology (NEST) research has largely been removed from universities and classified. Is that true? Is that because there is an operational need for the technology?

A: Yes, there is an operational need for the technology and this is a specific case where the original 6.2 effort was successful to the point that further efforts became classified.

DARPA's NEST program started in 2001, and was scheduled to end in FY05 (this year). DARPA is extending the program for an additional year to focus on military applications of the technology. In order to protect the U.S. advantage in this technology, it is necessary to classify and protect aspects of the technology.

Previous NEST university performer work is all unclassified, and university researchers can publish information on their concept, findings, algorithms, and other basic research academic material. Under the terms of their NEST contracts, university researchers provide their source code to the Government as a deliverable. DoD does plan to protect the source code and military applications of the technology appropriately.

DARPA expects to involve the defense contractor community in the next phase of the NEST program. It is also expected that many of the university researchers will become subcontractors to the defense contractors.

In addition, all of the current NEST university efforts are continuing. Some individual university NEST activities were reduced, but other university NEST activities were increased. Overall, there was increased funding for universities in NEST over what was originally planned.

5. There was a specific effort to remove the NEST Tiny OS research at the University of California at Berkeley. Do you know why DARPA attempted to classify that re-

search? Is it true that there was a prior contract that stipulated that the research results would be available as open source?

A: TinyOS research is not classified. In fact, all basic level fundamental research in sensor network systems is unclassified. The DARPA NEST program is funding University of California at Berkeley to continue their research work through FY05. However, DOD does plan to protect the source code and military applications of the technology by taking the deliverable software from all such researchers to further develop it with other defense contractors.

6. Was research being done by Jack Stankovic at the University of Virginia on sensor networks classified?

A: All university research on the NEST program, including that of Professor Stankovic, was unclassified. University researchers, including Professor Stankovic, will continue to be funded for unclassified basic research in FY 2005 as well. In addition, the program plans to support classified work to be done by defense contractors.

7. A November 2004 report by the President's Information Technology Advisory Committee states that DARPA has departed from its historical support of longer-term research. Is this accurate?

A: This is not accurate, DARPA has always supported a mix of longer- and shorter-term research.

DARPA mines fundamental discoveries and accelerates their development and lowers their risks until they prove their promise and can be adopted by the Services. The key is a focus on high-risk, high-payoff research.

DARPA has two fundamental types of technical offices. Technology offices focus on new knowledge and component technologies that might have significant national security applications, which often involved longer-term research. System offices focus on technology development programs leading to products that more closely resemble a specific military end-product.

During periods of active conflict, DARPA adds an additional type of activity—quick reaction projects that take the fruits of previous science and technology investment and very quickly move the technology into a prototype, fieldable system and into the hands of deployed forces. There have been many published articles on some of these technologies.

Quick reaction projects are done in addition to DARPA's usual activities, not instead of.

The PITAC report addresses specifically cyber security research for commercial applications and seems to think that if research is classified, it is by definition short-term.

DARPA expects that its information assurance research will have a broad, beneficial impact on the commercial world, as commercial networks move toward the mobile, ad hoc, peer-to-peer features common to today's military networks.

Recall that the Internet, which came from DARPA research, progressed in the 1970s for DOD reasons, not commercial reasons. There are many other commercial products available today to protect the Nation's computer networks that are the result of DARPA research on information assurance for military networks having a fixed infrastructure similar to those encountered in the civilian community.

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. The military must achieve what has been called "critical infrastructure protection" without infrastructure. In the most advanced cases, these are peer-to-peer or "infrastructureless" networks. There is no fixed, in-place network equipment—the whole network architecture is fluid and reassembles dynamically.

In the long-term, commercial networks will acquire some of these features. Why? Because the cost of these networks will be considerably less than today's networks, in which fixed assets such as towers, etc., have to be built and maintained.

8. The report also states that DARPA programs are increasingly classified, thereby excluding most academic institutions. Is that accurate?

A: DARPA follows Executive Branch guidelines when classifying its programs—classification is only used to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to the national security.

It is true that some universities are not able to perform classified or ITAR research. But many DARPA programs are not classified and university researchers are often involved in them. 6.1 programs are defined as programs without a specific application in mind and are very seldom classified or have ITAR restrictions.

DARPA's programs are developing technologies to benefit the warfighter. DOD has an ongoing effort to streamline and shorten the amount of time necessary for advanced technology to be incorporated into new weapons systems and become operational. DARPA's role is to transition technology into military applications and demonstrations.

It should not be a surprise that, as the programs mature, they move from research that is unclassified to research that is either classified and/or ITAR restricted. In addition, as technology development moves along this continuum, it tends to increasingly involve industry performers who can actually produce the product.

This progression, which results in either classification as the application becomes focused, or ITAR restrictions at the component level, or the increasing involvement of industry, seems to account for the decrease in university performers in DARPA's 6.2 and 6.3 research. However as the answer to an earlier question showed, Universities receive nearly four times more resources from the 6.2 and 6.3 accounts as they do from 6.1

9. The report also asserts that DARPA's new mission is to incorporate pre-existing technology into products for the military rather than funding basic research. Is that accurate?

A: This is not true, there has been NO change in DARPA's core mission.

Our mission, established in 1958 in response to Sputnik, is to prevent technological surprise for the U.S. and create technological surprise for our adversaries. Our focus is and has always been solely on research and development for national security, and therefore portions of DARPA's research have always been classified or subject to ITAR restrictions.

Please read the answers to the previous questions and download "Bridging the Gap" from our website to find out what we are doing.

10. Reporter would like an interview w/Dr. Tether or other DARPA official to discuss these questions.

A: DARPA will provide written answers in lieu of an interview.

Appendix B

Senate Armed Services Committee Staff Request for DARPA Investment in Computer Science and Opportunities for University Participation

Introduction:

DARPA was requested by the SASC staff to provide an historical estimate of DARPA funding for Computer Science (CS), and the amount of that funding given to Universities.

The following material provides data to answer the questions.

For the purposes of this discussion, Computer Science (CS) is defined as:

> The systematic study of computing systems and computation. The body of knowledge resulting from this discipline contains theories for understanding computing systems and methods; design methodology, algorithms, and tools; methods for the testing of concepts; methods of analysis and verification; and, knowledge representation and implementation.

However it is doubtful that any accurate assessment whether or not DARPA interest in Computer Science has increased or decreased can be made.

Why is this true?

First of all, DARPA does not directly seek efforts in Computer Science; that is, DARPA does not publish Broad Agency Announcements (BAA's) requesting ideas to advance the field of Computer Science as a discipline.

Instead, DARPA publishes BAA's to solicit ideas for obtaining a particular capability, such as achieving 24 by 7 situational awareness, or developing a new High-Performance computer based upon productivity as a goal rather than raw speed as measured by instructions per second.

Whether or not Computer Science was needed to achieve these capabilities is a consequence of the effort and not a prime reason in its own right.

Because of this, it required significant effort to compile the numbers in this report. Each of DARPA's 400-plus efforts had to be examined individually to determine whether or not Computer Science was an ingredient.

In order to avoid having almost every effort classified as such, only those where Computer Science as defined above was a significant ingredient were included.

Hence the following funding data should be considered as a low estimate of the actual funding.

In addition, due to database constraints, the university participation funding data is limited to those instances where the university is identified as the prime (or sole) performer on the contract or grant. The database records the amounts obligated and disbursed to the performer of record on each contracting vehicle; subsequent funding distributions made by the prime contractor to subcontractors, which could include Universities, is not captured in the database.

Overall Computer Science Funding trends:

DARPA conducted a review of FY 1994–2004 funding for computer science research. The following table summarizes CS research funding for those years ($, Millions).

FY 94	FY 95	FY 96	FY 97	FY 98	FY 99	FY 00	FY 01	FY 02	FY 03	FY 04
471	546	536	512	523	557	525	546	571	613	583

These funds support a vast array of information research including basic (6.1) research, traditional software and high performance computing programs, information assurance and security, and applications of the technology for warfighter requirements in such areas as language translation, advanced networking, robotic systems control, and command and control systems.

Increasingly, DARPA funding is being applied to long-term research that is exploring cognitive computing, which is the quest for computers that are interactive with the user and capable of learning as opposed to the current generation of machine tools; the use of advanced quantum theory and biological based computer science; and, Defense applications of computer science research. Universities are not excluded from any of these research areas and are welcome to participate to the extent they are willing to comply with basic DoD oversight and security requirements and ITAR restrictions.

The years following the FY 1995 budget ($546 million) reflected completion of a number of software (architectures, persistent object bases), hardware programs (completion of the first high-performance computing initiative) and applications (global grid communications, defense simulation Internet, transition of the advanced simulation program to the Defense Simulation Systems Office).

As a consequence, funding declined in FY 1996–98 in comparison to the FY 1995 level.

The decline in computer science funding in the late 1990s would have been far more severe had it not been for the significant funding increases for information assurance programs (all of which had computer science as a significant part), and DARPA's participation in the Next Generation Internet program, a multi-agency, term limited (five-year) effort to explore network bandwidth expansion and quality of service initiatives.

Information assurance programs increased five fold between FY 1995 and FY 1999. In FY 1995, Information Assurance programs were only $10 million or less than two percent of computer science funding. By FY 1999, Information Assurance funding had increased to $55 million or 10 percent of the computer science total.

After a temporary lull in FY 2000, increases in middleware research and expanded emphasis on information tools for Asymmetric Threat prediction and prevention fueled the major expansion of IT funding in FY 2001–2003.

From FY 2000 to FY 2003 computer science funding rose $88 million or 17 percent. Yet even as the budget was increasing, the portfolio mix was changing. Agent based software, Quality of Service programs, and high performance computing architectures transitioned into DOD applications programs, and the Software Engineering Institute was transferred from DARPA's accounts to OSD.

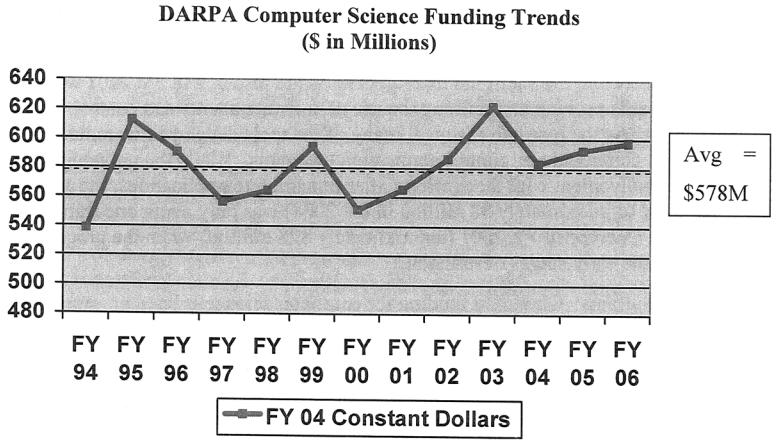
Between FY 2003 and FY 2004, overall funding for computer science research declined slightly, by $30 million or five percent, from $613 million to $583 million. A number of ongoing embedded software programs transitioned to major applications efforts such as the Future Combat Systems. Like FY 2000, the FY 2004 decrease is more an anomaly than a significant trend.

All computer science research activities associated with Asymmetric Threats programs were eliminated by congressional decree in FY 2004, thus further reducing the FY 2004 computer science budget by nearly $80 million, and also reduced out-year outlays. Funding increases in cognitive computing, language translation efforts, and classified applications partially offset the congressional action.

The FY 2005–06 budgets have held computer science funding constant at the FY 2004 level. The following table displays the budgets for FY 2004–2006 as reflected in the FY 2006 President's budget.

FY 04	FY 05	FY 06
583	583	584

Another way to look at the computer science trends, without the masking effect of inflation, is to covert and display the data in constant dollars. The following graph does just that.



When expressed in constant dollars, it becomes clear that the trend in DARPA computer science funding was downward from FY 1995 to FY 2000. The downward trend stopped in FY 2000 and has been increasing since then.

University Involvement in DARPA Computer Science Research: Data constraints limited the evaluation of university research funding to the FY 2001–2004 period. The following table shows university funding for those years.

	FY 2001	FY 2002	FY 2003	FY 2004
Total Comp Science	546	571	613	583
University Funding	214	207	173	123

There are factors for the decline, some of which were beyond DARPA's control. They are:

1. High Performance Computing (HPC): In FY 2001, over 50 percent of HPC funding ($67 million) went to universities. However, the program focus shifted from pure research to super computer construction. This change in emphasis resulted in the major CS vendors—Sun, IBM, Cray, etc.—receiving the bulk of the funding and as a result, universities received only 14 percent of the HPC funding in FY 2004 ($14 million). But, they are included in the program through sub-contract relationships
2. Information Assurance (IA): University research comprised $20 million of the $70 million applied to IA efforts in FY 2001. During the subsequent years, the IA program classification increased. By FY 2004, the unclassified budget for IA was less than half of the FY 2001 program, and the amount issued to universities had dropped to $4 million.
3. Asymmetric Threats: Universities received a consistent $11-12 million per year for asymmetric threat program research. This ended with congressional cancellation of the program in FY 2004.
4. Intelligent Software: Much of the intelligent software research in FY 2001 was oriented towards proving and refining the use of software agents and control architectures. As the research matured, many of the tools developed were integrated into network command and control application programs. While the universities continued involvement with these efforts after transition to applications, the amount they received (approximately $8 million in FY 2004) was only about one third the amount they received in FY 2001 (approximately $28 million) when the programs were still in the early stages of research.
5. Classified programs: Classified funding for computer science-related programs increased markedly between FY 2001 and FY 2004. Universities received none of this funding.

Appendix C

REPRINTED FROM

The New York Times

April 2, 2005

Pentagon Redirects Its Research Dollars; University Scientists Concerned by Cuts in Computer Projects

By JOHN MARKOFF

SAN FRANCISCO, April 1

The Defense Advanced Research Projects Agency at the Pentagon—which has long underwritten open-ended "blue sky" research by the Nation's best computer scientists—is sharply cutting such spending at universities, researchers say, in favor of financing more classified work and narrowly defined projects that promise a more immediate payoff.

Hundreds of research projects supported by the agency, known as DARPA, have paid off handsomely in recent decades, leading not only to new weapons, but to commercial technologies from the personal computer to the Internet. The agency has devoted hundreds of millions of dollars to basic software research, too, including work that led to such recent advances as the Web search technologies that Google and others have introduced.

The shift away from basic research is alarming many leading computer scientists and electrical engineers, who warn that there will be long-term consequences for the Nation's economy. They are accusing the Pentagon of reining in an agency that has played a crucial role in fostering America's lead in computer and communications technologies.

"I'm worried and depressed," said David Patterson, a computer scientist at the University of California, Berkeley who is President of the Association of Computing Machinery, an industry and academic trade group. "I think there will be great technologies that won't be there down the road when we need them."

University researchers, usually reluctant to speak out, have started quietly challenging the agency's new approach. They assert that DARPA has shifted a lot more work in recent years to military contractors, adopted a focus on short-term projects while cutting support for basic research, classified formerly open projects as secret and placed new restrictions on sharing information.

This week, in responding to a query from the staff of the Senate Armed Services Committee, DARPA officials acknowledged for the first time a shift in focus. They revealed that within a relatively steady budget for computer science research that rose slightly from $546 million in 2001 to $583 million last year, the portion going to university researchers has fallen from $214 million to $123 million.

The agency cited a number of reasons for the decline: increased reliance on corporate research; a need for more classified projects since 9/11; Congress's decision to end controversial projects like Total Information Awareness because of privacy fears; and the shift of some basic research to advanced weapons systems development.

In Silicon Valley, executives are also starting to worry about the consequences of DARPA's stinting on basic research in computer science.

"This has been a phenomenal system for harnessing intellectual horsepower for the country," said David L. Tennenhouse, a former DARPA official who is now Director of Research for Intel. "We should be careful how we tinker with it."

University scientists assert that the changes go even further than what DARPA has disclosed. As financing has dipped, the remaining research grants come with yet more restrictions, they say, often tightly linked to specific "deliverables" that discourage exploration and serendipitous discoveries.

Many grants also limit the use of graduate students to those who hold American citizenship, a rule that hits hard in computer science, where many researchers are foreign.

The shift at DARPA has been noted not just by those researchers directly involved in computing technologies, but by those in other fields supported by the agency.

"I can see they are after deliverables, but the unfortunate thing is that basic research gets squeezed out in the process," said Wolfgang Porod, director of the Center for Nano Science and Technology at the University of Notre Dame.

The concerns are highlighted in a report on the state of the Nation's cyber security that was released with little fanfare in March by the President's Information

Technology Advisory Committee. DARPA has long focused on long-term basic research projects with time horizons that exceed five years, the report notes, but by last year, very little of DARPA's financing was being directed toward fundamental research in the field.

"Virtually every aspect of information technology upon which we rely today bears the stamp of federally sponsored university research," said Ed Lazowska, a computer scientist at the University of Washington and co-chairman of the advisory panel. "The Federal Government is walking away from this role, killing the goose that laid the golden egg."

As a result of the new restrictions, a number of computer scientists said they had chosen not to work with DARPA any longer. Last year, the agency offered to support research by Leonard Kleinrock, a computer scientist at the University of California, Los Angeles who was one of the small group of researchers who developed the Arpanet, the 1960's predecessor to today's Internet.

Dr. Kleinrock said that he decided that he was not interested in the project when he learned that the agency was insisting that he employ only graduate assistants with American citizenship.

DARPA officials, who declined repeated requests for interviews, disputed the university researchers. The agency, which responded only in writing to questions, contended that the criticisms leveled by the advisory committee and other researchers were not accurate and that it had always supported a mix of longer- and shorter-term research.

"The key is a focus on high-risk, high-payoff research," Jan Walker, a DARPA spokeswoman, stated in an e-mail message. Given the threat from terrorism and the demands on troops in Iraq, she wrote, DARPA is rightly devoting more attention to "quick reaction" projects that draw on the fruits of earlier science and technology to produce useful prototypes as soon as possible.

The Pentagon shift has put added pressure on the other federal agencies that support basic information technology research.

At the Directorate for Computer and Information Science and Engineering of the National Science Foundation, the number of research proposals has soared from 2,000 in 1999 to 6,500 last year. Peter A. Freeman, its director, said that the sharp rise was partly attributable to declines in Pentagon support.

"DARPA has moved away from direct funding to universities," Mr. Freeman said. "Even when they do directly fund, some of the conditions and constraints seem to be pretty onerous. There is no question that the community doesn't like what the head of DARPA has been doing, but he has his reasons and his prerogatives."

The transformation of DARPA has been led by Anthony J. Tether, a Stanford-educated electrical engineer who has had a long career moving between executive positions at military contractors and the Pentagon.

Last year, Dr. Tether's new approach led to a series of cutbacks at a number of computer science departments. Program financing for a DARPA project known as Network Embedded Sensor Technology—intended to develop networks of sensors that could potentially be deployed on battlefields to locate and track enemy tanks and soldiers—has been cut back or ended on as many as five university campuses and shifted instead to traditional military contractors.

"The network has now become as vital as the weapons themselves," Dr. Tether said in an appearance before the advisory committee last year, testifying that secrecy had become—more essential for a significant part of the agency's work.

That has created problems for university researchers. Several scientists have been instructed, for example, to remove previously published results from Web sites. And at U.C.L.A. and Berkeley, DARPA officials tried to classify software research done under a contract that specified that the results would be distributed under so-called open-source licensing terms.

"We were requested to remove all publicly accessible pointers to software developed under the program," said Deborah Estrin, Director of Embedded Network Sensing at U.C.L.A. "This is the first time in 15 years that I have no DARPA funding."

At Berkeley, Edward A. Lee, who was recently named Chairman of the Computer Science Department, agreed not to publish a final report at DARPA's request, even though he told officials the data had already become widely available.

Despite the complaints, some pioneering researchers support the changes being driven by Dr. Tether and say they are necessary to prepare the Nation for a long battle against elusive enemies.

"There are pressures and demands on DARPA to be relevant," said Robert Kahn, a former DARPA administrator who is now President of the Corporation for National Research Initiatives in Reston, Va. "People think it should stay the same, but times have changed."

Still, a number of top scientists argue that the Pentagon's shift in priorities could not have come at a worse time. Most American companies have largely ended basic research and have begun to outsource product research and development extensively even as investments in Asia and Europe are rising quickly.

And many computer scientists dispute DARPA's reasoning that fighting wars demands a shift away from basic research. During the Vietnam War, they say, DARPA kept its commitment to open-ended computer research, supporting things like a laboratory in the hills behind Stanford University dedicated to the far-out idea of building computing machines to mimic human capabilities.

John McCarthy founded the Stanford artificial research lab in 1964, helping to turn it into a wellspring for some of Silicon Valley's most important companies, from Xerox Parc to Apple to Intel.

"American leadership in computer science and in applications has benefited more from the longer-term work," Mr. McCarthy said, "than from the deliverables."

Copyright © 2005 by The New York Times Co. Reprinted with permission.

Appendix D

Typical DARPA Research Efforts

1. **3–Dimensional Integrated Circuits:** Three dimensional stacked integrated circuits to achieve "human brain-like" complexity in digital circuits.
2. **Adaptive Focal Plane Array:** Tunable microelectromechanical (MEMS) etalons at each pixel of an infrared focal plane array for chip-scale hyperspectral imaging.
3. **Advanced Soldier Sensor Information System and Technology:** Methods that will allow machines to automatically parse multimodal sensory input into meaningful "experiences" and support intelligent indexing and retrieval of useful episodes.
4. **Architectures for Cognitive Information Processing:** Radically new computer architectures that are a better match to cognitive information processing algorithms than conventional Von Neumann machines.
5. **Biological Sensory Structure Emulation:** Fundamental understanding of biological sensory structures, and emulating this knowledge to create superior synthetic sensors.
6. **Biologically-Inspired Cognitive Architectures:** Relatively complete models of the brain's functioning mapped to brain structures; models for cognition, as well as understanding memory models used by people for everyday reasoning.
7. **Bio-Magnetic Interfacing Concepts:** Novel capabilities for integrating nanomagnetics with biology as a powerful new tool for manipulation and functional control of large numbers of cells and biomolecules, including magnetically actuated, on/off control of cellular functions, and magnetic filtration of pathogens.
8. **Canard Rotor Wing:** Aircraft capable of transforming from a helicopter into a jet-and retaining all the advantages of either.
9. **Chip Scale Atomic Clock:** Atomic time precision in devices smaller than a dime that will revolutionize modern networking and communications.
10. **Close Combat Lethal Reconnaissance:** A new weapon approach that allows long-range indirect fire to occur at the individual soldier level.
11. **Computational Fluid Dynamics:** Incorporation of underlying physics will enable advances in CFD for building ships with greatly reduced friction drag, and building extraordinarily quiet helicopter blades.
12. **Coordination Decision-Support Assistants:** Personalized machine-based cognitive coordination agents to assist commanders in adapting complex plans in real time to changing situations.
13. **Cormorant:** Unmanned aircraft that can be launched from a submarine and retrieved at the end of a mission.
14. **Data in Optical Domain—Network:** All-optical communications with optical coding, storage, multiplexing, and routing.
15. **Defense Against Cyber Attacks on Mobile Ad Hoc Network Systems:** Cognitive, autonomous, information assurance tools for next-generation, yet-to-be-deployed, tactical military networks.
16. **Disruption Tolerant Networking:** Replacing the connection oriented philosophy of today's Internet with protocols that guarantee message delivery, even when connections are disrupted.
17. **Dynamic Quarantine of Computer-Based Worms:** Computer defenses that operate "faster-than-worm-speed" against zero-day worms.
18. **Electronic and Photonic Integrated Circuits:** Ubiquitous photonics produced on the same wafer as silicon microelectronics.
19. **Engineered Bio-Molecular Nano-Devices/Systems:** Engineered bio-molecular nanoscale devices that emulate the behavior of membrane ion channels to enable real-time observation and analysis of bio-molecular signals, enabling single-molecule sensitivity.

20. **Exploitation of 3D Data:** New methods to describe and analyze shape signatures from advanced 3D sensors that can recognize specific targets from a vast array of alternatives; e.g., finding a specific terrorist vehicle in urban clutter.
21. **Focus Areas in Theoretical Mathematics:** New mathematical foundations for conformal field theory in physics.
22. **Global Autonomous Language Exploitation:** Ultimately replace human language translators and human analysts with machine language processing that leads directly from source natural language (speech or text) to actionable intelligence.
23. **Global Reach With Global Endurance:** Novel aircraft and propulsion concepts to enable aircraft to launch from the United States and reach anywhere in the world—and stay aloft for weeks at a time.
24. **Heterogeneous Urban Reconnaissance Teams:** System to provide real-time reconnaissance, surveillance, targeting, and acquisition services directly to warfighters in complex urban environments.
25. **High-Productivity Computing Systems:** Viable peta-scale processor to be available (in small numbers) by 2010.
26. **Handheld Isothermal Silver Standard Sensor:** Develop a handheld sensor for biological warfare agents that brings laboratory-quality assays into the field.
27. **Human Assisted Neural Devices:** Fundamental research to enable the understanding and use of brain activity to control external prosthetic devices, using sensory feedback and memory.
28. **Hypersonic Aircraft and Missiles:** Controlled flight at higher speeds than ever before, exploring the uncharted territory of flight at six to 20 times the speed of sound.
29. **Immune Buildings:** Buildings to actively defend against chemical and biological warfare agent releases inside or near them.
30. **Improving Warfighter Information Intake Under Stress:** A machine that recognizes a human's cognitive state (especially under stress) and adapts its mode of information presentation based on the state.
31. **Indoor and Underground Navigation:** GPS-like capability to navigation inside and underground.
32. **Innovative Space-Based Radar Antenna Technology:** Components, deployment technologies, and active calibration methods to enable affordable, tactical-grade targeting from space, thereby enabling true persistent surveillance of all moving ground vehicles.
33. **Integrated Sensor Is Structure:** Integrate the world's largest radar into a station keeping airship, to enable uninterrupted, persistent surveillance of all air and ground targets, including dismounted troops.
34. **Intelligence, Surveillance, and Reconnaissance (ISR) for Building Internals:** Extend the range of our ISR capabilities to include determining building layout and occupancy from outside, prior to entry.
35. **Laser Weapons:** Tactical and practical laser weapons that can be carried in a HMMWV or fighter jet and are capable of shooting any tactical threat out of the air-from missiles to mortars.
36. **Low Power Micro Cryogenic Coolers:** Local refrigerators machined into regions of highly sensitive circuits to increase the performance of the electronics without appreciable increases in the direct current power.
37. **Machines That Mimic Nature:** Nano-flapping winged vehicles, vehicles that flare to land like birds, and snake-like robots.
38. **Mission-Adaptable Chemical Spectrometer:** A man-portable, chemical identification system with a sensitivity of 10 parts per trillion.
39. **Mobile Integrated Sustainable Energy Recovery:** Novel mechanical and chemical approaches to allow the processing of military waste into logistics fuels.
40. **Negative Index Materials:** Novel microwave materials that have a negative refractive index ("left handed") behavior, and extending this behavior to the optical regime.

41. **New Concepts for Logistics:** Novel, heavy lift aircraft concepts capable of moving an entire army brigade from fort to fight-eliminating any need for bases outside the United States.
42. **Novel Satellite Communications:** Jam-proof communications satellites.
43. **Ocean Wave Energy Harvesting:** High efficiency harvesting of electrical energy from wave motion.
44. **Opto-Electronics for Coherent Optical Transmission And Signal Processing:** Exploit phase control of photons to realize coherent optical free-space communications.
45. **Persistent Operational Surface Surveillance and Engagement:** Persistent surveillance system that can respond rapidly to a rapidly evolving insurgent threat.
46. **Personalized Assistant That Learns:** Integrated, enduring personalized cognitive assistant that perceives, reasons, and learns.
47. **Protein Design Processes:** Approaches to radically transform the protein design process by developing new mathematical and biochemical approaches to the in silico design of proteins.
48. **Quantum Information Science and Technology:** Fundamental technology and ideas that could ultimately lead to a quantum computer.
49. **Rad Decontamination:** First methods to decontaminate buildings after release of radiological dispersal device; provides a clean-up option other than rubbleization.
50. **Radiation Hard By Design:** Putting Moore's Law into space by exploiting commercial integrated circuit fabrication of military-critical circuits for satellites.
51. **Rapid Vaccine Assessment:** Interactive and functional in vitro human immune system that will replicate the in vivo human immune response.
52. **Real-time Adversarial Intelligence and Decision-making:** Methods that model an adversary's likely course of action in different urban combat scenarios.
53. **Real-World Reasoning:** Fundamental research in machine reasoning, trying to drastically improve the scale at which certain types of reasoning can be done.
54. **Restorative Injury Repair:** Fundamental understanding of the behavior of cells as they recover from injury, and learning how to control their regeneration in order to regrow the original structure (skin, muscle, etc.), rather than scar.
55. **Robotic Ground Vehicles:** Ground vehicles that can sense and react to complex terrain-negotiating obstacles, discovering paths, avoiding detection, and conducting military missions.
56. **Robotic Space Assembly Concepts:** Revolutionary space capabilities on orbit—systems too complex and fragile to be constructed anywhere but in zero-G.
57. **Robotic Spacecraft:** Autonomously repairing, upgrading, and refueling other satellites-completely changing the paradigm and economics of "disposable" military spacecraft.
58. **Satellite Navigation:** Using pulsing neutron stars as GPS-like sources.
59. **Self Forming Constellations of Tiny Intelligent Spacecraft:** Spacecraft that are cheap, easy to launch, and swarm together to provide entirely new capabilities beyond current space systems.
60. **Self-Regenerative Systems:** Revolutionary capabilities for computer systems under cyberattack to heal themselves, create immunity to future attack, and recognize and stop insider threats.
61. **Semiconductor Ultra Violet Optical Sources:** New region of the photon spectrum with wide bandgap semiconductor lasers and light emitting diodes.
62. **Slow Light:** Fundamental physics and new solid-state materials that slow, store, and process light pulses, i.e., optical information, in optical components.
63. **Standoff Precision Identification in Three Dimensions:** New long-range ladar that can acquire entire scenes in a single frame, rather than by scanning.

64. **Statistical and Perturbation Methods in Partial Differential Equation (PDE) Systems:** Stochastic treatment of fundamental PDEs modeling physical systems; e.g., Maxwell, Navier-Stokes, Helmholtz, Poisson, and Laplace.

65. **Surviving Blood Loss:** Fundamental understanding of the mechanisms of oxygen use in cells and the mechanisms of hibernation in order to increase the time before onset of hemorrhagic shock.

66. **Sustained Littoral Presence:** Using the chemistry of the undersea environment to generate electrical power.

67. **Swarming Robotic Flyers for Urban Reconnaissance:** Controlling every intersection and rooftop and reporting directly back to the soldier on the ground.

68. **Technology for Frequency Agile Digitally Synthesized Transmitters:** 500 GHz transistors with large dynamic range to support circuits for direct digital generation of microwave waveforms.

69. **Terahertz Imaging Focal Plane Array Technology:** Bridging the terahertz gap with sources and detectors in the 300 to 3,000 GHz (3 THz) frequency range.

70. **Triangulation Identification for Genetic Evaluation of Biological Risk:** The first, truly broadband sensor for detecting biological warfare agents, as well as diagnosing human disease, including agents/diseases never before seen or sequenced.

71. **Tiny Bullets and Grenades:** Munitions capable of steering themselves in flight to hit the hardest targets at the farthest ranges.

72. **Topological Data Analysis:** Mathematical concepts and techniques necessary to determine the fundamental geometric structures underlying massive data sets.

73. **Traction Control:** Nonlethal force multiplier to develop capability to adjust traction on surfaces to allow traction by U.S. forces, but deny it to the enemy.

74. **Transfer Learning:** New methods for learning that ultimately will allow the transfer of knowledge learned on one problem to many others not anticipated when the initial learning was done.

75. **Untouchable Aircraft:** Giving aircraft the capability to shoot down modern missile threats with high power beam weapons.

76. **Very High Efficiency Solar Collectors:** Engineered biomolecules to guide the assembly of inorganic molecules to create solar cells that are 50 percent efficient.

77. **Wide Bandgap Semiconductors for RF Applications:** High power, high frequency transistors based on wide bandgap semiconductors for future radar, electronic warfare, and communications systems.

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.

Chairman BOEHLERT. Dr. Wulf.

STATEMENT OF DR. WILLIAM A. WULF, PRESIDENT, NATIONAL ACADEMY OF ENGINEERING

Dr. WULF. Good morning, Mr. Chairman and Members of the Committee. I am Bill Wulf. I am President of the National Academy of Engineering. I am on leave from the University of Virginia, Computer Science Department where, among other things, I did research on cyber security. I really appreciate the opportunity to testify to the Committee today, because I think this is a really important issue.

I come at this from the, I think, fortunate perspective of an academic who has received federal support from both DARPA and NSF, being the founder of a software company and thus a personal witness to how that federal support translates into commercial product, as someone who had the responsibility of dispensing those research funds as Assistant Director of the National Science Foundation, and now, at the Academies, as a participant in a broad range of technology-related public policy discussions.

Before I respond to the specifics of the questions that were in the letter inviting me here, I would like to touch on three points having to do with how I think about these issues.

First, in "Science the Endless Frontier," the report that established the system of federal funding of basic research that we now have, Vannevar Bush advocated a system in which the government funds research, but the research to be done is selected on its merit by the researchers themselves. He said that such a system would

pay dividends to the Nation in national security, prosperity, and health. Frankly, I think it is hard to think of a better "poster child" for the truth of this assertion than computer science.

From smart bombs for defense, to a three percent productivity growth due to information technology, to cochlear implants, the Nation has benefited tremendously from the federal investment in long-term basic research at universities. Note I said "investment" in long-term research. I think it is a mistake to think of such funding as an expense. It is an investment that demonstratively has had a huge return.

Second, computing and computer science is in the unusual position of being both a challenging intellectual discipline in itself and providing an infrastructure for other fields of science, engineering, and commerce. While many benefits to society can be directly attributed to computer science, there are many more that have resulted from the use of computing in everything from cosmology, to weather prediction, to health care, to Wal-Mart's "just in time" delivery system. Across this broad spectrum, computer science has been an investment with an enormous multiplier, because advances in computing and information technology have immediate, direct, and tangible benefits on virtually all human activities.

Third, it is about people, stupid! It is worth reminding ourselves that Bush's "Science the Endless Frontier" was written in response to President Roosevelt's question about how we would ensure, how the country would ensure, that if there were another world war we would have the people able to do what the scientists and engineers did to help win World War II. For all of the bounties that we can point to as coming from computing research, the most important output has been the cadre of educated women and men that can take us to the next level.

So with that context, let me touch now on some of the questions in your invitation letter to me. I hope I have answered them all and answered them more fully in my written testimony.

I must say that although this hearing is about the state of computer science, I am more generally concerned about what I perceive as a shift to more risk-adverse funding of research in all of the physical sciences and engineering. But with respect to computer science, within the context of this general drift toward conservatism, I would make several points.

First, the NSF budget for computer and information science and engineering has grown nicely from when I ran that directorate in the '80s, and I think the CISE Directorate is to be congratulated for using that growth to increase the average grant size rather than taking the politically easier route of funding more proposals.

This has, however, led it to a potentially serious decline in the success rate; that is, the number of proposals that are funded as a fraction of those that are submitted, although I must say that the success rate is determined by a number of factors, not just the amount of funds. I don't have access to the data that would let me analyze how serious the problem is in specific areas. What I can say, from discussions with my colleagues, however, is that the computer science community believes that it is a serious problem and has adapted its behavior accordingly. More time is spent writing

proposals rather than doing research, more failed proposals are recycled, more incremental and less bold ideas are advanced.

NSF has, by the way, and with thanks to this committee, focused more resources on cyber security research. It is, in fact, now the major supporter of university-based research in this area. This is, however, also an example of the success rate problem. Only slightly more than eight percent of the proposals in response to its Cyber Trust Initiative were funded.

Second, I am deeply concerned about what I believe is happening at DARPA. On top of what I perceive to have been a many-year drift toward the less ambitious and more incremental, the Iraq War has been described as a reason to dramatically accelerate this to focus on reaping the successes of the past, to focus on rapid deployment, to focus on industrial development over university research, and to shift the balance strongly toward near-term topics.

While I can certainly agree that reaping, developing, and focusing on the near-term are needed, so is long-term investing. Without current investment, there won't be anything to reap in the future. Moreover, there are many DOD organizations that can reap and develop. There was only one old style DARPA, and it is gone.

The problem with trying to assess the consequences of the kind of shift we have seen at DARPA is that they are opportunity costs. They are measured in "might have beens," and at best, are evident only years after the fact. By comparison with tangible, immediate results of reaping and developing, such costs may appear ephemeral and perhaps even wasteful. Yet one can only wonder at what the world would be like today if the immediacy of the Vietnam and Cold Wars had diverted ARPA—intentionally ARPA, not DARPA—from funding crazy ideas like networking, timesharing, VLSI, graphics, RISC architectures, RAID disk systems, parallel computing. These and any number of other technologies are central to today's computer industry and the results pay off daily to industry, government, consumers, and the military.

It is well known that it takes about 15 years, plus or minus a few, for ideas to make their way from laboratory to product. One way to look at that is that there is normally a 15-year pipeline of ideas and technologies. In fact, only a few of the ideas in that pipeline will, in fact, become commercial, and we have no good way to predict which of them will be the most important. Thus, if one stops filling the pipeline, the effect on industry will not be immediately visible as it "drains" the pipe, nor will the exact nature of the future impact be predictable. But that there will be an impact is an inescapable lesson of history.

As was noted in the recent Defense Science Board Task Force, this was from February of 2005, on High Performance Microchips, I quote: "University and independent laboratory work has played an important role in microelectronic history in that it has sown the seeds for major technological shifts. At a time when the effectiveness of conventional approaches to the extension of Moore's Law are nearing their end, new ideas are essential to continue the progress on which the industry and future military systems depend."

Although this DSB report is focused on microelectronics, much the same can be said for all aspects of information technology. At

a time of growing global competition, DARPA's disinvestment in university-based, long-term research is, in my view, a risky game for the country.

You also asked me about the government's priorities for research. I suspect that the answer to that question, by a set of randomly-chosen computer scientists would very enormously and probably correlate pretty well with whether their individual research interests are on today's "in list." Frankly, my concern is less with what is on that "in list" than with the frequency with which the list changes.

As I tried to say in my previous testimony to this committee on the issue of cyber security, stability of funding is as important as its magnitude. Academic careers are built on a reputation for work done over decades. If the perception is that the area is a "fad," it may attract a few weaker researchers, but the best researchers will migrate to where multi-decade support is probable.

Given that I have already run over my time, Mr. Chairman, I will end there and thank you very much for the opportunity.

[The prepared statement of Dr. Wulf follows:]

PREPARED STATEMENT OF WILLIAM A. WULF

The State of Computer Science Research in the U.S. and the Evolution of Federal Support for It

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

A few words about my background will provide a context for my remarks. I was a professor at Carnegie Mellon University (CMU) for 13 years (from 1968 to 1980); and during that time I did research in a number of subfields of Computer Science—specifically computer security, computer architecture, operating systems, programming languages, and optimizing compilers. I left CMU in 1980 to found and run a software company and subsequently served as an Assistant Director of the National Science Foundation (NSF). In 1991, I returned to academia at the University of Virginia, where I resumed my research in Computer Science. In 1997 I became President of the National Academy of Engineering which, together with the National Academy of Sciences, is chartered by the Congress to provide advice to the government on issues of science, engineering and health. Thus I have the fortunate perspective of being a recipient of federal research support, a witness to how that support translates into commercial product, someone with the responsibility of dispensing that research support, and a participant in a broad range of technology related public policy deliberations.

Before responding to the specifics of the questions in your letter inviting me here today, I would like to make four points concerning how I think about these issues.

First, in *Science The Endless Frontier,* the report that established our system of federal funding of basic research, Vannever Bush advocated a system in which the government funds research, but the research to be done is selected on its merit by the researchers themselves. He said that such a system would pay dividends to the Nation in national security, prosperity, and health. It is hard to think of a better "poster child" for the truth of this assertion than Computer Science. Consider the abbreviated list:

National Security: smart bombs, GPS, unprecedented "information awareness" for the war-fighter, unmanned robotic vehicles for surveillance, enormously enhanced training through use of virtual reality, etc.

Prosperity: a three percent national productivity growth fueled by information technology, dozens of multi-billion dollar per year industries (see Figure 1), Internet-enabled business models, a 40-fold reduction in the cost of telephony, a global wireless phone system, etc.

Health: Medical imagery (CAT scans, etc.), cochlear implants, bio-sensors, smart prosthetics, smart defibrillating pacemakers, etc.

All of these were made possible by the federal investment in long-term, basic computing research. It is a mistake to think of such funding as an "expense;" it is an investment that demonstrably has had a *huge* return! Technology such as that listed above is the return on the investments made a decade or more ago. Investments made today in research will have equally large returns for our children and grandchildren; conversely, it is our children and grandchildren that will pay if we do not make them now.

Second, computing and computer science is in the unusual position of being both a challenging intellectual discipline in itself, and providing an infrastructure for other fields of science, engineering, and commerce. While the benefits to society listed above can be directly attributed to computer science, there are also many more benefits that have resulted from the use of computing in everything from cosmology, to weather prediction, to health care, to Walmart's "just in time" inventory. Across this broad spectrum, computer science has enabled a better quality of life for us all. For me this simply reinforces the notion that funds expended on computing research are demonstrably investment, not expense. They are, in fact, an investment with an enormous multiplier because advances in computing and information technology have immediate, direct and tangible benefits on virtually all human activities.

Third, I do not believe the "linear model" of technology development! In my experience, the idea that basic research begets applied research begets development begets benefits to society is both wrong and counter-productive when applied to public policy decisions! Instead, there is a marvelously rich and productive interplay between basic scientific discovery and application, between universities and industry, between societal need and technology. We refer to Figure 1 as the "tire tracks chart;" it shows the relation between industry and universities in the development of about twenty information technologies, each of which produces more than a billion dollars of revenue per year. As you can see, progress does not always start with basic research, and it often involves iteratively exchanging roles between university and industry. The bottom line, however, is that if federally-funded, university-based basic research weren't "in the loop," these enormously beneficial technologies would not exist. Basic research may not be the original source for all the benefits we enjoy from technology, but it is a vital and irreplaceable component of the rich system that produces them.

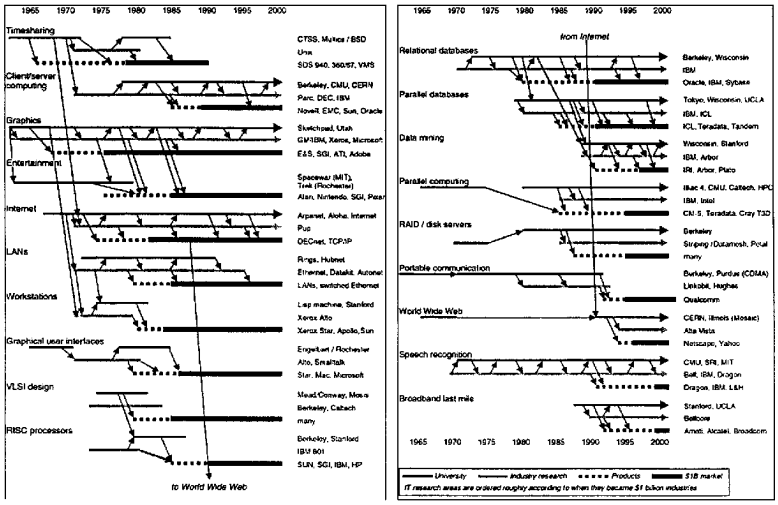


Figure 1:

Fourth and finally, it's about people, stupid! It is worth reminding ourselves that Bush's *Science The Endless Frontier* was written in response to President Roosevelt's question about how we can ensure that, if there were another world war,

we would have the *people* able to do what scientists and engineers did to help win WWII. For all the bounties that we can point to as coming from computing research, the most important output has been the cadre of educated women and men that can take us to the next level. From personal experience, I firmly believe that the U.S. early dominance in electronics and software was because of the students educated by the enlightened policies of DARPA and NSF beginning in the 1960's! If computing research has a large multiplier because of its broad application, then the people capable of doing that research are yet another multiplier on top of that! Disinvestment in university-based research is a disinvestment in the production of the next generation of people, with far greater negative impact than simply the loss of the research.

With that context, let me now turn to the three questions in your invitation to me:

1. What effects are shifts in federal support for computer science—e.g., shifts in the balance between short- and long-term research, shifts in roles of different agencies—having on academic and industrial computer science research? What effects are changes in the research likely to have on the future of the U.S. information technology industry and on innovation in the field?
2. Are the Federal Government's current priorities related to computer science research appropriate? If not, how should they be changed?
3. What are [my] views on the recent President's Information Technology Advisory Committee (PITAC) report on cyber security? What should the Federal Government be doing to implement the recommendations of this report? Should PITAC be renewed when its current term expires on June 1?

Although this hearing is about the state of computer science, I am concerned about what I perceive as a shift to more risk averse funding of research in *all* of the physical sciences and engineering, and in all of the agencies that have traditionally funded such research. At a macro-level, I am concerned that while this committee has authorized a doubling of the NSF budget, the funds have not been appropriated. I am equally concerned about the proposed decrease of DOD 6.1 funding. It is easy to make, and even to understand, the argument that in the current budget situation increases are not likely in either of these accounts; nonetheless, I find it *deeply* troubling that there seems to be little recognition of the long term consequences of a decision not to make these investments.

As I have testified to this committee before, it is *not* just that there is an increasingly short-term focus in some agencies, it is that even in those agencies with a longer-term focus, when resources are tight, researchers themselves propose more incremental, less risky projects. Where bold new ideas are needed, as in cyber security, we see conservatism and temerity instead. There are exceptions of course, but perversely, when resources are tight we generally get less out of what we do spend. Someone once said that great research does not come from moments of great insight, but from moments of great courage! When the existence of one's research program is on the line, courage becomes even rarer than usual. There is a cascading effect of this—more timid PI's educate students to be more timid, provoking a long-term decline in the quality of research.

With respect to computer science within this general drift towards conservatism, I would make several points:

First, at NSF the budget for Computer and Information Science and Engineering (CISE) has grown nicely from when I ran it in the late 80's, and CISE is to be congratulated for using that growth to increase the average grant size rather than taking the politically easier route of funding more proposals. In addition, it has added center-scale projects through its Information Technology Research (ITR) program. Together, however, this has led to a potentially serious decline in the "success rate" in some areas—although the success rate is determined by a number of factors and I do not have access to the data to let me analyze just how serious this is in specific areas. What I *can* say from discussions with my colleagues is that the computer science community *believes* that it is serious and has adapted its behavior accordingly: more time is spent writing proposals, more failed proposals are "recycled," more incremental and less bold ideas are advanced, etc. I suspect that the decline in success rates is serious, but I know that even if it is not, it is having a significant negative impact.

NSF has, by the way, and with thanks to this committee, focused more resources on cyber security research. NSF is, in fact, now the major supporter of university-based research in this area. It is, however, also an example of the success rate problem mentioned above—only slightly more than eight percent of the proposals in response to its Cyber Trust initiative were funded!

Having been the Assistant Director in charge of CISE, I can't help also remarking that there is often a misunderstanding of the CISE budget. About half of it is leverage for other fields, not computer science. CISE manages the Foundation's investment in cyber-infrastructure that is devoted to supporting those other fields. When at the Foundation I felt simultaneously proud to have the opportunity to leverage the success of those other fields, and frustrated at the misunderstanding by many of how little of our budget was actually devoted to the basic underpinning that created that leverage.

Second, I am deeply concerned about what has happened at DARPA. On top of a many year drift toward the less ambitious and more incremental, the Iraq war has been described as a reason to dramatically accelerate this—to focus on reaping the successes of the past, to focus on rapid development, to industrial development over university research, and to shift the balance strongly toward near-term topics. While I can agree that reaping, developing and focusing on the near-term *are* needed, so is long-term investing. Without current investment there won't be anything to reap next time. Moreover, while there are many DOD organizations that can reap and develop, and that collectively have the bulk of DOD's Science and Technology budget, there was only one old-style DARPA, and it is gone.

The problem with trying to assess the consequences of the kind of shift we have seen at DARPA is that they are opportunity costs, measured in "might have beens," and at best evident only years after the fact. By comparison with the tangible, immediate results of reaping and developing, such costs may appear ephemeral and perhaps even wasteful. Yet one can only wonder at what the world would be like today if the immediacy of the Vietnam War had diverted ARPA from funding crazy ideas like networking, timesharing, VLSI, graphics, RISC architectures, RAID disk systems, parallel computing—or any number of other technologies that are *essential* to today's computer industry and whose results pay off daily to industry, government and the consumer *as well as* the military.

Any number of studies have shown that it takes about fifteen years, plus or minus a few, for ideas to make their way from laboratory to product. One way to look at that is that there is a fifteen year pipeline of ideas and technology. Only a few of these ideas will, in fact, become commercial, and we have no good way to predict which of them will be the most important. Thus, if one stops filling the pipeline, the effect on industry will not be immediately visible as it "drains" the pipeline, nor will the exact nature of the future impact be predictable. But that there will *be* an impact is an inescapable lesson of history.

As was noted in the recent (February 2005) Defense Science Board (DSB) Task Force on High Performance Microchip Supply:

> *"University and independent laboratory work has played and important role in micro-electronic history in that it has sown the seeds for major technological shifts.. . . At a time when the effectiveness of conventional approaches to the extension of Moore's Law are nearing their end, new ideas are essential to continue the progress on which the industry and future military systems depend."*

Although this DSB report is focused on micro-electronics, much the same can be said for all aspects of information technology. At a time of growing global competition, DARPA's disinvestment in university-based, long-term research is, in my view, a risky game for the country.

Third, please permit me to vent an old annoyance. Information technology has become critical to virtually every agency of the Federal Government, and specifically to those that fund research—NASA, DOE, NIH, EPA, NOAA, etc. I believe it is fair to say that these agencies could not fulfill their primary mission without the information technology developed in the last 50 years. Yet none of these agencies has contributed significantly to the development of the basics underlying that technology. As concerned and unhappy as I am with the trends at the traditional funders of computer science, I am at least as much so with the complete absence of those other agencies that benefit enormously from computer science research!

Now let me turn to the question about the government's priorities. I suspect that the answer to this question by a set of randomly chosen computer scientists would vary enormously and correlate well with whether an individual researcher's interest was on today's "in list." My concern is less with what is on today's "in list" than with the frequency with which the list changes. As I tried to say in my previous testimony to this committee on the issue of cyber security, stability of funding is as important as its magnitude. Academic careers are built on a reputation for work done over decades. If the perception is that an area is a "fad," it may attract a few weaker researchers, but the best researchers will migrate to where multi-decade support is probable.

I understand the desire for program officers and agency heads to "make their mark," but I think the most effective and profound change the government could make would be to ensure that any new programs last long enough to have an effect—to attract people, let them find their footing, have a real chance to succeed or fail, and produce real benefit to society! Such a move would both raise the bar on evaluation of new programs and create the stability that will ensure that the best researchers become involved.

To answer your third question—as you might expect from my previous testimony to this committee,[1] I am strongly in agreement with the recent PITAC report on Cyber Security.[2] I am particularly pleased that they strongly identified the need for a better funded and stable program of long-term basic research; as you will recall, that was what I also recommended. In my view, the dominant model of cyber security, namely a perimeter defense, is flawed and incremental patches to it will never result in the level of security we need for today's systems, much less the increased dependence we should expect for future ones. This is an excellent example where boldness and courage are needed, and hence where the perception of excessively low proposal success rates can have severe consequences! Their one recommendation that was not in my previous testimony concerns the need for coordination among the various agencies that fund cyber security research, and I concur that such coordination is needed. It is too soon to know what will happen as a result of the report, but I hope it will be aggressively implemented.

Concerning PITAC—I believe it fulfills a unique and important role. Its reports on Health Care Information Technology and Cyber Security have been extremely valuable, and I expect their forthcoming report on Computational Science will be as well. So, from my perspective it is important for PITAC to be re-chartered, but that clearly hinges on the Administration's perception of its utility, not mine. If it is re-chartered, I would like to see PITAC tackle the broader issues that are the subject of this hearing, namely whether the Nation's overall information technology R&D investment appropriate for us to maintain our lead in this critical field.

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

BIOGRAPHY FOR WILLIAM A. WULF

Education:

B.S. Engineering Physics University of Illinois, 1961

M.S. Electrical Engineering University of Illinois, 1963

Ph.D. Computer Science University of Virginia, 1968

Positions:

President, National Academy of Engineering, 1996 to present.

AT&T Prof. of Engr., University of Virginia, 1988 to present.

Assistant Director, National Science Foundation, 1988 to 1990.

Chairman & CEO, Tartan Laboratories Inc., 1981 to 1987.

Professor, Carnegie-Mellon University, 1975 to 1981.

Associate Professor, Carnegie-Mellon University, 1973 to 1975.

Assistant Professor, Carnegie-Mellon University, 1968 to 1973.

Instructor, University of Virginia, 1963 to 1968.

Descriptive Biography:

Dr. Wulf was elected President of the National Academy of Engineering (NAE) in April 1997; he had previously served as Interim President beginning in July 1996. Together with the National Academy of Sciences, the NAE operates under a congressional charter and presidential executive orders that call on it to provide advice to the government on issues of science and engineering.

Dr. Wulf is on leave from the University of Virginia, where he is a University Professor and the AT&T Professor of Engineering and Applied Science. Among his activities at the University were a complete revision of the undergraduate Computer Science curriculum, research on computer architecture and computer security, and an effort to assist humanities scholars exploit information technology.

---

[1] Testimony to the House Science Committee, *CYBER SECURITY: BEYOND THE MAGINOT LINE,* 10 Oct. 2001

[2] President's Information Technology Advisory Committee (PITAC), *Cyber Security: A Crisis of Prioritization,* February 2005.

In 1988-90 Dr. Wulf was on leave from the University to be Assistant Director of the National Science Foundation (NSF) where he headed the Directorate for Computer and Information Science and Engineering (CISE). CISE is responsible for computer science and engineering research as well as for operating the National Supercomputer Centers and NSFNET. While at NSF, Dr. Wulf was deeply involved in the development of the High Performance Computing and Communication Initiative and in the formative discussions of the National Information Infrastructure.

Prior to joining Virginia, Dr. Wulf founded Tartan Laboratories and served as its Chairman and Chief Executive Officer. Before returning to academe, Dr. Wulf grew the company to about a hundred employees. Tartan developed and marketed optimizing compilers, notably for Ada. Tartan was sold to Texas Instruments in 1995.

The technical basis for Tartan was research by Dr. Wulf while he was a Professor of Computer Science at Carnegie-Mellon University, where he was Acting Head of the Department from 1978–1979. At Carnegie-Mellon Dr. Wulf's research spanned programming systems and computer architecture; specific research activities included: the design and implementation of a systems-implementation language (Bliss), architectural design of the DEC PDP–11, the design and construction of a 16 processor multiprocessor and its operating system, a new approach to computer security, and development of a technology for the construction of high quality optimizing compilers. Dr. Wulf also actively participated in the development of Ada, the common DOD programming language for embedded computer applications.

While at Carnegie-Mellon and Tartan, Dr. Wulf was active in the "high tech" community in Pittsburgh. He helped found the Pittsburgh High Technology Council and served as Vice President and Director from its creation. He also helped found the CEO Network, the CEO Venture Fund, and served as an advisor to the Western Pennsylvania Advanced Technology Center. In 1983 he was awarded the Enterprise "Man of the Year" Award for these and other activities.

Dr. Wulf is a member of the National Academy of Engineering, a Fellow of the American Academy of Arts and Sciences, a Corresponding Member of the Academia Espanola De Ingeniera, a Member of the Academy Bibliotheca Alexandrina (Library of Alexandria), and a Foreign Member of the Russian Academy of Sciences. He is also a Fellow of five professional societies: the ACM, the IEEE, the AAAS, IEC, and AWIS. He is the author of over 100 papers and technical reports, has written three books, holds two U.S. Patents, and has supervised over 25 Ph.D.s in Computer Science.

NATIONAL ACADEMY OF ENGINEERING

2101 Constitution Avenue, NW
Washington, DC 20418
http://www.nationalacademies.org

Office of the President
202 334 3201 / Fax: 202 334 1680
E-mail: wwulf@nae.edu

May 6, 2005

The Honorable Sherwood Boehlert
Chairman
House Committee on Science
2320 Rayburn House Office Building
Washington, DC 20515

Dear Mr. Chairman:

As requested, as Chair of The National Academies Division of Engineering and Physical Sciences which has jurisdiction over the Computer-Science and Telecommunications Board, I am attaching a list of federal funding (by agency and program) which that Board has received during the current fiscal year and two preceding fiscal years

Please let me know if you need any clarification or additional information. I look forward to appearing before your Committee on Thursday, May 12, 2005.

Sincerely,

Wm. A. Wulf
President

Enclosure

sponsor	awardtitle	Award Amt
USDOE	COMPUTER SCIENCE AND TELECOMMUNICATIONS BOARD	$687,900.00
USNAVY	COMPUTER SCIENCE AND TELECOMMUNICATIONS BOARD CORE SUPPORT	$915,000.00
NSF	FUNDAMENTALS OF COMPUTER SCIENCE - CHALLENGES AND OPPORTUNITIES	$600,000.00
USNAVY	NETWORK SYSTEMS OF EMBEDDED COMPUTERS/BROADBAND LAST MILE TECHNOLOGY	$702,700.00
NSF	INTERNET ADDRESSING AND THE DOMAIN NAME SYSTEM: TECHNICAL ALTERNATIVES AND POLICY IMPLICATIONS	$497,500.00
NATLAERO	TO #106: COMMITTEE ON RADIO FREQUENCIES	$413,400.00
USARMY	COMPUTING FRONTIERS: PROSPECTS FROM BIOLOGY	$684,000.00
NSF	AUTHENTICATION TECHNOLOGIES AND THEIR PRIVACY IMPLICATIONS	$300,000.00
USDHHS	CORE SUPPORT FOR THE ACTIVITIES OF THE COMPUTER SCIENCE AND TELECOMMUNICATIONS BOARD	$210,000.00
NSF	SUPPORT FOR THE CORE RESEARCH ACTIVITIES OF THE COMPUTER SCIENCE AND TELECOMMUNICATIONS BOARD	$240,002.00
USDHHS	TO #082: COMPUTING FRONTIERS: PROSPECTS FROM BIOLOGY	$100,000.00
SSA	AUTHENTICATION TECHNOLOGIES AND THEIR PRIVACY IMPLICATIONS	$50,000.00
USDOE	CO-SUPPORT OF A STUDY ON COMPUTING FRONTIERS: PROSPECTS FROM BIOLOGY	$48,569.42
ARCHIVES	STUDY OF THE PRESERVATION OF ELECTRONIC RECORDS (NARA)	$554,000.00
NSF	TELECOMMUNICATIONS RESEARCH DEVELOPMENT	$711,500.00
NSF	WIRELESS TECHNOLOGY PROSPECTS AND POLICY	$652,501.00
NSF	SUFFICIENT EVIDENCE? BUILDING CERTIFIABLY DEPENDABLE SYSTEMS	$345,602.00
COMMERCE	CORE SUPPORT FOR CSTB (NIST)	$80,000.00
AIRFORCE	CORE SUPPORT FOR THE ACTIVITIES OF THE COMPUTER SCIENCE & TELECOMMUNICATIONS	$32,500.00
USDOE	TO #23: SUPPORT OF A STUDY OF SUPERCOMPUTING SOFTWARE AND HARDWARE TECHNOLOGY	$800,000.00
USGAO	TO #2: CYBERSECURITY TECHNOLOGIES FPR CRITICAL INFRASTRUCTURE PROTECTION	$64,700.00
NSF	WHITHER BIOMETRICS	$777,471.00
NATLAERO	CORE RESEARCH ACTIVITIES AND STUDIES OF THE COMPUTER SCIENCE AND TECHNOLOGY BOARD	$60,000.00
COMMERCE	STUDY OF CYBERSECURITY, RESEARCH BY THE COMPUTER SCIENCE AND TELECOMMUNICATIONS BOARD	$280,000.00
USNAVY	SUPPORT FOR THE CORE RESEARCH ACTIVITIES AND STUDIES OF THE CSTB*	$423,171.00
AIRFORCE	CORE SUPPORT FOR THE ACTIVITIES OF THE COMPUTER SCIENCE & TELECOMMUNICATIONS BOARD	$32,500.00
COMMERCE	SPECTRUM MANAGEMENT POLICY REFORM	$121,700.00
JUSTICE	REVIEW OF TRILOGY (FBI)	$33,000.00
NSF	SUPPORT FOR THE CORE RESEARCH ACTIVITIES AND STUDIES OF THE CSTB*	$540,000.00
USNAVY	RESEARCH AND STUDIES OF THE COMPUTER SCIENCE AND TELECOMMUNICATIONS BOARD	$240,000.00
NSF	PARTIAL SUPPORT OF THE COMMITTEE ON RADIO FREQUENCIES	$562,000.00
NSF	A FRAMEWORK FOR UNDERSTANDING ELECTRONIC VOTING	$200,000.00
USDOE	COMPUTING FRONTIERS: PROSPECTS FROM BIOLOGY	$100,000.00
NATLAERO	TO #103: COMMITTEE ON RADIO FREQUENCIES	$628,409.00

*CSTB=Computer Science and Telecommunications Board

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

Dr. Leighton.

STATEMENT OF DR. F. THOMSON LEIGHTON, CHIEF SCIENTIST AND CO-FOUNDER, AKAMAI TECHNOLOGIES

Dr. LEIGHTON. Sorry. I will start over.

Mr. Chairman and Members of the Committee, my testimony today is based on my experience as the co-founder and Chief Scientist of Akamai Technologies. I am also a professor of Applied Mathematics at MIT and Chair of the PITAC Subcommittee on Cyber Security.

Akamai is the leading provider of content-delivery services on the Internet. Using sophisticated algorithms to coordinate computers in thousands of locations spanning 70 countries, Akamai distributes content and applications for thousands of websites to hundreds of millions of consumers worldwide. We serve each of you every day. One out of every five Global 500 companies and many government agencies, including the House of Representatives, rely on Akamai's services.

Akamai also provides the primary means of defense against cyber attacks for many key websites. When the FBI website was brought down on September 11, they turned to Akamai to help them restore service. On behalf of our customers, we fight a nonstop battle against cyber attacks that are increasing in sophistication and scale every day.

Like the Internet itself, Akamai evolved from an academic research project sponsored by DARPA. DARPA has a long and very successful history of funding basic research by the Nation's best computer scientists. But recently, DARPA has shifted IT funding away from basic research at universities in favor of classified work and/or more development-related projects.

If DARPA's current practices had been in effect in the mid-1990s, it is unlikely that the development of Akamai's technology would have taken place. That is because no other agency has stepped in to fill the gap created by the shift at DARPA. This is particularly evident in the area of cyber security.

Although DHS is tasked with providing security for the homeland, they spend less than two percent of their S&T budget on cyber security. And of that amount, less than one-tenth, a mere $2 million, is spent on fundamental research for cyber security.

Today, NSF has the only substantial civilian program for cyber security research, and it is seriously underfunded. In 2004, NSF funded just eight percent of the qualified research proposals in the area of cyber security. This is a factor of three less than the overall agency average. In IT overall, the funding rate is only 16 percent, an amount that has dropped by a factor of two over the last four years.

As a result of the decline in government funding for basic research in IT, we are now facing a serious lag in our nation's ability to continue to innovate, and at a time when innovation is most needed.

The need for innovation is especially urgent in the area of cyber security. Today, it is possible for a malicious agent to penetrate millions of computers around the world in a matter of minutes and

then exploit those machines to attack the Nation's critical infrastructure, penetrate its sensitive systems, or steal valuable data.

As we have documented in a recent PITAC report, cyber attacks are growing at an alarming rate, and they now cost the Nation billions of dollars annually. The financial sector is being particularly hard hit. New forms of electronic crime, such as phishing, pharming, and cyber extortion, unheard of only a few years ago, are now commonplace. Eighty-three percent of financial institutions reported compromised systems in 2003, a rate that doubled in just two years. And at least one percent of U.S. households fell victim to electronic identity theft at a cost of over $400 million in the first half of 2004.

Everyone is vulnerable. Today, a criminal can steal most any password that is used for access over the Internet. Beyond the economic repercussions, there are serious risks to our national security.

Today, virtually every sector of the Nation's infrastructure, including communications, utilities, finance, transportation, law enforcement, and defense, is critically reliant on networked IT systems, and these systems have very little, if any, defense against cyber attack. All elements of the Nation's infrastructure are insecure if the IT is insecure. And today, our IT is insecure.

Our national defense systems are also at risk, because the military increasingly relies on many of the same vulnerable IT systems as the civilian sector. This is one reason why it is vital that DARPA not ignore the civilian sector when allocating funds for cyber security research.

We are now just beginning to see the effects of a decades-long failure to develop the security protocols and practices needed to protect the Nation's IT infrastructure. Although the short-term patches and fixes that are the norm today can be useful in response to isolated vulnerabilities, they do not adequately address the core problems.

In order to make true progress against the core problems that plague our IT infrastructure, PITAC believes that fundamental research is required to develop entirely new approaches to cyber security. We recommend that the NSF budget for cyber security be increased by $90 million annually and that DARPA restore its historical role of funding basic, unclassified research in cyber security. We also recommend that DHS significantly expand its funding for cyber security research.

It is imperative that the Federal Government take action before the situation worsens and the cost of inaction becomes even greater.

Thank you.

[The prepared statement of Dr. Leighton follows:]

PREPARED STATEMENT OF F. THOMSON LEIGHTON

Chairman Boehlert, Ranking Member Gordon, and Members of the Committee, I appreciate the opportunity to testify this morning about *The Future of Computer Science Research in the United States.*

I am appearing today in my role as the Co-founder and Chief Scientist of Akamai Technologies. I am also a Professor of Applied Mathematics at MIT, a member of the President's Information Technology Advisory Committee (PITAC), and Chair of the PITAC Subcommittee on Cyber Security.

Although I will focus my remarks on the crisis this nation faces in the area of cyber security, the challenges we face with cyber security research are very similar to those we face with IT at large. Namely, there is much research that urgently needs to be done, little of which will be funded by industry. And, the current under-investment in fundamental research by the government could lead to dire consequences for the Nation.

Akamai is the leading supplier of content delivery services on the Internet. Using sophisticated algorithms to coordinate the operation of 15,000 web servers in 70 countries, Akamai distributes content and applications from thousands of web sites to hundreds of millions of consumers worldwide. We serve each of you every day. One out of every five Global 500 companies and many government agencies (including the House of Representatives) utilize the Akamai platform to distribute their content and applications over the Internet.

As part of our business, we provide the primary means of defense against cyber attacks for many web sites. When the FBI web site was brought down on September 11, 2001, they turned to Akamai to help them restore service. On behalf of our customers, we fight a nonstop battle against cyber attacks that are increasing in sophistication and scale every day.

Like the Internet itself, Akamai evolved from what was originally an academic research project sponsored by the Defense Advanced Research Projects Agency (DARPA). DARPA has a long and very successful history of funding research by the Nation's best computer scientists. But recently, DARPA has shifted funding away from fundamental research at universities in favor of financing classified work and/or more development-related projects.

If DARPA's current practices had been in effect in the mid-1990s, it is unlikely that the development of Akamai's technology, to improve the distribution of content and applications over the Internet, would have taken place. That is because no other agency has stepped in to fill the gap created by the shift at DARPA. This is particularly evident in the area of cyber security.

Although the Department of Homeland Security (DHS) is tasked with providing security for the homeland, including cyber security, they spend less than two percent of their Science and Technology budget on cyber security, and, of that amount, less than 1/10 (a mere $2 million) is spent on fundamental research for cyber security.

Although many agencies are concerned with cyber security, the National Science Foundation (NSF) has the only substantial program for funding fundamental research on cyber security, and it is seriously under funded. In 2004, NSF funded just eight percent of qualified research proposals in the area of cyber security. This is a factor of three less than the overall agency average. In the related area of computer science and engineering, the funding rate is only 16 percent, and decreasing. In fact, the success rate for NSF's Computer and Information Science and Engineering (CISE) Directorate proposals has dropped by a factor of two over the last four years.

As a result of the changes in government funding for basic research, we are now facing a serious lag in our nation's ability to continue to innovate, and at a time when innovation is most needed.

The need for innovation is especially urgent in the area of cyber security. Because of the great improvements in functionality and efficiency afforded by Internet technology, it has been incorporated into most every aspect of our society. Today, virtually every sector of the Nation's infrastructure—including communications, utilities, finance, transportation, law enforcement, and defense—is now critically reliant on networking technology.

Unfortunately, the revolution in connectivity afforded by the Internet has also dramatically increased the capabilities of those who would do harm. Today, it is possible for a malicious agent to penetrate millions of computers around the world in a matter of minutes, exploiting those machines to attack the Nation's critical infrastructure, penetrate sensitive systems, or steal valuable data. The growth in the number of attacks matches the tremendous growth in connectivity, and dealing with these attacks now costs the Nation billions of dollars annually.

We have included numerous statistics that document the rapidly escalating nature of the cyber security problem in the PITAC report, titled "Cyber Security: A Crisis in Prioritization." I will mention just a few here.

In the last half of 2004, over 7,000 different viruses and worms were released across the Internet. This is a 64 percent increase over the first six months of 2004.[1] Because of such viruses and worms, the percentage of computers that became in-

[1] Symantec, *Internet Security Threat Report,* March 21, 2005.

fected each month grew from one percent in 1996 to over 10 percent per month in 2003.[2]

These infected computers reside in our homes, offices, and schools. No computer is immune. Indeed, the networks of 40 percent of the Fortune 100 companies were so severely compromised in 2003 that they became the source of a spreading virus.[3]

Once infected, a computer can be reprogrammed so as to reveal confidential information to attackers, destroy or alter important data, and/or to carry out attacks against others. When infected computers are incorporated into so-called "bot armies," they can be used as platforms for launching unwanted spam or, even worse, denial of service attacks against critical infrastructure. In the first half of 2004, the rate at which newly-infected computers were incorporated into bot armies rose from 2,000 per day to over 30,000 per day.[4]

The use of bot armies to attack web sites has given rise to a new form of crime known as cyber extortion, in which the criminal will demand payment in return for not attacking a businesses' web presence. Although cyber extortion was unheard of just a few years ago, 17 out of 100 companies surveyed in a recent poll reported being the target of cyber extortion in 2004.[5]

The financial sector is one of many key industry segments that are being particularly hard hit by cyber crime. 83 percent of financial institutions reported compromised systems in 2003, more than double the rate in 2001. The use of phishing scams to direct unwitting citizens to fake web sites, whereupon they are tricked into revealing their passwords and other sensitive information is now rampant.[6]

In the last two months, a new and even more pernicious kind of attack known as pharming has become widespread.[7] Pharming is different from phishing in that it makes use of fundamental vulnerabilities in the basic protocols that are used to run the Internet. As a result, the attack is virtually undetectable, even by an experienced professional.

It is estimated that over one percent of U.S. households fell victim to electronic identity theft at a cost of over $400M in the first six months of 2004.[8] Everyone is vulnerable. Today, a criminal can steal most any password that is used for access over the Internet.

Beyond the economic repercussions, there are serious risks to our national security. Today, virtually every sector of the Nation's infrastructure—including communications, utilities, finance, transportation, law enforcement, and defense—is critically reliant on networked IT systems, and these systems have very little, if any, defense against cyber attack.

All elements of the Nation's infrastructure are insecure if IT is insecure, and, today, our IT is insecure.

Our national defense systems are also at risk, because the military increasingly relies on many of the same vulnerable IT systems as the civilian sector. This is one reason why it is vital that DARPA not ignore the civilian sector when allocating funds for cyber security research.

In response to the growing crisis, some have stated that if only the citizens at home and in small business would keep their firewalls and software patches up to date, we would be OK. While such safeguards are clearly necessary, they are far from sufficient. After all, if the most sophisticated and IT-savvy companies in the world are routinely falling victim to cyber attacks, how can we expect our citizens at home and in small business to fare any better?

Moreover, the problem is not just about ubiquitous software that is vulnerable to viruses and worms. The core protocols that form the underpinnings of the Internet were simply not designed with security in mind.

We are now just beginning to see the effects of a decades-long failure to develop the security protocols and practices needed to protect the Nation's IT infrastructure, and to adequately train and grow the numbers of experts needed to employ those mechanisms effectively. The short-term patches and fixes that are deployed today can be useful in response to isolated vulnerabilities, but they do not adequately address the core problems.

---

[2] ICSA Labs Virus Alerts; PITAC—February 2005 Report, *"Cyber Security: A Crisis of Prioritization,"* p. 10.

[3] Symantec *Internet Security Threat Report,* March 21, 2005.

[4] PITAC—February 2005 Report, *"Cyber Security: A Crisis of Prioritization,"*p. 10.

[5] 2004 poll by Carnegie-Mellon University—*InformationWeek;* PITAC—February 2005 Report *"Cyber Security: A Crisis of Prioritization,"* p. 8.

[6] Anti-Phishing Working Group *(www.antiphishing.org).*

[7] Anti-Phishing Working Group *(www.antiphishing.org).*

[8] Consumers Union *(www.consumersunion.org)*; PITAC—February 2005 Report *"Cyber Security: A Crisis of Prioritization,"* p. 9.

In order to make true progress against the core problems that plague our IT infrastructure, PITAC believes that fundamental research is required to develop entirely new approaches to cyber security. We recommend that the NSF budget for cyber security be increased by $90M annually and that DARPA restore its historical role of funding basic, unclassified research in cyber security. We also recommend that DHS significantly expand its funding for cyber security research.

The report goes on to describe ten specific research areas that are in the greatest need of support as well as specific recommendations to improve coordination of research efforts, to facilitate technology transfer, and to increase the pool of experienced researchers in the area of cyber security.

In summary, the PITAC finds that the IT infrastructure of the United States—and thus all other elements of our infrastructure that rely on IT, such as the electric power system, the government, and the military—is highly vulnerable to terrorist and criminal attacks. Fundamental research is urgently required to improve our defenses. It is imperative that the Federal Government take action before the situation worsens and the cost of inaction becomes even greater.

Thank you.

Appendix A

The Threat from "Phishing" and "Pharming"

(excerpts from: *The Arizona Republic*—'Pharmers' hit online bank users with fraud scam, April 22, 2005, by Jane Larson)

A new malicious cyber security crime is emerging that has serious ramifications for consumers, business, and even government agencies. The criminal act is called pharming—a play on "phishing," and another type of Internet fraud—that involves highly skilled hackers who secretly redirect users' computers from financial sites to the scammers' fake ones, where they steal passwords and other personal information. Even the Web address looks the same.

Unlike phishing, where users click on links in e-mails and are taken to fake sites, pharming intercepts a user on his or her way to the bank or credit-card firm. And it potentially can affect thousands of users at a time. Hackers are targeting small sections of the Internet and rerouting traffic to fake bank sites to capture users' passwords. The legitimate sites don't notice the drop in Web traffic because it is just a fraction of the total.

Criminals can 'pharm' data online with little or no knowledge by consumers. Even experienced Internet users can become victims and not know it. It is just a matter of time before the scam becomes widespread.

An anti-phishing bill introduced in Congress last month would also apply to pharming. It calls for prison time and fines for those caught either phishing or pharming.

Consider the following facts:

— Over 7,300 new Windows-based virus and worm variants emerged over the last six months of 2004. This is a 64 percent increase over the first six months of 2004. (Symantec)

— Over 2,600 active phishing sites were reported in February of 2005. (Anti-Phishing Working Group)

— 64 brand name businesses were targeted by phishing scams in January 2005. (Anti-Phishing Working Group)

— The United States ranks first among countries hosting the most phishing Web sites. (Anti-Phishing Working Group)

Pharmers have four main ways of operating: attacking a user's computer, attacking the large servers that find web sites for users, compromising the routing infrastructure, or by intercepting wireless communications.

The first way is to send virus-laden e-mails that install small software programs on users' computers. When a user tries to go to his bank's web site, the program redirects the browser to the pharmers' fake site. It then asks a user to update information such as log-ons, PIN codes or driver's license numbers. Scammers use the information to steal identities.

Other viruses, called key loggers, track a user's key strokes on legitimate sites and can be used to steal passwords.

The pharmers' second method takes advantage of the fact that Web sites have verbal names but reside at numeric addresses on the Internet. When users type a Web site's name into their browsers, Domain Name System (DNS) servers read the name and look up its numeric address so that users can get to the site.

Pharmers interfere with that process by changing the real site's numeric address to the fake site's numeric address.

The servers can belong to financial institutions, Web-hosting companies or Internet service providers. This tactic, called DNS poisoning, has been around for years, but it is only in the past six months that techies have seen it used for identity theft and dubbed it pharming.

The third way is by sending incorrect data to an Internet router, exploiting the fact that the Border Gateway Protocol (BGP) has no security. A hacker can then induce the router to send traffic to the wrong place.

The fourth method is to intercept wireless traffic. If a user is, for example, in a cyber/wireless café, a hacker can bring his own Dynamic Host Configuration Protocol (DHCP) server, intercept a wireless signal, and reply to an end user's Internet request prior to the response from the actual origin page. The hacker then takes over the session, and is controlling all communications.

What is alarming is that pharming can re-route many thousands of Internet users at a time, making the impact potentially huge. With phishing, you're scamming one person at a time; pharming allows you to scam a large group at once.

Pharming can also easily be evolved to impact businesses and military personnel, essentially collecting confidential data, and jeopardizing national infrastructure.

Appendix B

PITAC Letter to the President to Accompany PITAC Report on Cyber Security

[Note: The Executive Summary of this Report is included in the hearing charter.]

February 28, 2005
The Honorable George W. Bush
President of the United States
The White House
Washington, D.C. 20500

Dear Mr. President:

We submit to you the enclosed report entitled *Cyber Security: A Crisis of Prioritization.* For nearly a year, the President's Information Technology Advisory Committee (PITAC) has studied the security of the information technology (IT) infrastructure of the United States, which is essential to national and homeland security as well as everyday life.

The IT infrastructure is highly vulnerable to premeditated attacks with potentially catastrophic effects. Thus, it is a prime target for cyber terrorism as well as criminal acts. The IT infrastructure encompasses not only the best-known uses of the public Internet—e-commerce, communication, and Web services—but also the less visible systems and connections of the Nation's critical infrastructures such as power grids, air traffic control systems, financial systems, and military and intelligence systems. The growing dependence of these critical infrastructures on the IT infrastructure means that the former cannot be secure if the latter is not.

Although current technical approaches address some of our immediate needs, they do not provide adequate computer and network security. Fundamentally different architectures and technologies are needed so that the IT infrastructure as a whole can become secure.

Historically, the Federal Government has played a vital, irreplaceable role in providing support for fundamental, long-term IT R&D, generating technologies that gave rise to the multi-billion-dollar IT industry. The PITAC's review of current federally supported R&D in cyber security finds an imbalance, however, in the current cyber security R&D portfolio: most support is for short-term, defense-oriented research; there is relatively little support for fundamental research to address the larger security vulnerabilities of the civilian IT infrastructure, which supports defense systems as well. Therefore, PITAC urges changes in the Federal Government's cyber security R&D portfolio to:

- Increase federal support for fundamental research in civilian cyber security by $90 million annually at NSF and by substantial amounts at agencies such as DARPA and DHS to support work in 10 high-priority areas identified by PITAC.
- Intensify federal efforts to promote recruitment and retention of cyber security researchers and students at research universities, with an aim of doubling this profession's numbers by the end of the decade.
- Provide increased support for the rapid transfer of federally developed cutting-edge cyber security technologies to the private sector.
- Strengthen the coordination of the Interagency Working Group on Critical Information Infrastructure Protection and integrate it under the Networking and Information Technology Research and Development (NITRD) Program.

These actions will lead the way toward improving the Nation's cyber security, thereby promoting the security and prosperity of our citizens. We would be pleased to discuss this report with you and members of your Administration.

Sincerely,

Marc R. Benioff
PITAC Co-Chair

Edward D. Lazowska
PITAC Co-Chair

Appendix C

PITAC Executive Summary

(FROM FEBRUARY 2005 REPORT: CYBER SECURITY: A CRISIS OF PRIORITIZATION)

The information technology (IT) infrastructure of the United States, which is now vital for communication, commerce, and control of our physical infrastructure, is highly vulnerable to terrorist and criminal attacks. The private sector has an important role in securing the Nation's IT infrastructure by deploying sound security products and adopting good security practices. But the Federal Government also has a key role to play by supporting the discovery and development of cyber security technologies that underpin these products and practices. The PITAC finds that the Federal Government needs to fundamentally improve its approach to cyber security to fulfill its responsibilities in this regard.

Background

The Nation's IT infrastructure has undergone a dramatic transformation over the last decade. Explosive growth in the use of networks to connect various IT systems has made it relatively easy to obtain information, to communicate, and to control these systems across great distances. Because of the tremendous productivity gains and new capabilities enabled by these networked systems, they have been incorporated into a vast number of civilian applications, including education, commerce, science and engineering, and entertainment. They have also been incorporated into virtually every sector of the Nation's critical infrastructure—including communications, utilities, finance, transportation, law enforcement, and defense. Indeed, these sectors are now critically reliant on the underlying IT infrastructure.

At the same time, this revolution in connectivity has also increased the potential of those who would do harm, giving them the capability to do so from afar while armed with only a computer and the knowledge needed to identify and exploit vulnerabilities. Today, it is possible for a malicious agent to penetrate millions of computers around the world in a matter of minutes, exploiting those machines to attack the Nation's critical infrastructure, penetrate sensitive systems, or steal valuable data. The growth in the number of attacks matches the tremendous growth in connectivity, and dealing with these attacks now costs the Nation billions of dollars annually. Moreover, we are rapidly losing ground to those who do harm, as is indicated by the steadily mounting numbers of compromised networks and resulting financial losses.

Beyond economic repercussions, the risks to our nation's security are clear. In addition to the potential for attacks on critical targets within our borders, our national defense systems are at risk as well, because the military increasingly relies on ubiquitous communication and the networks that support it. The Global Information Grid (GIG), which is projected to cost as much as $100 billion and is intended to improve military communications by linking weapons, intelligence, and military personnel to each other, represents one such critical network. Since military networks interconnect with those in the civilian sector or use similar hardware or software, they are susceptible to any vulnerability in these other networks or technologies. Thus cyber security in the civilian and military sectors is intrinsically linked.

Although the large costs associated with cyber insecurity have only recently become manifest, the Nation's cyber security problems have been building for many years and will plague us for many years to come. They derive from a decades-long failure to develop the security protocols and practices needed to protect the Nation's IT infrastructure, and to adequately train and grow the numbers of experts needed to employ those mechanisms effectively. The short-term patches and fixes that are deployed today can be useful in response to isolated vulnerabilities, but they do not adequately address the core problems. Rather, fundamental, long-term research is required to develop entirely new approaches to cyber security. It is imperative that we take action before the situation worsens and the cost of inaction becomes even greater.

BIOGRAPHY FOR F. THOMSON LEIGHTON

Tom Leighton co-founded Akamai Technologies in September 1998. Serving as Chief Scientist, Dr. Leighton is Akamai's technology visionary as well as a key member of the Executive Committee setting the company's direction.

As one of the world's preeminent authorities on algorithms for network applications, Dr. Leighton's work behind establishing Akamai was based on recognizing that a solution to freeing up Web congestion could be found in applied mathematics and algorithms. Akamai has demonstrated this through the creation of the world's largest distributed computing platform that dynamically routes content and applications across a network of over 15,000 servers. Dr. Leighton's technology achievements at Akamai earned him recognition as one of the Top 10 Technology Innovators in *U.S. News & World Report.*

A Professor of Applied Mathematics at MIT, he has served as the Head of the Algorithms Group in MIT's Laboratory for Computer Science since its inception in 1996.

Dr. Leighton holds numerous patents involving cryptography, digital rights management, and algorithms for networks. During the course of his career, he has served on dozens of government, industrial, and academic review committees; program committees; and editorial boards. He is a former two-term chair of the 2,000-member Association of Computing Machinery Special Interest Group on Algorithms and Complexity Theory, and a former two-term Editor-in-Chief of the *Journal of the ACM,* the Nation's premier journal for computer science research. Dr. Leighton is a Fellow for the American Academy of Arts and Sciences, and is currently serving as Chair of the President's Information Technology Advisory Committee (PITAC) Subcommittee on Cyber Security. In 2004 he was elected into the National Academy of Engineering for contributions to the design of networks and circuits and for technology for Web content delivery.

Dr. Leighton has published more than 100 research papers, and his leading text on parallel algorithms and architectures has been translated into several languages. In 2002, Dr. Leighton was recognized by his alma mater as Princeton University's seventh Gordon Wu Distinguished Lecturer. He graduated *summa cum laude* from Princeton with a B.S. in Engineering. He received his Ph.D. in Mathematics from MIT.

DISCUSSION

Chairman BOEHLERT. Thank you very much, Dr. Leighton, and thank all of you.

Let me just clarify a couple of points, for openers.

We are not suggesting that DARPA is anti-university or against computer science, nor are we suggesting, Dr. Tether, that somehow the agency is going in the wrong direction that has been dragged into the ground. What we are suggesting rather emphatically—and there is more than one way to analyze the data—what we are suggesting is that there has been a trend at DARPA over the last five or six years away from certain kinds of research, and your charts verify that. And Dr. Wulf and Dr. Leighton pointed that out in their testimony. We need to have a discussion about the impact of that shift and what should be done about it across the Federal Government. What this is all about, what we hope to do, is come reasonably together about forging an overall policy, not about singling out a particular agency which has a long and distinguished record and sort of call the agency on the carpet.

But I am concerned, we are concerned collectively about the trends short-term versus long-term. Well, we will go beyond that.

Dr. Tether, let me get back to some of the data you showed in your slides.

I think we can have a good debate about whether DARPA has struck the right balance in its research. There really are two sides to that issue, and it is a question of balance to begin with. And I

think you have acknowledged that. But we ought to be able to agree on the facts about what you are funding.

According to the information that DARPA itself provided the Senate, that other body, as we refer to it here in the House, DARPA's computer science funding to universities dropped by 50 percent from fiscal year 2001 to fiscal year 2004. The charts you showed us talked about overall university funding, not just for computer science, and overall computer science funding, not just for universities. One can argue that the decline in funding for universities might be good or bad or indifferent, but do you acknowledge that DARPA funding has shifted? And that is what we are talking about, the shift in emphasis.

Dr. TETHER. Well, the shift in computer science at DARPA has been towards the cognitive side, which, by the way, no one, I don't think, anywhere would say is a near-term vision. Cognitive means having a computer that basically learns your habits and supports you. And as I said, Bill Gates said in response to the kids asking why should we go into computer science and what other adventures are there, that if we can make a computer software that learns that it will have the value of more than 10 Microsofts. Now that is a big deal. So yes, we did shift. We shifted into that area. We shifted away.

Now let me say one thing else that I would like with respect to what we are doing in cyber security.

The incident that I believe Tom was talking about is what was called the "slammer worm," which basically, in about, oh, I don't know, 10 minutes compromised over 90 percent of the computers on the Internet. Just two weeks ago, we built ourselves a computer test bed comprised of several hundreds of computers. And we use that to test out things. Just two weeks ago on that computer test bed, we let loose a worse-than-the-slammer worm and stopped it cold. Now we also let it loose without having our new technique on there, and it devastated that computer network in seconds.

Now this work, however, was classified. Now you might ask why on earth would we have that classified. Well, first of all, we took a worm that devastated the world and we mutated it into a bigger worm. I wouldn't want many people to know how to do that. Okay. We also came up with techniques to stop that worm, but we are still not done with those techniques, because if people knew what the technique was, they could design around it. So we are now in the process of basically that red team and blue team where now that we stopped that worm, the red team is now looking: we give them full knowledge of the technique. They are trying to come up with another worm that can destroy that technique, and so forth and so on.

And that is why we are keeping it classified until we fully—we understand that we don't want a short-term fix like he talked about. We want to find the fix that we can then put out in code that no one can reverse-engineer and protect the commercial market.

Now by the way, just as an aside, all of that was done through your Rome labs. That was the executor of that——

Chairman BOEHLERT. They are our Rome labs. I want you to have partial ownership, too.

Dr. TETHER. I am sorry. I forgot. I am sorry. Our Rome labs.

Chairman BOEHLERT. All right. Let me just add, look, that is a good story. And we all understand the need for classification. Good gosh. Every——

Dr. TETHER. Well, apparently some people believe that if it is classified it is not long-term research.

Chairman BOEHLERT. All right. I have got—let me ask Dr. Wulf and Dr. Leighton, if I may, to consume the rest of my time, and we will go to others for questions. Sort of comment on Dr. Tether's testimony. He is skilled. He is a master at this. And why don't I look about the rest of the story? And if you want to give a plug to our Rome lab, I would be glad to hear from you.

Dr. WULF. I have not had a lot of dealings with Rome in the last few years, but I had a lot before that. We had some joint research that we did with them, as a matter of fact.

The problem with the kind of approach that Dr. Tether is pointing out is that at any given point in time, there are about a half a million bugs in the Windows operation system. You only need one—to exploit one—to be able to compromise a system. Simply reacting to the slammer or a mutated slammer, all you have done is you have reacted to one way of potentially compromising the system out of potentially a half a million others.

As I testified before this committee before, we will not have secure computer systems based on the current models of security. They will not work. They will always have this problem. They are perimeter defense models, and they will always have the difficulty that there is a way to penetrate the perimeter.

Chairman BOEHLERT. Dr. Leighton.

Dr. LEIGHTON. Yes. Slammer was released in early 2003. It is one virus. In the last half of 2004, there were over 7,000 different viruses released into the Internet. The slammer virus, of course, is very interesting. It was not designed to attack, just to replicate itself. And when slammer was released, actually the Defense Department networks were the second most impacted network in terms of a failure to be able to route packets through the Internet. If the research on defending against viruses and worms is classified, that means that it won't be of use to the government, to the population, and to enterprises, and we will be defenseless if, indeed, they have discovered a way to defend networks against viruses and worms. And if they have, I would be very interested to see that technology. And I think our government would be very interested in having it deployed to protect ourselves. We are basically defenseless today against viruses and worms.

Dr. TETHER. I agree, and I would be very happy to actually show them what we are doing, but it does require classified information.

The slammer worm that was a—what we did with the mutation, just to get technical, was that we made it into a single packet worm so a signature detection couldn't detect the worm. And it was not just replicating.

We also did the hard test. We had an insider. In other words, this worm was released into the network pretending that there was somebody inside the network who let it go. So it wasn't coming through the perimeter. It was inside. And yeah, he is right that

that is the harder problem, because they will always get through the perimeter.

Chairman BOEHLERT. All right. Doctor, my time is up, and we could engage you in a very interesting discussion, but to draw upon my passion, baseball, for an analogy, you are looking at the box score, Dr. Tether, and you are talking about a home-run, and boy, we all applaud that. It is very important. But what about the Minor League system? And what about the rest of the system? And if we are not investing in long-term research, if the trend continues, and Dr. Wulf and Dr. Leighton share our concern, then we are not going to win championships in the future.

Dr. TETHER. I absolutely agree, and that is why I believe that we really need to concentrate on the feedstock, on getting those kids into high school who want to go into science and engineering. And if we can't do that, we are going to lose the ball game, because there is going to be nobody in the minor leagues.

Chairman BOEHLERT. You know, I have got a program up in Rome I want to talk to you about. The ACE program, Advanced Course in Engineering. If you haven't heard about it, then you should hear about it, and you should understand what we are doing with high school kids and college kids building that team.

But my time long ago was expired. But I tried to follow your lead, Dr. Tether, so—Mr. Davis.

Mr. DAVIS. Chairman Boehlert, thanks very much.

DARPA, Defense Advanced Research Projects Agency. That is a pretty powerful name. Indications of a lot of good things, perhaps, to happen. It started in 1958. The hopes, the funding of university research, this is an area where they could reach out and find funding that could provide the dollars needed for the research that has been a great deal, I think, for Americans. Certainly it has helped our economy, and the technology today that we see occurring, partially, and perhaps in many cases, is wholly because of the dollars that we have given to our universities for the research.

The question is for Dr. Marburger. It is really a two-fold question. Do you see the changing mode for federal support as a problem for maintaining a robust federal research investment in basic computer science research and since OSTP is charged with setting overall federal research priorities, are you taking any steps to try to offset the effects of the shift in funding behavior by DARPA by encouraging increased support by other civilian and federal R&D agencies, such as the Department of Energy and National Institutes of Health or the National Institute of Standards and Technology? Do I need to repeat those two questions?

Dr. MARBURGER. I think I can remember the gist of them.

Congressman, the fields of science are always shifting, and of course the shifting fields, where the work is done and the specific disciplines that are involved in moving ahead the frontiers of science require constant attention. That is why we have a new budget every year. We try to make budget requests that request funds for the agencies that we think are most appropriate for delivering on basic research and applied research in these shifting areas.

We do have mechanisms to do this. We coordinate the efforts in the information technology area through a robust interagency

working group and an office, a national office for the National Information Technology R&D program.

I mention that we actually move to begin implementing a recommendation from the PITAC Subcommittee on Cyber Security even before the report came out, and it is precisely in the area of increased coordination among different agencies that we began to act. I mentioned that in my testimony.

I think it is important for us to be responsive to the concerns that exist in the community, and I believe we have the apparatus there to do it. It is, as I mentioned before, it is a priority for the Administration, and we are acting to address that priority through our mechanisms.

Mr. DAVIS. Are you satisfied with the current priorities for basic computer science research across different agencies?

Dr. MARBURGER. That is a hard question to answer, because I am not completely aware of how those priorities get embedded in the specific programs at NSF, for example, in the Department of Energy and the Department of Defense, which are the major Departments that fund this kind of work. They are certainly concerned about it. I know that, because we talk with them all of the time, they have strategies for dealing with their mission needs in each of the areas in which we work closely with them. I am satisfied that there is adequate attention being paid in the agencies for this. Whether we are able to get the funds in the right places immediately as soon as people would like to have them there is another question. It is obviously in a rapidly-changing environment. We can't always move immediately to get the funds where we want them. I do believe that the requests that are made in the President's budget each year are appropriate for the levels of funding overall that are required to address this problem.

Mr. DAVIS. My time is about to expire, but let me reiterate my belief that one of the reasons that we have the strongest economy in the world today with perhaps less than five percent of the entire population of the world, the reason that if someone gets in trouble, the 911 number they call is really USA, is that we have provided dollars for research and development and that much of that success that we have has come from some of the research universities that we have in this country. And it is my hope that we realize from the Administration, from DARPA, that coordinated effort and that cooperation and the funding needs to continue at a level to where the future generations will see the America that we see it today. And I have some real concerns about research and development dollars. With all of the dollars that we spend, $2 trillion and some, that we are not doing enough research and development. And I think, excluding or using a part of the dollars in other areas, which appears to be what is happening with DARPA, and removing those dollars from our fine universities is probably not as wise a decision as I would like to see us be making.

Thank you for your testimony.

Chairman BOEHLERT. The Chair identifies with the remarks of the distinguished gentleman.

Mr. Rohrabacher.

Mr. ROHRABACHER. Well, first of all, let me congratulate DARPA for highlighting high school road warriors. I believe they are in my

district, so that was a great selection. Also, the selection of your site for your DARPA gathering in August happens to be very close to my district, and hopefully I will be able to join you there, so thank you very much.

This is a little frustrating to me, because, to be quite frank, people can use pious words to discuss things, and it sort of does not lead to a better understanding of what the reality is. It seems to me what we have here is not a decline in money for research for computers. I mean, Dr. Tether was very clear, the amount of money being spent for research on computers is actually on the upward trend. The question is whether we should channel the amount of money that is being spent on research into esoteric projects in the universities that may or may not ever come to fruition and help anybody versus actually spending money in developing ways to make sure people's lives are changed and bettered within a lifetime at least.

You know, when I first became the Chairman of the Subcommittee on Energy and Environment Research, we had to take a look at what was actually getting done with the amount of money that we were spending. And of course, nobody ever wants to try to prioritize around here and say what isn't working. They always want to say, "Give more money to us and we will, you know, spend it wisely," I guess. And I found out that we have been spending all kinds of money in various areas, but one area really stood out, and there had never been anything demonstrated that the money had been actually put to use for our benefit yet. And that was in fusion research. It seemed to me, after looking at that program, that we were spending more and more and more money over the years in fusion research. We have spent, I think, billions of dollars, but we didn't have anything to show for it after 20 years. Now is it inaccurate then to say if the Administration or someone would say, "Well, we should channel that money someplace else where it is actually being put to use that we are spending less money on energy research"? No. In fact, we weren't.

And let me get to the specifics on this. What I see this as, and what, Mr. Chairman, what I have seen today, in terms of the central argument, is whether or not money should be spent on basic and fundamental research that may never come to fruition or should we actually start channeling a little bit more of that money into developing the research necessary to develop some of these ideas that have been discovered through research in the past so that it actually changes our life somewhat. And I have no argument whatsoever with the approach that this Administration and Dr. Tether are taking, and I would congratulate them. I am the father of triplets, and they are one year and two weeks old today, and I think what you are doing is long-term, because what you are doing is going to make their lives better. And just channeling money, more and more money, into esoteric research at the university is not necessarily going to make their lives better.

And I thank you for that. And I can see that you are taking heat for it, Dr. Tether, today, and I want you to know that some of us understand that you are making very, very positive and, I would say, common sense decisions.

With that said, let me ask you about this. You were talking about computers, and that is supposedly why we are here today. You were actually criticizing; I will have to tell you, fellows, you have sort of a critical tone to your voice when Dr. Tether is talking about the research that he is doing, because after all, there are so many other areas. Isn't it better for him to be doing this research to try to fight—if he can't fight it for everything, isn't it good for him to find some sort of shield against a limited number of worms, even though there might be 7,000 other worms that he isn't tackling?

Dr. WULF. No.

Mr. ROHRABACHER. It is not? It is better for us to spend the money on some guy who is doing research that may or may not ever be applied anywhere?

Dr. WULF. I would be happy to get you references. I don't have them on the top of my head, but there have been any number of economic studies of what the social rate of return on investment in long-term basic research is, and they tend to run in numbers like 80 percent per year compounded. Okay. Yes, it is absolutely true. Long-term basic research is risky. It, by definition, is risky. We don't know what we don't know. Nonetheless, we wouldn't have the Internet, and we wouldn't have a lot of other very practical things had we not invested in that kind of long-term basic research.

Mr. ROHRABACHER. Didn't DARPA have something to do with the Internet?

Dr. WULF. It absolutely did.

Mr. ROHRABACHER. Right.

Dr. WULF. That was back in the days when they invested in people rather than projects.

Mr. ROHRABACHER. Let me ask, Dr. Tether. You just heard that big challenge there. The Internet. These guys are taking credit for long-term research money that was spent probably, what, I don't know—there was a lot of other money that was spent at the universities that never saw the light of day, but can we say that it was the basic research and not DARPA's developmental dollars that can be given credit for the Internet?

Dr. TETHER. Actually, there is probably enough credit for everybody, but let me tell you——

Mr. ROHRABACHER. Okay.

Dr. TETHER. Let me tell you, the way I understood it is that really what brought around the Internet was that at that time computers were very small. I mean, they were not very powerful, and the idea was, "Well, maybe we could net them together." And by netting them together, you get more out of them than just one computer. So a network was really created. This was a product. It was to put together computers, because we had problems to solve like air defense and so forth and so on.

Along with putting those computers together, the researchers were around the country. And some of them said, "You know what, I will just leave a message for that fellow, because he is on the West Coast, and he will pick it up in the morning." And that really was the genesis of e-mail. It wasn't that somebody was being funded to create e-mail, it was a fallout out of a product, out of a pro-

gram that was a development of making computers be netted together.

The same thing goes on today. I will go back to what we are doing today in computer science, and we are doing the cognitive computing, which is really so far out, you know. It is amazing to have these people say that this is near-term. I mean, I——

Mr. ROHRABACHER. I would agree with that. I mean, I have—Mr. Chairman, I want to emphasize that point. To suggest that the cognitive research and computers is short-term development——

Dr. TETHER. Well, they can have their opinion that maybe the money shouldn't go into cognitive research, that it ought to go someplace else, as you said, but to say that cognitive research is not short-term, and to say that if we can do it, it is not a major economic impact, I think is wrong.

Mr. ROHRABACHER. Okay. Thank you, Mr. Chairman.

Chairman BOEHLERT. The gentleman's time has expired.

Mr. Matheson.

Mr. MATHESON. Thank you, Mr. Chairman.

And I want to thank the Committee. It has been a very interesting hearing.

Dr. Wulf, I wanted to ask you a question. You testified before the Science Committee on cyber security issues in October of 2001. And at the time, you appeared to be worried about these issues. And you said that—and I am going to quote you. You said, "Our research base in computer security and network security is minuscule." And you also said that there has never been a funding agency that believed that it was its responsibility to develop the community of scholars researching this area and that because the resources are so scarce, the community gets very conservative, leading to what you called the Maginot Line model for cyber security.

Dr. WULF. The Maginot Line, yes, sir.

Mr. MATHESON. Maginot. Sorry. Now approaching four years since you made that statement to this committee, how do you feel today? Are you more upbeat about the state of cyber security research at academic institutions? And have there been any positive changes in this regard? And what do you see as the remaining challenges in this area?

Dr. WULF. Let us see. Thanks to this committee, Chairman Boehlert, there has been an increased emphasis on computer security. Again, I am talking about long-term basic research, because I don't believe that the fundamental model that we are currently using will ever produce secure systems, so we do really need the disruptive idea, the rethinking of the basics. As a consequence, there has been more money at NSF. NSF, under its current Assistant Director, has taken on that responsibility. Sure, he could use more money and that sort of thing, but the fact that they have taken on that responsibility, I think, is a very positive step forward.

It is still the case, unfortunately, that the research community, the collection of scholars, is still minuscule. When we testified here, what, three years ago now, four years ago, good heavens, we had an estimate that the number of Ph.D.s being produced per year was seven. We have done some counting since then. The estimates now are maybe 20. But it is still an incredibly small community. The largest conference in computer graphics attracts about 50,000

people. The largest conference in computer security attracts about 200. So it is still a very, very small community. And the argument I made then, and I would make again, is there ought to be more money, but actually the most important thing is predictability.

As I said in my testimony today, academics make their reputation in a career over decades. And if there is not some reasonable assurance that money will be there over that period of time, they will run.

Mr. MATHESON. Let me ask you, what are your views on the recommendations of the President's Information Technology Advisory Committee report on cyber security?

Dr. WULF. I am very pleased with the recommendations that they made. In fact, I think there was only one that wasn't really directly in my testimony of 2001, and that was for more coordination among the agencies involved, and that is obviously a very good idea.

Mr. MATHESON. In terms of that coordination, how do you see that being improved, or who should be responsible for that?

Dr. WULF. You know, the only way that really ever works is if all of the agencies see something in it for themselves. When we structured the High Performance Computing and Communication Initiatives in the late '80s and early '90s, we crafted a way to find a special niche for each of the agencies involved and gave them a responsibility for that. I think a similar sort of thing would be really advantageous here.

Mr. MATHESON. I think this issue is not going away.

Dr. WULF. No. No.

Mr. MATHESON. I would like to think that this committee would continue to have great interest in what we can do to improve efforts for cyber security.

With that, Mr. Chairman, I will yield back the balance of my time.

Chairman BOEHLERT. I think it is difficult for Dr. Marburger, for example, to respond to the question from Mr. Davis, I mean because of his position and everything. But I have to believe, in his heart of hearts, I have to believe all of the people involved in the science enterprise within the federal establishment are not satisfied with our investment in the science enterprise within the government. I don't expect you to respond to that. And boy, I would be the most surprised guy in the world if you could find anybody employed by the U.S. Government in a position of responsibility who can, with a straight face, say, "We are putting enough emphasis on the challenges in the area of cyber security."

And so Dr. Wulf, thank you so much. We have been talking about this for years. And seven to 20 is a big percentage increase, but boy oh boy, that is not nearly adequate to meet the challenge.

With that, the Chair recognizes the very distinguished Vice Chairman of the Science Committee, Mr. Gutknecht.

Mr. GUTKNECHT. Well, thank you very much, Mr. Chairman. I am not sure I deserve that, but I do want to thank the panelists for coming today. This has been a fascinating discussion. Especially, Dr. Tether, I loved your slide presentation. I only wish more Members of Congress could get a chance to see that. I have been an admirer of DARPA for a very long time, and I think part of the

reason was expressed by my colleague from California, and that is that it is very much a results-oriented endeavor. And I suspect at some level that does cause conflict among various academicians. I mean, they all have their own points of view in areas that they would like to pursue, but ultimately, I think DARPA is very much results-oriented. And I think that that is something that at least many of us on this committee appreciate.

Let me just add a little bit of grist to the mill here in terms of this whole discussion. I wouldn't call it a debate or even an argument, but a discussion about computer sciences. I think an important element that could have been included in your presentation is how the cost of computing systems, particularly supercomputers, have come down just dramatically. Just last week, I toured the supercomputer center inside the Mayo research facility at the Mayo Clinic in Rochester, Minnesota. They already have one supercomputer, and they are in the process now of acquiring and building what they believe will be the 14th fastest computer in the world. And the cost, I don't want to quote it, but it seemed to me infinitesimally smaller than the supercomputers that I saw just eight years ago at the University of Minnesota.

Another point I wanted to make, and as I say, I am not sure I have a good question here, but a couple of comments. One of the things that you had in your presentation, and I have been meeting with some scientists who have been working with the University of Minnesota on this whole issue of photonics. Now it is way over my head, but they put it in language good enough that I could understand most of what they were talking about. And I do hope it is something that DARPA will take very seriously, because I think there are enormous possibilities of this particular technology, assuming the physics is what they think it is, not only from a defense standpoint but I think from an economic standpoint. As I listened to their presentation, my eyes started to spin at all of the possibilities.

Finally, though, and I think this is a comment for all of you, and perhaps you want to comment on this, I am particularly pleased with this thing we call the Grand Challenge. And I really want to encourage all agencies, all science agencies, and all universities to look for ways to encourage, principally, I would say, high school students and their science and math and physics teachers to get more involved in these kinds of endeavors, because I think if there is one thing we need more of in the United States today, it is to get young people actively engaged in science projects. And so I think the Grand Challenge is a very important first step, but I hope it is not the last step. I hope we look for other ways to bring young people into this and get them excited about using some of the things that they learn in their classes in science and physics and others.

So not so much a question in any of that, but a comment. If you want to respond, you are more than welcome.

Dr. WULF. I would just say I couldn't agree more with your last point about the Grand Challenge. It just so happens that, I think, about five or six years ago DARPA asked the Academy of Engineering to do a study on these so-called "inducement prizes." This was before they had received the authority to do that sort of thing. We

did that study, and I became totally enamored of this as a way of provoking certain kinds of behavior. One of the things we learned, for example, that the typical winning team spends more money to win than they actually make with the prize. They are really after the bragging rights, not the money. And in fact, I liked it so much that I have, I think, talked a foundation into funding the Academy to do an inducement prize in the general area of sustainable development. And in fact, the first one we are doing is a contest like the contest that DARPA is doing on inexpensive removal of arsenic from drinking water, one of the real banes of existence of people around the world.

Dr. LEIGHTON. I would also like to, you know, second your recommendation.

As a high school student, I was an active participant in science fairs and so forth and it made a big impact on my career.

I would also like to mention that you mentioned the decreasing costs of the computing infrastructure, which has been vital to our economy. That is featured in the historic role of federally-supported R&D in creating billion-dollar segments of the IT industry. Programs like VLSI design, RISC processors, parallel computing and databases are critical to being able to lower the cost of computing. And university-sponsored basic research played a vital role in actually making that possible.

Chairman BOEHLERT. Thank you very much.

The gentleman's time has expired.

Mr. Sherman.

Mr. SHERMAN. Thank you, Mr. Chairman. It won't surprise you if my questioning focuses on DARPA and other U.S. Government efforts that will lead, whether they are intended to or not, to self-aware computers equaling or exceeding human intelligence. We are funding here an all-out effort to develop all kinds of new and advanced computer technology. However, I think we are maybe a couple of decades away from computers that are self-aware, independent, and deserving of a minimum wage. We are funding all of the technology to do more, and we refuse, as a Committee and as a Congress, to fund any research into do we want to develop a new independent intelligent lifeform on this planet. And secondly, we don't fund any research into how to prevent the computers that we are developing from self-awareness, independent motivation, or desire to go on strike for an even higher wage.

Now I have had a lot of correspondence with Dr. Tether, where he has assured me that all of this is just vague science fiction. But I would say that rare is it in science that our research exactly goes to where we were aiming. Often, we do less, we do more, and we do something different. And with science, it shouldn't surprise us at all if we hit something close to the target.

So let us take a look at the target. Now I get these letters saying not to worry, we are not really trying to do this. And then 10 minutes ago, my staff looked at your web page saying that it is your mission to develop a computer that knows what it is doing, will be able to reason, will learn from their experience, be capable of explaining themselves and talking naturally, or taking naturally-expressed direction, and will be aware of themselves and able to re-

flect on their own behavior. In other words, you are talking about a computer considerably smarter than my last opponent.

We are in the spin business. I know that the Administration and the science establishment doesn't want to fund research into whether we should create what I would refer to loosely as a silicon-based intelligent lifeform and does not even want to research the much more technical issue of how we develop higher and higher levels of computer capacity while deliberately engineering devices to make sure that we do not create self-awareness. I would point out that many of those who have thought about the issue of when will we know that computers deserve the minimum wage have described it as when you can have an e-mail conversation with a computer and not know whether you are talking to a computer or a human being. And DARPA's mission statement says you are aiming for computers that will be capable of explaining themselves and taking naturally-expressed direction.

So when you are dealing with Sherman with his concerns that you wish to allay, I get a letter saying not to worry. But when I look on your web page it is with the intention of developing a computer that will pass the test put forward by some as to when computers equal human intelligence, and that is to have a natural conversation, and as I say, able to reason, learn from their experiences, capable of explaining themselves, aware of themselves, and able to reflect on their own behavior. How many of us in this room could ask more of ourselves than to be self-aware and reflective? Will DARPA fund research, at least into how to prevent a computer with enormous computational capacities from achieving self-awareness and self-direction?

Dr. TETHER. Well, that might be one of those good university programs.

Mr. SHERMAN. How confident are you that if I support this effort that research with that as a goal will be funded?

Dr. TETHER. You know, when you sent your letter to me last year, I thought it was actually, quite frankly, a very thoughtful letter. I thought you brought up some good points. I didn't try to be flip in answering your letter. In the '50s, about 50 years ago, Turing came up with a test, and it was called the Turing Test, and that was if you could talk on the phone or whatever your mode of communication was and couldn't tell that it wasn't a machine, then it was alive, or artificial intelligence. That was the term. And in fact, that has been reached in a few cases, but when it has been reached, it has always been reached in a very narrow domain. You know, in fact, if you go on the phone company now and ask for information, you will most certainly be talking to a computer, and you can actually ask a lot of questions and get a lot of answers, as long as you can keep your conversation restricted to that domain.

Will we ever get to the point that—and I believe that we are going to have computers that are going to be very good in specialized domains, you know—that we'll actually be able to, in a specialized domain, communicate with a person in a way where the person might not realize that he is really talking to a machine? But the difference between that and a human is that a human can learn something in an area and then be subjected to a whole new

area that he has never been and be able to use that knowledge from that other area in a way that is mysterious. But that seems to be the difference between these computers that we are trying to build and a human being, that we can learn something and go to a brand new area, never having been there, and project somehow, that information.

I guess that is why I said earlier that I couldn't believe that anybody would call cognitive processing near-term. It is most certainly not. But it is important for the Department of Defense, in fact, it is probably important for the U.S. economy, to be able to get that capability.

For the Department of Defense, it is important for the following reasons. Let us go to network security.

If you go to an area, you will find that the reason that networks are vulnerable are usually because people don't put them together correctly. When they set them up, they make an error. They make a mistake. And what you really want to have is a computer system that can do that for you.

Mr. SHERMAN. Dr. Tether, I haven't even questioned whether cognitive reasoning and incredible computational capacity and all of the ability to reason in a computer would not be an incredibly valuable thing for our country, for our world, and for our Defense Department. What I have asked you, though, is two questions. Will you fund research into how to make sure that no matter—I will—make sure is too strong of a word, how to increase the likelihood that a computer with tremendous cognitive ability, if you want to use that term, a tremendous computational ability does not have self-awareness, self-direction, and that is the one question?

Dr. TETHER. I will tell you what I will do. Quite frankly, I think it is an interesting question. I will, and I believe it actually is one of these questions that somewhere in the university we ought to have that done. Yes, I will.

Mr. SHERMAN. Thank you.

Dr. TETHER. We will see what happens. It will be interesting to. I will try to formulate that question in a way that I—it is a little—I must admit, it is a little counterculture for us to say, "Tell us how to not do this," but that is an interesting question. And I will try to—I will do that. I will——

Mr. SHERMAN. The engineers that developed engines developed governors and developed brakes.

Dr. TETHER. They did. They did.

Mr. SHERMAN. And you wouldn't want to be an automotive engineer without knowing how to——

Dr. TETHER. I promise you, I will do it. I will——

Mr. SHERMAN. Thank you.

Dr. TETHER. At least I will make an attempt to have somebody do it for us. Okay.

Mr. SHERMAN. Thank you. I look forward to working with you.

Chairman BOEHLERT. Thank you.

The gentleman's time has expired.

Ms. Biggert.

Ms. BIGGERT. Thank you, Mr. Chairman.

I think I will go back to computer science in general.

But how can we determine if federal funding is adequate? Dr. Marburger, you mentioned a 33 percent drop in DARPA's funding in NITRD. Was there debate over whether that was appropriate? And do other agencies need to pick up the slack? And are they doing so?

Dr. MARBURGER. The NITRD budget is a composite of budgets from each of the agencies, and we only get the information about these numbers after the budget is already out. We do produce a supplementary report associated with the budget request each year that has these numbers in it, but they are a composite of decisions that are made in the agencies.

Now when we see the amounts that are actually out there, then we bring the agencies together, through the coordinating committees that we have, and discuss what the significance is of these numbers, and try to identify holes and strategies for making the requests in the following budget year. That is how it works.

So that obviously leaves room for fluctuations in programs that are unexpected. But in general, we try to have communication among the agencies so that they are aware of impacts of decisions that one agency might take on the others.

Ms. BIGGERT. Well, but then you see the numbers and see that DARPA has dropped their funding. Is that a problem, or do other agencies then up the amount of money that they are going to put into something?

Dr. MARBURGER. We have conversations all of the time about how the agencies will fulfill their missions and the priorities that they establish for them. I am going to ask Dr. Tether to say a word about that at this point.

Dr. TETHER. Let me first say that Dr. Marburger does a great job. You know, he calls us into hearings, and sometimes we say, "oh, we are busy," and he says, "There is still going to be a hearing," and we do eventually go. And we talk. And we do do a lot of talking. He really does a great job.

Now on the budget that he is talking about, unfortunately, it is not really fair to say that we dropped IT that much because it is an accounting problem. The way the crosscuts are, the money that we put into cyber security, for example, which are all IT, are not included in that cut, because it is included in another OMB cut. The amount of money that we put into microelectronics and things like spintronics, which is making the brand new memories for the future, which again you would think would be IT, are not included in that number he gave, because it is another OMB cut, and OMB did not want us to take the same dollar and have it show up three places. And so unfortunately, what you have is a decrease, which if I were to add all of the IT that I also provide to these other two organizations, they would not—it would not have shown that much of a drop.

Ms. BIGGERT. But was that in the previous year? I mean, if you have a drop there, with the dollars that you have got in that funding, it still is a drop. Something has been cut out of it.

Dr. TETHER. Well, the problem is that the comparison is over years where these other programs are brand new programs, so they wouldn't have appeared in the first category. I really can't say. I am trying to actually, because of this controversy over this drop,

do exactly what you are asking, try to get a true apples-to-apples comparison, forget what OMB tells us to do, God bless us, you know, but we will add up——

Chairman BOEHLERT. I wish you had that luxury.

Dr. TETHER. We will add up IT apples to apples and see what it turns out to be. But, by the way, we have lots of conversations about this subject. And I wish we knew, I wish we had an algorithm out of which would spit out exactly how much funding should go into a particular discipline. I mean, I really wish we had that.

Ms. BIGGERT. Will you make that available to us, then?

Dr. TETHER. Yes, I will.

Ms. BIGGERT. Thank you.

Thank you, Mr. Chairman.

Chairman BOEHLERT. Thank you.

Ms. Jackson Lee.

Ms. JACKSON LEE. Thank you very much, Mr. Chairman. This is an important hearing, as a number of our hearings have been, as we have focused on some of the deficiencies in the oversight responsibilities that we have.

I would like to focus my remarks, and I would ask unanimous consent, Mr. Chairman, to put my total opening statement into the record.

Chairman BOEHLERT. Without objection, so ordered.

Ms. JACKSON LEE. Thank you.

I would like to just focus my remarks on the perception that I have, and that is that we are in trouble, frankly, and I am not sure if we are going to dig ourselves out of the hole. I think we are in trouble because we are not creating a legion, an army of new technocrats. I recall some years ago when every graduating senior was talking about being a computer scientist. Unfortunately, the thrust of that computer scientist or doing computer work was working on computers. It really had nothing to do with creating new technologies. It certainly had nothing to do with software technology, which at that time we were very proud to have focused in the Silicon Valley. Even now, we are draining the resources out of that particular region, and much of our work is finding itself offshore in places like China.

I happen to be holistically concerned about the world's upliftment, but I would also argue that it has always been the United States' ability to survive to be at the cutting-edge.

I cite as a premise, or one of my premises, the work of Vinton Cerf and Robert Kahn that was noted in "An Endless Frontier Postponed," in *Science,* Volume 308, May 6, 2005. It specifically notes that in June, these scientists will receive the A.M. Turing Award from the Association for Computing Machinery based upon their creation in 1973 of the language of the Internet. Where would we be if we did not have the language of the Internet? Twenty years later, the Mosaic web browser gave the Internet its public face. This, of course, had some basis in our public funding. And of course, DARPA was organized—it funded TCP, but the Soviet satellite Sputnik in 1957 led to the creation of DARPA, a very important agency, and it has been on the cutting-edge. U.S. IT research grew largely under DARPA and the National Science Foundation.

So if we are underfunding our university research, and I cite for you the numbers that may have already been cited, but I want them in the record. Between fiscal year 2001 to fiscal year 2004, DARPA support for university-based, non-classified research dropped by order of 40 percent from $214 million to $123 million. The Internet research that these two gentlemen will be honored for, as I understand, was not military-classified research, and therefore, here lies my angst.

If you look at the number of potential scientists in this area or in the area of physics, chemistry, and other areas, we know that our numbers are going drastically down. We also know that we are suffering because of a lack of technology. I will give you one example. In talking about securing America and cargo screening, simple screening of cargo in airplanes, right now we screen every single suitcase of a traveling passenger on an airplane. We do not screen cargo. That raises a great outcry, and of course, the easy response is, "Go screen cargo." It makes sense. But in fact, we don't have the technology to be able to screen cargo. A sad state of affairs.

In fact, I think the very infrastructure and underpinnings of Homeland Security is technology. One, when we speak about improving our security at the borders, we talk about technology, the new types of screening technology. When we talk about securing, if you will, various documents, we talk about cyber security and the vulnerability of that.

So my general question would be aren't we in a mess. And how do we get out of that mess? Where are the advocacy groups to demand? You know, the National Science Foundation has its public underpinnings, fearful of any misstatements to go contrary to Administration policies, no matter what the Administration might be. It might be Democrat or Republican or otherwise. Where are the voices to suggest that we are not training a whole battalion of scientists to come forward, and computer science happens to be uniquely situated? You don't have the high school students taking physics. And I have heard some questions about we should—or some comments of what we should be doing, but it is going to take money.

So maybe I could just get one response from that. My time is out, but I think we are in a mess, and it is hard to dig out of it, and I really don't hear any voices being provocative and thinking out of the box.

I yield back. If there is someone who wants——

Chairman BOEHLERT. Well, the gentlelady's time is expired with her initial summary of events, but we will ask the witnesses. She has restated something that we are all vitally concerned about and all working, hopefully, to address.

Who wants to respond?

Dr. Marburger.

Dr. MARBURGER. Let me say a few words about this. There is no question that the world is changing rapidly, and nations that formerly did not have the capacity to participate in a technology-based economy are acquiring that capacity very rapidly. And the rates of change are very impressive, and they are to be taken quite seriously, which is why we really have to tune up our own prior-

ities as a Nation. And certainly computer science and cyber security are among those priorities.

The situation is not as gloomy as it seems, and some of these dramatic rates of change have to be put in perspective. The absolute numbers of scientists in these developing countries are much smaller than in the United States, for example. We should welcome the emergence of new economies that can participate in our own trade and help us to resolve problems of society.

But there are some good stories here, and as a result of efforts that Administrations have made, the number of high school graduates that take a physics course is, in fact, going up. It has not been going down. In a decade, it has increased from about one-fourth of all high school graduates to about—to more than one-third of all high school graduates. So the numbers of scientists are going up. It fluctuates with the kinds of programs that we have or the prospects for jobs in these areas, but the indicators are, by no means, as universally bleak as we hear. That does not mean that we should not take these issues lightly. We must continue to support the areas that we know our economy in the future depends upon.

Thank you.

Chairman BOEHLERT. Thank you very much, Dr. Marburger, but Ms. Jackson Lee is absolutely right with the general thrust of her comments. I mean, this glass is not half full. And when the NSF education directorate, for example, is being asked to absorb a rather substantial cut, we sort of think that some people have priorities wrong. And so we are trying to address a wide range of subjects.

And in response to Mr. Rohrabacher's earlier comments, I would point out that one of the long-range investments we need to make as a Nation is do a hell of a lot better than we are doing in K–12 science and math education, because all of you are not going to get what you need in the future to do what we demand of you and expect of you unless we start at the beginning. So the whole science enterprise, as I refer to it, requires more investment. And we are not just throwing money at things. And it is naive to suggest that any investment in long-term research—the investors have every right to expect that every dollar invested is going to produce immediate significant results. I mean, that just defies basic logic when you are dealing with research matters.

But let me ask just——

Ms. JACKSON LEE. Mr. Chairman, would you yield for just one moment?

Chairman BOEHLERT. I will for one moment.

Ms. JACKSON LEE. All right.

I appreciate Dr. Marburger's comments, and when I say bigger and better, I don't suggest, Mr. Chairman or panelists, that we should be arrogantly bigger and better. But one physics course is good, but it is not cutting-edge technology. That is what I am fearful of is that we are losing that, and I hope that we can be working toward that effort collectively.

Chairman BOEHLERT. Thank you.

Ms. JACKSON LEE. I yield back.

Chairman BOEHLERT. Thank you very much.

What I would like to do to wrap up is say, Dr. Tether, you feel we have sort of backed you into a corner. That is not our goal at all. But let me ask Dr. Wulf and Dr. Leighton, what isn't DARPA doing now that you think they should be doing? Give us some guidance.

Dr. LEIGHTON. Well, I would like to start in the area of cyber security. DARPA has, by and large, withdrawn the bulk of their funding for university research in the area of cyber security. And I think you can see the explanation of that in page 16 of Dr. Tether's written testimony where it is documented in the various areas in computer science, at large, what has happened there. And part of that is through classification. And I think, you know, a great example is the work that Dr. Tether quoted from Rome labs in trying to contain a virus that was released two and a half years ago.

If, indeed, DARPA can discover a way to stop the spread of viruses, that is vital technology for the government to be able to use just to defend itself and for enterprises and our companies and our schools and the people at home to defend themselves. If it is classified and not going to be released to the general public to be able to defend themselves, then one can question the value of the research. And if the concern is that by releasing it the bad guys are going to find a way around it, then one questions the value of the research in the first place, because if you can't actually use it to defend yourself because you are worried the bad guys are going to get around it, then it wasn't a very good thing to do. And it is vital, I think, to have the university researchers who are, in some ways, in the best position to develop entirely new approaches to cyber security, which our Internet and our IT network systems need.

And I would also like to say, it is not just viruses and worms. The fundamental protocols that make up the Internet, the domain name system, which is the equivalent of the 411 service, BGP, which routes your packets in the Internet, they have no security at all. I could pretend to be a bank. I can steal your banking passwords today without you having a clue that I have done it. It is called pharming. And there are many different ways to do pharming today. And you will see, I think, an increasing number of articles in the paper of just more and more people that have their identity stolen. And so I think university research plays a critical role in the long-range thinking about how do we start over again with the Internet in the same way that you see university research having an impact on lowering the cost of computing or developing the Internet. And in the past, these efforts were funded by DARPA as part of a basic research program at universities in computer science, and that is what is changing. And that is what is causing the problem.

Chairman BOEHLERT. Dr. Wulf.

Dr. WULF. I have two points, just one very briefly on classification.

In the computer security, cyber security research domain, there is a phrase that you will hear a lot. That phrase is: "There is no security in obscurity." That is, if you are depending upon something not being known, that is itself a vulnerability, which can be a very, very serious one.

So, for example, in all of the work on cryptographic algorithms, the method of cryptography is published broadly. It is only the key that you have to depend on. So if it is necessary to classify some of this material, I can see classification, by the way, for offensive techniques. But if it is necessary to classify defensive techniques, they are probably not very strong techniques.

Chairman BOEHLERT. Look, let me just ask you something else, and Dr. Tether, I will give him a chance, but is it just a question of more funding? Because I can guarantee you what Dr. Tether requested as it worked its way out was a hell of a lot more than he got, and justifiably so. He can justify and make a good case for a number of items that he had requested money for that were stricken from the request. So that is the reality of dealing in this town in the whole budget process.

So is it just getting more money, or is it—do you suggest that maybe some investments are made in areas that you would assign a lower priority to and take those resources and put them in areas that you think are deserving of a higher priority?

Dr. WULF. That is, in fact, exactly the second point that I wanted to get to.

It is not just more money. It also has to do with the style of funding. Now this may sound nostalgic or something like that, but when I was being funded by DARPA—ARPA, actually, back in the '70s and early '80s, DARPA made very long-term agreements. Certainly they monitored what we were doing, but they understood that results might not occur for five years, 10 years. The style that ARPA has—DARPA has gone to more recently are very short-term contracts and require demonstrable deliverables every 12 months. That, no matter what the amount of money, builds in a short-term focus that—well, I just think we are missing about——

Chairman BOEHLERT. Thank you.

And in all fairness, and I don't mean to get in point/counterpoint, but Dr. Tether, who we value very highly as a resource to this committee, we want to give you a chance to comment on that observation.

And then I will wrap it up with a final question to Dr. Marburger about the future of PITAC.

Dr. Tether.

Dr. TETHER. Okay. Let me—I have two comments.

One is on these so-called deliverables. They are really not deliverables. What we do in our programs, they are really long-range programs. What we do, what our program managers do, is we ask them to say okay, what is the first thing that has to be true in order for this, whatever you are doing, to happen? And then what is the second thing? Because there is no sense spending money on the second thing if the first thing is not going to be true. And we have them lay out a program over many years that has these gates that have to be passed. We call them go/no-gos, which I think frightens some people. But it is a little bit to me like what is happening at universities is that you go in as a freshman and you spend four years, give them your money, and you get a degree and never had to take an exam. You never had to show that you had the knowledge to pass Physics 1, and that is a go/no-go. That

is all we are really talking about here is a way to measure progress. And that progress is being put together.

Now we have our 6.1 program, which is what he is nostalgic about, which is the basic research, which is just really done with grants. And with these grants, you typically give somebody a couple years, two or three years of money. You don't say, "Write if you get work," but it really is somewhat unfettered research. And that money is a small amount of the DARPA budget, and always has been a small amount of the DARPA budget. You saw what I have, about $150 million in 6.1, and $90 million of that goes to universities. And it goes in the form of grants.

The rest of the money, the other $450 million going to universities is really in creating products. And when you get into the creating products business, or the demonstration business, it is not unreasonable to have somebody tell you, "What is your plan? How are you going—what are your metrics? How are you going to measure yourself to know that you are making progress?" And that is what these so-called deliverables are about. These are negotiated between us and the person doing the work. Now if they don't want to do that, then they shouldn't try to get into the 6.2 or 6.3 arena, because that is a different arena than the normal universities.

Now the second thing. You know, I don't get any actionable information from these guys. I get a wringing of hands that the money is going down, but not one person has ever clearly defined, and you asked for it, the specific research that is not being done, the problems that are not being solved, or the progress that is impeded. Not one of them is saying, "Look, you are not funding me, and I was on the verge of creating the unifying theory of computer science." All of the people that you hear complaining are only complaining because they are not being funded, but they are never telling you what it is that they want to do, other than get the money.

Chairman BOEHLERT. Well, we could be engaged all afternoon in this subject, but we will ask specifically from Dr. Wulf and Dr. Leighton, for the record, and we would ask for a timely submission, in response to the challenge that Dr. Tether has rightfully advanced.

Dr. TETHER. And not say that it is classification that is the problem. I want to know the problem that they want to work on that if they got the money, and the only thing stopping them is getting the money, to work on a specific problem that they can do it, it would be fantastic. And it could be something that could take 20 years. We are used to that, because I will tell you, Mr. Sherman, you know, I don't know what he is worrying about, but he doesn't have to worry about the cognitive research that we are doing achieving what he is worried about in a long time.

Chairman BOEHLERT. Well, I think Dr. Wulf and Dr. Leighton are up to the challenge, and so you will respond to the challenge offered by Dr. Tether, to him and a copy to the Committee, please.

And Dr. Marburger, what about PITAC? Are you going to renew it?

Dr. MARBURGER. The PITAC charter is up shortly, and there is a process for examining all Presidentially-appointed Advisory Committees that has begun, and it is in process, and that is about all I can say at this point.

Chairman BOEHLERT. What about your gut feeling right now?

Dr. MARBURGER. Well, Mr. Chairman, as the President's Science Advisor, I don't have just gut feelings. I try to speak from best knowledge, and I would prefer not to second-guess the President on any Presidentially-appointed committee.

Chairman BOEHLERT. I see. But what about—what—it is in statute, counsel points out. PITAC is in statute.

Dr. MARBURGER. Yes.

Chairman BOEHLERT. So you are saying your authority, statutory authority expires on a date certain, and then what? You are going to have a recommendation from the Administration whether——

Dr. MARBURGER. Right.

Chairman BOEHLERT.—to renew, and that will require a new statute?

Dr. MARBURGER. I am not sure about the legal status. I am aware that there are usually long delays and times associated with reconstituting Presidential Advisory Committees. And in response to legislation and to statute, the President usually does this through a series of Executive Orders, and the Executive Order under which the current PITAC has operated is due to expire, and a new Executive Order is required. And that process of generating a new Executive Order, deciding what the content of it will be and so forth, it is taking place.

Chairman BOEHLERT. We are confident that you will give the President the benefit of your best judgment.

Dr. MARBURGER. Thank you.

Chairman BOEHLERT. And with that, let me say thank you to all of you for appearing here today. Pretty darn important subject matter. The room should be filled to capacity, and the press corps should be here, you know, weighing every word you are say, because what we are talking about is very, very important, and so thank you for what you do so well. And continue the good work. And we will continue the relationship we have. We are partners in this venture.

This hearing is adjourned.

[Whereupon, at 12:15 p.m., the Committee was adjourned.]

Appendix 1:

Answers to Post-Hearing Questions

ANSWERS TO POST-HEARING QUESTIONS

Responses by John H. Marburger, III, Director, Office of Science and Technology Policy, The White House

Questions submitted by Chairman Sherwood L. Boehlert

Q1. You said at the hearing that the NITRD budget is a "composite of budgets from each of the agencies, and we only get the information about these numbers after the budget is already out." This statement implies that there is no active planning process that considers overall NITRD goals in determining individual agency budget allocations. Is this the case? If not, was there debate over whether DARPA's 33 percent drop in NITRD funding (over the last five years) was appropriate? Do other agencies need to pick up this slack, and are they doing so?

A1. Agencies determine their budget requests for R&D in NITRD Program areas after close interagency coordination through a series of formal and informal meetings of Coordinating Groups, Interagency Working Groups, and the NITRD Subcommittee itself, many of which OSTP oversees or participates in. This process involves setting federal priorities for IT R&D, determining agency priorities within these, and coordinating federal spending to ensure that the priorities are met. However, as I stated, the specific agency spending levels reflected in the President's Budget are not finalized until just prior to its release, and therefore the complete, final details of the budget for the NITRD Program are not available until then.

The level of DARPA funding that falls within the NITRD Program reflects the evolution of DARPA's priorities, and an increasing emphasis on interdisciplinary R&D. This emphasis on interdisciplinary R&D for tackling important defense-related technological challenges evolved over the last five years while being shaped by the NITRD interagency planning and coordination process. The growth in the overall NITRD program budget during that period demonstrates that the NITRD Program agencies continue to address the Federal Government's priorities for information technology R&D.

Q2. What impact is DARPA's reduced support for computer science research having on the Federal Government's ability to meet its overall objectives in information technology?

A2. The overall NITRD Program budget grew from $1,928 million in 2001 to the budget request of $2,155 million in 2006. That this happened during a tight budget climate demonstrates that information technology R&D continues to be a priority for the Administration. The Federal Government continues to invest in the R&D needed to meet its overall objectives in information technology. However, at the same time, DARPA has been investigating new R&D topics, including some that are not necessarily central to the NITRD focus areas and that may lead to future discoveries that could unlock unexpected areas of future computer science investigations. The IT R&D investments at DARPA and the other NITRD agencies provide a healthy mixture of types and topics of research that will contribute to broad advances across a wide range of science and technology.

Q3. What criteria should we be using to determine if federal support for fundamental research in computer science in general and cyber security in particular is adequate?

A3. The determination of what is "adequate" depends on one's perspective. Federal agencies generate their budgets in the context of their overall mission and develop priorities that are consistent with that mission. Adequacy is thus judged in light of meeting mission needs. From the standpoint of the broader S&T portfolio, we must balance new and emerging research areas with currently productive ones, which can result in different trade-offs.

While we don't have specific criteria we can use to set funding levels for our research investments, in general we ask if overall S&T funding levels are reasonable and balanced, if a large share of research proposals are proposed competitively and are awarded in a merit-reviewed process by technically qualified reviewers, if agency missions determine the funded projects and levels, and if agency management and oversight processes lead to the performance of high-quality research. These standards have been used in the formulation of the President's Budget Request.

More specific to computer science and cyber security, we consider many factors including protecting infrastructure, safeguarding commerce, and preserving privacy, but what is "adequate" remains a fundamental question, particularly with such a dynamic system, where the threats constantly evolve and adapt.

Question submitted by Representative Dave G. Reichert

Q1. The Advanced Scientific Computing Research (ASCR) program provides the Department of Energy (DOE) with world class scientific computation capabilities and high-throughput networking research. The ASCR program is a multidisciplinary effort involving teams of mathematicians, computer scientists, and application area scientists working to develop new scientific simulation codes, technologies, and the networking capacity required to fully exploit the next generation of Leadership Class Computing resources.

One rapidly emerging mission need is cyber security. Cyber threats are becoming increasingly malicious, and regularly outpace the protections that can be put in place using the current "border-based" cyber security model. There is an urgent need for aggressive design and implementation of novel integrated cyber security systems that would coordinate both protective and response measures. Development of such architecture will require close cooperation between researchers and operational cyber security personnel to build an effective, layered approach that is tested and vetted in an operational environment. DOE's national laboratories provide an ideal environment to conduct such a cyber security program to develop solutions for both the classified and the open science communities, but current funding may be insufficient to initiate a cyber security effort adequate to this challenge.

Dr. Marburger, do you agree that the DOE's Office of Advanced Scientific Computing Research should create cyber security research testbeds at its national laboratories? Pacific Northwest National Laboratory (PNNL), in my home State of Washington, is an ideal site for such an undertaking.

A1. While cyber security research testbeds are an important component of the overall cyber security R&D activities for the Federal Government, there is already a significant investment across federal agencies in such testbeds, including DETER (Defense Technology Experimental Research) and EMIST (Evaluation Methods for Internet Security Technology), both jointly funded by DHS and NSF; ISEAGE (Internet-Simulation Event and Attack Generation Environment), funded by the Department of Justice; and another cyber security testbed for emulating current and legacy industry environments at the Idaho National Laboratory. This Department of Energy testbed has synergies with other testbed activities at the Laboratory, including a wireless testbed, a SCADA testbed, and the Critical Infrastructure Test Range. Additional investments in cyber security testbeds must be weighed against other important cyber security priorities.

Questions submitted by Representative Bart Gordon

Q1. The President's Information Technology Advisory Committee (PITAC) report on cyber security finds the current federal effort unfocused and inefficient because of inadequate coordination and oversight. The PITAC's upcoming report on computational science, according to preliminary reports from the committee, faults the federal interagency Networking and Information Technology R&D program for placing too much focus on incremental and tactical planning rather than on strategic planning.

What is your response to these findings, and do you see a need for changes to refocus and improve the interagency planning process for information technology research and development?

A1. The current interagency coordinating body for cyber security R&D is the Critical Information Infrastructure Protection Interagency Working Group (CIIP IWG), which reports to the Infrastructure Subcommittee of the NSTC. The PITAC report concluded that the federal coordination of cyber security R&D would be more focused and more efficient if a coordinating group were formed under the Networking and Information Technology R&D (NITRD) Subcommittee. To implement the recommendation of the PITAC for improving coordination, the charter for the CIIP IWG is being changed so that the IWG reports to both the Infrastructure and NITRD Subcommittees, where it will now be known as the Cyber Security and Information Assurance (CSIA) IWG, a name that more accurately reflects its activities. Reporting to both Subcommittees has several advantages. First, it maintains the vital connection between the security of our cyber and physical infrastructures through the Infrastructure Subcommittee. Second, it strengthens the integration of cyber security with the rest of the Federal IT research portfolio. Finally, it provides

the IWG with technical and administrative support through the National Coordination Office for IT R&D. Completion of this reorganization is imminent.

The PITAC report on computational science recommends the development of a multi-decade roadmap for R&D investments in computational science, and a restructuring of computational science activities within universities and federal agencies that better mirrors their interdisciplinary nature. Specifically, it recommends tasking the National Academies to launch studies and convene task forces that seek to address each of these goals. Based in part upon early input from the PITAC, the Analytical Perspectives of the 2006 Budget directs the National Coordination Office to commission an NRC study of scientific questions "for which an extraordinary advancement in our understanding is difficult or impossible without leading-edge scientific simulation capabilities." Additional studies to facilitate the development of a strategic roadmap for computational science are also being considered.

While several of the recommendations of the PITAC for both cyber security and computational science are already being implemented, they contribute to an already strong and effective interagency planning process for the NITRD Program. Interagency coordination, including budget planning, is active and vigorous. In 2005, the Supplement to the Budget for the NITRD Program was delivered to Congress in mid-February. Both the content and the timing of the Budget Supplement are evidence of the strength of interagency coordination.

Q2. What efforts are now being made and what mechanisms exist to transition the results of federally funded cyber security research to commercial products and methods, and do you have recommendations for additional federal efforts in this area?

A2. There are several existing agency programs aimed at cyber security technology transfer. These include the Computer Security Resource Center and the Cryptographic Module Validation Program, both at the National Institute of Standards and Technology, and several pilot projects and deployments of cyber security technology funded by the Department of Homeland Security. The PITAC report on cyber security makes some constructive suggestions regarding ways to increase technology transfer, including the suggestion of an annual cyber security interagency workshop with industry participation.

Questions submitted by Representative Sheila Jackson Lee

Q1. While I am unsatisfied by the status of computer science research being conducted on the federal level, I am also disturbed by the lack of female and minority representation in the field of computer science. The statistics show that women and minorities are not being proportionally represented in academia when it comes to computer science. In 2003, women represented barely over 20 percent of the computer science doctoral degrees granted. The same statistics show that in 2003 the White population made up about 70 percent of the doctoral degrees granted to U.S. citizens and permanent residents. At the same time, Asian/Pacific Islanders made up about 20 percent of the doctoral degrees granted, but Blacks, Hispanics and American Indian/Native Alaskans made up less than five percent of the doctoral degrees granted. These statistics are very discouraging and show that we are not reaching out to our entire population. Indeed, the problem starts in the classroom, where many under-privileged youth do not have nearly the same access to computers and the Internet. If they don't have this background at an early age, its not surprising that they don't pursue the field in higher education and later in life. What are we doing to reach women, minorities and the under-privileged in our society?

A1. Access to educational opportunities is an important prerequisite for a career in scientific research, but even more important is continuity of preparation; that is, adequate education at every grade level. At the heart of President Bush's signature education initiative, the *No Child Left Behind (NCLB) Act,* is a commitment to eliminate the achievement gap between minority and white students by insisting on greater accountability and ensuring that all students have access to a quality education. This kind of strong academic foundation can lay the groundwork for more students to pursue careers in science and engineering. Continued implementation of NCLB is an important step towards the goal of representative participation by women and minorities in all S&T fields.

To improve educational outreach specifically with minority populations, President Bush has issued 1) an Executive Order in October 2001 establishing a President's Advisory Commission on Educational Excellence for Hispanic Americans in the Department of Education to provide advice on closing the achievement gap for His-

panic American children in reaching the goals outlined in NCLB; 2) an Executive Order in February 2002 establishing the President's Board of Advisors on Historically Black Colleges and Universities in the Department of Education to provide advice on ways to strengthen the capacity of historically black colleges and universities to provide the highest quality education; and 3) in May 2004 an Executive Order establishing an Interagency Working Group on American Indian and Alaska Native Education to provide assistance in meeting the goals of the NCLB with Native populations in a manner that is consistent with tribal traditions, languages and cultures. Additionally, Mrs. Bush in June 2004 accepted the position of Honorary Chair of the Advisory Committee for the Extraordinary Women Engineers Project, an awareness and outreach program designed to encourage young women to choose engineering as a career and to develop a new generation of role models for those already in the field.

Many federal agencies have on-going programs that target women, minorities and the under-privileged directly. For example: at the National Science Foundation (NSF), the Louis Stokes Alliances for Minority Participation Program is aimed at increasing the quality and quantity of students successfully completing science, technology, engineering and mathematics (STEM) baccalaureate degree programs and increasing the number of students interested in, academically qualified for, and matriculated into programs of graduate study. NSF's ADVANCE program focuses on increasing the participation and advancement of women in academic science and engineering careers. Additionally, from an institutional perspective, NSF's Centers of Research Excellence in Science and Technology (CREST) program makes resources available to significantly enhance the research capabilities of minority-serving institutions through the establishment of centers that effectively integrate education and research. CREST promotes the development of new knowledge, enhancements of the research productivity of individual faculty, and an expanded diverse student presence in STEM disciplines. NSF currently provides support for 14 CREST Centers.

There are also other programs at other agencies. The Department of Education's Minority Science and Engineering Improvement Program supports grants to institutions of higher education that are designed to effect long-range improvement in science and engineering education at predominantly minority institutions and to increase the participation of under-represented ethnic and racial minorities in scientific and technological careers. The National Aeronautics and Space Administration's Minority University Research and Education Program focuses on collaborative efforts with minority serving institutions to support the advancement of under-represented students in the fields of math, science, engineering, and technology.

Recently, in an effort to coordinate on and maximize the impact of such agency programs, the National Science and Technology Council's Subcommittee on Education and Workforce Development has overseen the establishment of a Science Education Resource Virtual Diversity Center which will serve as a the major STEM education content portal for federal programs that target increased participation from women, under-represented minorities, and persons with disabilities, and will be a tool for sharing information on all strategies designed to address the Nation's STEM workforce needs.

Q2. The PITAC cyber security report makes specific recommendations for increased cyber security research funding for NSF, DARPA and DHS.

Q2a. What is your reaction to this recommendation; will future Administration budget requests respond to this recommendation?

A2a. Funding for cyber security R&D must be considered in the context of agency missions, agency budgets, the overall R&D budget, and the total federal budget, for which there are many competing priorities. A recommendation calling for a substantial increase in funding for a particular R&D area, given the current severely constrained fiscal environment, implies a re-prioritization of existing research areas. Any such re-prioritization must be based on an in-depth understanding of areas where specific gaps in our knowledge exist. Agencies are currently involved in developing this understanding to inform future budget development activities.

Q2b. Why does DHS now spend only 1/10 of two percent of their Science and Technology budget on fundamental research for cyber security? Is this an appropriate funding level?

A2b. The Science and Technology budget for the Department of Homeland Security funds a wide range of activities that include R&D to address radiological, nuclear, chemical and biological threats to the homeland, as well as cyber security research to address threats to our nation's information infrastructure. The S&T directorate must balance the funding for cyber security R&D against these other priorities.

Moreover, many of the activities funded through the DHS S&T directorate are short-term development investments to quickly generate the tools necessary for the detection and prevention of catastrophic physical attacks, essential to protect our nation from weapons of mass destruction. Such short-term tool development activities are inherently more expensive than research, which tends to skew any comparisons to research funding.

ANSWERS TO POST-HEARING QUESTIONS

Responses by Anthony J. Tether, Director, Defense Advanced Research Projects Agency

Questions submitted by Chairman Sherwood L. Boehlert

Q1. During a discussion with Representative Biggert at the hearing, you said that the 33 percent drop in DARPA's NITRD budget between fiscal year 2002 (FY02) and FY06 was inaccurate because of an OMB accounting problem, and you agreed to provide the Committee with an "apples-to-apples" comparison that would better explain DARPA IT support over the last five years. With that in mind:

Q1a. Please provide the correct budget numbers for FY02 to FY06 for DARPA's overall spending on information technology R&D. Include information about how much of those funds went to universities each year.

A1a.

$ in Millions	FY02	FY03	FY04	FY05	FY06
1. NITRD Budget Estimates Reported to Congress	263	223	222	154	176
2. Corrected NITRD estimates (FY02-05 reflecting actual appropriation)	217	204	215	162	
3. Nanotechnology Programs	0	26	62	71	43
4. Information Assurance Programs	86	49	37	69	84
5. NITRD updated to correct actual appropriation, plus Nanotechnology and Information Assurance Programs not previously included to avoid double counting	303	279	314	302	303

* University funding will be addressed in Question 2.

Q1b. Please explain any discrepancies with the published NITRD numbers.

A1b. Line 1 reflects DARPA's NITRD submissions published in the "Blue Book" for FY02 to FY06, which are based on the President's Budget Request. Line 2 reflects actual funding after appropriations. Lines 3 and 4 include additional Nanotechnology and Information Assurance programs that fit the NITRD categories but were previously excluded to avoid double counting on other OMB crosscuts. Line 5 reflects the total of these additions.

Q1c. Please explain DARPA's interaction in the NITRD budget process, including how you interact with OMB and OSTP in planning activities and in finalizing the numbers that are included in the annual "blue book."

A1c. Initial estimates for the annual NITRD submission are requested by the Office of the Secretary of Defense (OSD) Comptroller in the November/December timeframe as the Department is finalizing budget controls for the upcoming President's budget submission. The OSD Comptroller's office then forwards these estimates to the Office of Management and Budget (OMB) Analyst responsible for OMB Max C Data reporting. Often these numbers are requested prior to the final budget lock for the President's budget which usually occurs in the first week of January. A staff member from the National Coordination Office for Information Technology R&D contacts DARPA in the February to May timeframe to verify the NITRD final amounts for printing of the "blue book." At that time, if required, DARPA updates the numbers to reflect the final President's budget.

Q2. At the hearing you described DARPA's research in cognitive computing as an example of long-term IT research.

Q2a. What is the funding for this program, and how much of this funding is going to universities, and to computer science faculty? Please provide data for FY00 to FY05. Also, what funding is planned in this area for FY06 and beyond?

A2a. Funding for the Cognitive Computing Systems program is shown below with associated university funding. DARPA research in this area started in FY 2002.

$ in Millions	FY02	FY03	FY04	FY05	FY06
Total DARPA Cognitive Computing Systems Funding	11	62	119	149	201
Amount of Cognitive Computing Systems Funds Awarded to Universities (Includes prime contracts and subcontracts)	4	36	40	TBD*	

* FY05 is ongoing. Amount will increase over the period the funds are available for obligation.

Q2b. What other long-term research is DARPA currently supporting in computer science? How much funding in those programs is going to universities? How much is classified?

A2b. As previously reported in my testimony, the total DARPA Computer Science Research funding is below and covers the areas of High Performance and Global Scale Systems, Information Assurance and Survivability, Language Translation, Cognitive Systems, Nanotechnology and the applications of these efforts in the Networking, Logistics, Communications and Classified areas. More details on individual programs can be found in DARPA's detailed budget request.

$ in Millions	FY02	FY03	FY04	FY05	FY06
Total DARPA Computer Science Funding	571	613	583	583	584
Total Classified Programs (included in above total)	5	25	48	66	52
Amount of Computer Science Funding Awarded to Universities -- Only prime contracts	207	173	123	TBD*	
Amount of Computer Science Funding Awarded to Universities -- Only subcontracts	8	27	38	TBD*	
Total University Funding	215	200	161	TBD*	

* FY05 is ongoing. Amount will increase over the period the funds are available for obligation

Q3. What is DARPA's response to the recommendations in the recent President's Information Technology Advisory Committee (PITAC) report on cyber security?

A3. While recognizing the budget restraints that all federal agencies must operate under, DARPA wholeheartedly agrees with the idea that both the National Science Foundation (NSF) and the Department of Homeland Security (DHS) should increase their support for commercial cyber security research to build our commercial cyber security research base and protect our civilian computer networks, respectively. In fact, the PITAC was told as much when we met with them while they were preparing their report. Such increases at NSF and DHS would be completely in line with the mission of those agencies and the cyber security challenges we face.

As far as DARPA goes, our work in cyber security, what we called "information assurance," is aimed at making sure that the networks at the heart of DOD's transformation to network centric warfare are secure and robust, because the first thing a determined, sophisticated adversary will do is try to take down our networks. Moreover, the nature of our military networks will be different. These will be networks that must assemble on the fly without a fixed infrastructure, including pure peer to peer networks. We must achieve what has been called "critical infrastructure protection" without infrastructure. No one else, including the commercial sector or even civilian agencies, can or will do it for us. So, given our mission, DARPA's emphasis must be on those DOD problems.

Q4. You noted in your testimony that DARPA does not directly seek efforts in computer science, but rather solicits ideas for achieving particular capabilities. Without regard to funding constraints, what capabilities that demand a significant focus on computer science research merit further pursuit by DARPA? Or, put another way: If DARPA's budget were to receive a significant budget increase beyond the President's request, what capabilities with a significant computer science focus would you pursue?

A4. As I mentioned during the hearing, DARPA is perhaps the only agency actually doing something major to maintain our edge in high-performance computing—a subject that is of great interest to this committee and rightly so. Our High Productivity Computing Systems program is designing and will build prototypes of the next generation supercomputer. In Fiscal Year (FY) 06 we will down-select to one team to build the prototypes. If we had additional money, it would be better to have two teams. Two teams would allow us to compare different approaches, have a more diverse industrial base and maintain competitive pressure. An extra team would cost about $70M in FY07.

More broadly, it might be helpful to have somewhat more money for our work in cognitive computing, but the exact amount is hard to say. Our research in cognitive computing is very challenging and long-term and, to the extent it succeeds, will have an enormous impact. But, as path breaking research, adding large amounts of money to it quickly is not likely to get you much faster results. You would get more activity with more money, but since a limited number of people have path breaking ideas, you may not get more results. So, there might be some leeway for more funding in cognitive computing now, but not large amounts more.

Question submitted by Representative Sheila Jackson Lee

Q1. While I am unsatisfied by the status of computer science research being conducted on the federal level, I am also disturbed by the lack of female and minority representation in the field of computer science. The statistics show that women and minorities are not being proportionally represented in academia when it comes to computer science. In 2003, women represented barely over 20 percent of the computer science doctoral degrees granted. The same statistics show that in 2003 the White population made up about 70 percent of the doctoral degrees granted to U.S. citizens and permanent residents. At the same time, Asian/Pacific Islanders made up about 20 percent of the doctoral degrees granted, but Blacks, Hispanics and American Indian/Native Alaskans made up less than five percent of the doctoral degrees granted. These statistics are very discouraging and show that we are not reaching out to our entire population. Indeed, the problem starts in the classroom, where many under-privileged youth do not have nearly the same access to computers and the Internet. If they don't have this background at an early age, its not surprising that they don't pursue the field in higher education and later in life. What are we doing to reach women, minorities and the under-privileged in our society?

A1. DARPA agrees wholeheartedly that we need to get more Americans, and wider set of Americans, interested in computer science and science and engineering. The lifeblood of a place like DARPA is its program mangers, and it takes many years and many educational hurdles before someone can be hired by us. One of our biggest challenges is constantly finding the new people we need, people with great ideas and a passion to make a difference, who typically also have a doctorate and deep experience in demanding technical positions. You cannot just conjure up that kind of person when you need them.

So, if only from a self-interested point of view, DARPA needs more Americans entering the educational pipeline for technical careers. In this context, I should mention our Grand Challenge. The whole idea behind the Grand Challenge is to reach out to people who ordinarily do not work on problems for the Department of Defense by offering a large prize to whomever meets the challenge first. 118 teams applied this year. Of the 40 teams remaining, 14 of them are from universities and one from a high school. Young people from across the Nation have been excited by the Grand Challenge (and probably the recent privately funded X–Prize) because that's the nature of prize competitions. The goals are clear and the competition is exciting, so they are like a high tech sporting event. Now, education is not DARPA's area of expertise, but maybe if various educational organizations held prize competitions tailored to various levels of the educational process—university, high school, even elementary schools—such competitions could help lure people into technical careers by showing them how much fun they can have.

ANSWERS TO POST-HEARING QUESTIONS

Responses by William A. Wulf, President, National Academy of Engineering

Questions submitted by Chairman Sherwood L. Boehlert

Q1. What kind of computer science research isn't DARPA supporting that you think it should? Is it a matter of more funding or are there programs that are of lower priority that should be cut?

A1. There are two dimensions to the answer of this question—(1) the topics of research, and (2) the "style" of the support for that research, by which I mean the level of funding, the duration of that funding, the degree of control exercised by the funder, etc. The current DARPA management is, I believe, failing the country on both dimensions.

Along both dimensions, there are many organizations that support essential incremental improvements—the service laboratories and service R&D support organizations, for example. There is now no DOD organization like the "old DARPA," however, that fills the role of discovery of breakthrough technologies.

Concerning the topics of research—as I noted in my written testimony, there is a fifteen year delay between discovery of basic knowledge and its appearance in product. Failure to fill this pipeline will not be immediately evident, but the future consequences will be cataclysmic. I could name a long list of areas where filling the pipeline is needed, but just as a sampler:

- As I have testified before, our basic model of computer security (perimeter defense) is fatally flawed—we will never have secure computing systems so long as this is the underlying model! We need a breakthrough, and the only way to get that is to support a variety of radical approaches—and to expect most of them to fail! The short-term, risk-averse approach being currently taken by DARPA will not yield such a breakthrough.
- Our ability to produce reliable, effective software seems to always totter on the brink of disaster—and 100+ million dollar examples are all too common (e.g., the recent problem with the FBI TRILOGY system). It ought to be obvious that doing just "more of the same" will not solve the problem; a breakthrough is needed, and, as above, the only way to get that is to support a variety of approaches with a risky, long-term, basic emphasis.
- It is a bit more than slightly embarrassing that our current computer components are individually a million times faster than our brain cells, yet computers either cannot, or with great difficulty do what humans do easily. There simply must be a model of computing, especially of parallel computing, that we do not understand and that, if we did, would produce computing architectures and algorithms of immense power.
- The use of computers in education has progressed little from the "automated drill" model of the Plato system from the 1960's. Yet we now know much more about the way that people learn, physiologically and psychologically. We also have tacit knowledge about how emotion interacts with learning, and how to evoke emotion to train, for example, first responders and troops in urban combat zones.

I picked each of the examples above because they have a clear and compelling link to the mission of the DOD. Security, reliable software, high performance computing and education/training are all central to that mission—but there are undoubtedly many more such examples. To fail to "fill the pipeline" on any of them is akin to criminal—yet the current DARPA is AWOL on all of them!

Concerning the "style" of support for topics such as those above—I think it is important to understand that they can't be bought on a competitive market in the way that incremental technology improvements can. I am an engineer, former CEO of an engineering company, Director of another engineering company, and a big fan of commercial development. I am also a skeptic of the academic belief that basic research is the source of all new ideas. But, that said, I also deeply believe that a program of long-term, academic, risky, basic research is essential to the mission of the DOD; that is a role that DARPA used to play but is no longer playing. Not in the near-term—but in the 10–15 year time frame—the U.S. is endangered by DARPA's current style of funding!

Q2. At the hearing, Dr. Tether mentioned several times that his agency's work on cognitive computing as an example of long-range research underway at DARPA.

Is that the kind of long-range computer science research that you believe DARPA should be doing? Why or why not?

A2. I am very sorry, but I am not sufficiently acquainted with this program to answer. My schedule since the hearing in May has been such that I have not been able to inform myself about it. If the Committee wishes, I will be delighted to inform myself after returning from Australia in late July and submit an answer at that time.

Q3. What criteria should we be using to determine if federal support for fundamental research in computer science in general and cyber security in particular is adequate?

A3. That is, of course, one of the hardest questions to answer since one can never know with certainty whether the next incremental dollar will fund the breakthrough that revolutionizes a field, or results in a technology with profound implications for our quality of life.

At least at NSF, however, the success rate for proposals is probably a good surrogate. Historically NSF has funded about 30 percent of the proposals it receives. Informal conversations with program officers at NSF suggests that, in fact, probably 50 percent of the proposals they receive are worthy of funding, so a 30 percent success rate is covering the really outstanding proposals. If the success rate for cyber security were 30 percent, I would judge the funding to be adequate.

A general answer for mission agencies such as DOD and DOE is harder to give; each such agency must think in terms of its own needs in various areas. In the case of these two specific agencies, which are the most heavily dependent on high quality security and spend literally billions of dollars annually on largely manual systems, it is hard for me to understand why they aren't investing more on basic research in this area.

Questions submitted by Representative Bart Gordon

Q1. The President's Information Technology Advisory Committee report on cyber security finds that the academic research community in cyber security is below critical mass.

Q1a. To what extent would this be corrected simply by increasing the amount of research funding available?

Q1b. Are there other impediments to bringing more researchers to this field aside from the availability of research funding?

A1a,b. I am strongly in agreement with the PITAC conclusion, and there is no question that additional funding would help increase the amount of research done and hence increase the production of trained professionals in the area of cyber security. The fact that NSF received 12 times as many proposals as it was able to fund in its recent Cyber Trust Initiative demonstrates that there is a pent-up demand to do research in this area. I have long pointed out that there are some deep and very interesting problems in cyber security, and I think the response to NSF's initiative demonstrates that, given support, the CS community will be attracted to these problems.

But, as I have said before to this committee, at least as important as the amount of funding is its stability—an assurance that there will be funds in the future. Academic reputations are built on a lifetime of research and so the best researchers choose problem areas where there is likely to be funding over their whole research career.

Finally, the current tendency to classify security related research is an impediment to academic research. Speaking as one who has done cyber security research, much of this classification is counterproductive. There is a saying in the cyber security research community that "There is no security in obscurity"— meaning that if your security depends on hiding information, it is inevitable that information will leak out and you will be left insecure. That is why, for example, all cryptographic techniques are public. So, while I believe that there are a few cases associated with offensive cyber security that need to be classified, virtually nothing else does—and in fact classifying it will ultimately lead to less security.

In short, more funding would be helpful, but stable funding and an open approach to security research are essential to bringing more academic researchers into this field.

Q2. In your written testimony you mentioned that a significant portion of the NSF's computer science directorate's budget goes to fund cyberinfrastructure, which

largely supports research in fields other than computer science. This means that less funding is available for research in computer science.

Do you think this organizational arrangement at NSF for the support of cyberinfrastructure makes sense, or should the cyberinfrastructure be managed in a separate office and funded through a dedicated appropriations category?

A2. In the spirit of full disclosure I should first note that from 1988–1991 I was the Assistant Director of NSF responsible for what is now called the cyberinfrastructure, and I have wrestled with this question off-and-on for 17 years.

I want to be clear that the fact that cyberinfrastructure in housed in the Computer and Information Science and Engineering (CISE) Directorate causes some confusion, but in fact has worked quite well. The confusion results from a simplistic look at the NSF budget that leads some outside CS to assume that computer science is funded much better than it actually is. A similarly simplistic look at the CISE budget by some computer scientists leads them to assume that a lot of "their money" is being spent on cyberinfrastructure. In truth, the support of cyberinfrastructure is strongly in the national interest, and if its management were moved out of CISE, so would the resources to support it; that money would not become available for CS. To repeat, the problem is one of confusion arising from simplistic analyses; it is not a real problem of reduced funding of CS because of the infrastructure.

At least when I ran CISE, I tolerated this confusion because I believed (and still believe) that both the users of the infrastructure and computer science research benefited from the close and coordinated management of a research program on the infrastructure and its use. For example, we quickly learned that users of supercomputers needed to be able to visualize the results of their computations, which spawned a very fruitful program of research in computer graphics with wide application but that specifically was of great benefit to the supercomputer users. Thus my first preference would be to maintain the current arrangement, but it would not be a disaster to move the management of the cyberinfrastructure to a separate office—however, if that were done, I would think very carefully about how to maintain that close relationship of its use and further research on it. What we now call cyberinfrastructure has evolved very rapidly in part because of that relationship.

Question submitted by Representative Sheila Jackson Lee

Q1. While I am unsatisfied by the status of computer science research being conducted at the federal level, I am also disturbed by the lack of female and minority representation in the field of computer science. The statistics show that women and minorities are not being proportionally represented in academia when it comes to computer science. In 2003, women represented barely 20 percent of the doctoral degrees granted. The same statistics show that in 2003 the White male population made up about 70 percent of the doctoral degrees to U.S. citizens and permanent residents. At the same time, Asian/Pacific Islanders made up about 20 percent of the doctoral degrees granted, but black, Hispanics and American Indian/Native Alaskans made up less than five percent of the doctoral degrees granted. These statistics are discouraging and show that we are not reaching out to our entire population. Indeed, the problem starts in the classroom, where many under-privileged youth do not have this background at an early age, its not surprising that they don't pursue the field in higher education and later in life. What are we doing to reach women, minorities and the underprivileged in our society?

A1. I share Representative Jackson Lee's concern. Indeed it is perhaps even worse than she indicates. Taking engineering as a whole, not just computer science (which, incidentally does a bit better than the rest of the physical sciences and engineering, but much worse than the life sciences), for thirty years we made steady progress on the representation of women and minorities as a fraction of the graduating class. One might argue that the progress should have been faster—but at least there was steady progress. But then something happened in the early 90's and the proportion has been essentially flat since, and no one has been able to satisfactorily explain what happened.

I have attached (Attachment 1) an analysis by a joint committee of the Association for Computing Machinery (ACM), the Institute for Electrical and Electronic Engineers (IEEE), and the Computing Research Association (CRA)—the ACM and IEEE are the two principal professional societies in computer science, and the CRA is an organization of the CS departments and research laboratories. Although this list isn't complete (it doesn't mention the Academy of Engineering program on diversity, the Anita Borg Institute for Women and Technology, or MentorNet, just to

mention three that I am involved in), I think it does demonstrate that the computer science community broadly shares your concerns and is trying to do something about them.

Attachment 1

Information on Coalition to Diversify Computing (CDC) efforts

A JOINT ORGANIZATION OF THE ACM, CRA AND IEEE–CS[1]

PATRICIA TELLER, CHAIR,[2] VALERIE E. TAYLOR, CHAIR-ELECT,[3] J.S. HURLEY, IMMEDIATE PAST-CHAIR[4]

Major progress in computing technologies over the last decade has been accompanied by vast improvements in computing middleware, hardware and networking. An unexpected consequence of these advancements has been a shortage of a highly trained workforce of scientists and engineers capable of understanding and implementing the resources. The Coalition to Diversify Computing (CDC) seeks to address the shortfall through the development of a diverse community of professionals that can effectively meet the computing demands of an evolving society. CDC projects target students and faculty with the expressed intent of increasing the number of minorities successfully transitioning into computing-based careers in academia, federal labs and industry. Additional projects seek to increase the available pool of faculty members through partnerships and mentoring. Current emphasis is placed on the following three areas: (1) recruitment of minority undergraduates to MS/Ph.D. programs, (2) retention of minority graduate students enrolled in MS/Ph.D. programs, and (3) transition of minority MS/Ph.D. graduates into academia and industry. Current projects include:

1. Richard Tapia Celebration of Diversity in Computing Conference. Next conference (October 19–22, 2005 in Albuquerque, New Mexico), URL: *http://www.ncsa.uiuc.edu/Conferences/Tapia2005/*
2. Distributed Rap Sessions
3. CDC Database
4. Sending Students/Mentors to Technical Conferences
5. Collaborative Research Experiences for Undergraduates (CREU)
6. Workshop for Minority Junior Faculty

The diverse membership of CDC from areas of academia, industry and federal laboratories enables a variety of different perspectives and approaches to be utilized in achieving the above stated goals. CDC also partners with a number of organizations with similar missions to leverage resources to optimize outcomes.

CDC Programs

According to the 2003–2004 Taulbee Survey, in 2004 only 1.1 percent of the doctorates in computer engineering and computer science went to Hispanics, 1.5 percent went to African-Americans, and none went to Native Americans or Alaskan Natives.

The number in the pipeline is not increasing by much, either. In fall 2004, 1.3 percent of enrolled Ph.D. students were Hispanic, 1.8 percent were African-American, and only 0.2 percent were Native American.

"Under-representation of our communities in computing is an unacceptable loss of talent, creativity, and achievement for the Nation and the world and we must all work to change this situation," says Roscoe C. Giles (Professor, Department of Electrical and Computer Engineering, Boston University and team member of the NCSA Alliance Steering Committee). Prof. Giles also serves as Executive Director, Institute for African-American ECulture.

CDC focuses its efforts on programs that increase the visibility of minorities, and on providing networking opportunities for minority researchers, faculty, and students. The CDC, founded in 1996, is a program of the Computer Research Association (CRA), the Institute of Electrical and Electronic Engineering (IEEE–CS), the Association of Computing Machinery (ACM), and The National Computational Science Alliance (Alliance), a nationwide partnership of more than 50 academic, government and business organizations working together to prototype an advanced computational infrastructure for the new century. Started in 1997, the Alliance is

---

[1] *http://www.cdc-computing.org*
[2] *pteller@cs.utep.edu*
[3] *taylor@cs.tamu.edu*
[4] *john.s.hurley@boeing.com*

one of two national partnerships funded by the National Science Foundation's Partnerships for Advanced Computational Infrastructure (PACI) program and receives cost-sharing at partner institutions.

Information on CRA's Committee on the Status of Women in Computing Research (CRA–W) efforts

As Rep. Lee correctly points out, the problem of different levels of access to computer technology begins before college. While this is certainly a problem with underprivileged students, there are subtle social factors that affect pre-college girls in this regard as well. It is certainly the case that not getting computer experience and course work in K–12 can affect initial interest in pursuing a computer degree in college. Fortunately, skills acquired in high school math and science courses—rather than high school programming—are more important in preparing for computing research. Women are now taking math and science courses in high school (with the exception of physics) at almost the same rate as men, so they are not coming into higher education totally unprepared to move into computing if their interest can be engaged. It is interesting to note that while the proportion of B.S. degrees granted to women has been declining since 1985 (NSF data), both the number and proportion of graduate degrees (MS and Ph.D.) granted to women have generally increased (albeit slowly). One possible interpretation for this is that any advantage accrued by males of pre-college computer experience is more significant at the undergraduate level than at the graduate level leading to research careers where women are continuing to slowly make gains.

CRA–W has become a national leader in efforts to increase the number and success of women in computing research and innovation. CRA–W is an action-based committee, implementing projects aimed at eliminating barriers to the full participation of women at all stages of the research pipeline beginning at the undergraduate level. It is a group of very prominent, dedicated, senior women who volunteer their time and energy to design and manage projects and to secure funding needed to sustain those projects. CRA–W programs have had a direct impact on over 2,500 women and indirectly influenced thousands of others. We run a range of programs with the following aims:

1. To mentor individuals, by providing research experiences, information, access to role models, and networking opportunities that guide, support, and encourage women in computing,
2. To educate and influence organizations on issues, policies, and procedures that promote the full participation of women in computing, and
3. To build a community for women researchers that provides visibility for their accomplishments and reduces isolation.

CRA–W has recently been recognized for our past efforts. In 2003, CRA–W was awarded the *Presidential Award for Excellence in Science, Mathematics and Engineering Mentoring* for "significant achievements in mentoring women across educational levels," and this year, it was awarded the *National Science Board's Public Service Award.*

Programs for Undergraduates

CRA–W programs that are aimed at undergraduate women are designed to show them what a career in computing research can offer (and how research is qualitatively different from stereotypical IT programming jobs). The programs tend to focus on one-on-one research-oriented mentoring to encourage women to go on to graduate school in computer science and engineering.

- **Distributed Mentoring Project (DMP):** Since 1994, the DMP has matched outstanding female undergraduates with female faculty mentors for a summer of research at the mentor's research university. Students participate in a research project, observe graduate life, and benefit from a close mentoring relationship with their advisors. They also gain the prior research experience and personal recommendation letters that are increasingly important factors in graduate admission decisions. DMP students receive support for transportation to the host university, a weekly stipend for the 10-week project, and funding to attend a conference with their mentor to present their work. The two evaluations of the DMP by the Learning through Evaluation, Adaptation, and Dissemination (LEAD) Center at the University of Wisconsin show that the program has been very effective: 52 percent of DMP participants who had graduated by 2001 had gone on to graduate school. When asked what was most influential in that decision, students ranked their DMP experiences second—before career goals, technical interests, advisor/mentor at home institution, and influence of family members—only success

in undergraduate CS&E courses ranked higher. When this success rate was compared with a comparable population of high-achieving computer science women undergraduates (with GPA's above 3.5), it was found that only 2.5 percent attended graduate school. 55 percent of the participants were students from four-year colleges and universities who had no other exposure to graduate level research.

- **Collaborative Research Experiences for Undergraduates (CREU):** Started in 1998, the primary goal of this program, like DMP, is to provide undergraduates with research experiences that will increase their likelihood of continuing on to graduate school. Originally, the program focused on women, but in 2004 CRA–W formed an alliance with the Coalition to Diversify Computing and expanded the program to include all under-represented groups. The students, all of whom are CS&E majors, work on research projects in collaborative teams of two or three students at their home institution under the guidance of a faculty member during the academic year. Students are selected on a competitive basis from proposals written jointly with their mentor. CREU provides a collaborative experience to help combat the stereotype of computer scientists as lone hackers toiling away in sterile cubicles, to increase students' team building skills, and to decrease any sense of isolation they may feel in their male-dominated classes. The CREU program has grown from 19 women students in 1998 to 65 students in 2004, with six students on minority-based teams. Initial findings from an evaluation study of the CREU program done by the LEAD Center for 1998–2001, conclude that the program has served as a vehicle that promoted skills building, knowledge building, mentoring relationships, role modeling, and enhanced student career aspirations. The program appears to be successful in encouraging students to continue on to graduate school and the students themselves are enthusiastic about their experiences. Preliminary results found that 32 percent of the participants responding were in graduate school. 21 percent had plans to pursue a Ph.D. and 11 percent were receiving an MS degree. Another 32 percent were employed but still had plans to eventually return to graduate school in CS&E.

  Plans for the future include introducing a multi-disciplinary CREU-like program that will involve students and mentors from both computing and scientific disciplines that rely on computing in a collaborative project. This will expose women scientists in other fields to computing research.

- **Distinguished Lecture Series (DLS):** The DLS aims to increase the number of women undergraduates who successfully apply to graduate school in CS&E and to increase the visibility of distinguished women researchers from academia and industrial research labs. Selected sites host an event typically consisting of a lunch with the visitors for women faculty and students, a technical talk by the distinguished lecturer, and a panel discussion with women representing both academic and industrial career paths. The panels also include current women graduate students who give a "view from the trenches." Even at research universities, undergraduates have so many misconceptions about graduate school and the career choices open to those with advanced degrees that the information provided by these panels can be invaluable.

Programs for Graduate Students

With small numbers of women entering graduate school, it is important to ensure their success at navigating the challenges they will face. CRA–W programs for graduate students aim to improve their graduate school experience and increase the chances for successful completion of their graduate degrees.

- **Graduate Student Cohort Project:** The Cohort Project aims to build a community of female students from across the country as they enter graduate school. The program begins with a two-day mentoring workshop for all participants. At the workshop, a number of prominent senior women serve as role models, give practical advice and information, and provide personal insights on the challenges and rewards of their careers. As envisioned, established cohorts will return to the mentoring workshop at regular intervals to get advice on the later stages of graduate school and to provide peer mentoring to the newer cohorts. The Cohort Project provides increased access to information, a range of role models, networking skills and opportunities, and peer support among students at the same stage of their graduate careers. This relatively new project held its first workshop in February 2004 for 100 first-year graduate students, and held the second workshop in March 2005 for 288 first- and second-year graduate students. Informal feedback from participants was extremely positive. The design of the graduate cohort project allows long-term tracking of cohort members throughout their graduate careers and this kind of evaluation study is in progress. Microsoft funded the

2004 workshop for first group. Microsoft and Google jointly funded the 2005 workshop.

- **Best Practices Report on Retaining and Recruiting Women in CS&E Graduate Programs:** In 2000, CRA–W ran an NSF-sponsored workshop on recruiting and retaining women in CS&E graduate programs. Participants included long-time members of the CS&E academic and research communities, social scientists engaged in relevant research, and directors of successful retention efforts. Their findings were reported in the Best Practices Report, which aimed to provide practical advice to faculty, departments, and university administrations. It included recommendations in four categories: increasing the number of women enrolling in specific departments; increasing the number of women in CS&E graduate programs nationally; improving student-student and student-faculty relations; and fostering a research life. The report has been widely distributed. It was an insert in the September 2001 issue of *Computing Research News* (circulation 3,500 research faculty), reprinted for the 2002 *SIGCSE Bulletin* Special Issue on Women in Computing, and distributed at workshops and conferences. It is also available on the web. The report aimed to increase awareness of issues affecting the participation of women in CS&E, give well-meaning faculty a list of specific things that they can do to change their institution, and use the credibility of CRA to get people involved at the departmental level.

Programs for Faculty Career Development

The goal of CRA–W programs aimed at women who have earned their Ph.D. degrees and embarked on an academic/research career is to continue serving their mentoring needs until they become established leaders in their fields and inspiring role models for their women students.

- **Career Mentoring Workshops:** CRA–W has sponsored a series of Career Mentoring Workshops for women since 1993. Women often find themselves a minority at their workplace, and the CRA–W workshops bring them together with women already established in their fields. The established professionals provide practical information, advice, and mentoring support to their younger colleagues. The workshops have speakers and panels on varying topics. Recently, the Mentoring Workshops were expanded to include tracks for more established academics and to include panelists from industrial and government labs in order to raise awareness about alternate career paths and provide mentors from outside of academia. Each of the workshops has been held in conjunction with a major professional meeting, providing many attendees with the opportunity to attend technical talks and make contacts in their research areas. CRA–W runs a second version of the Mentoring Workshop at the SIGCSE (Special Interest Group in Computer Science Education) Conference. That workshop provides information on building successful academic careers that focus on undergraduate teaching.

- **Cohort of Associate to Professors Project (CAPP):** Less than 10 percent of the full professors in CS&E departments are women. Yet, they provide the role models and mentors for our students. CRA–W is attempting to address the problem by forming and mentoring a cohort of women from the associate professor ranks. The cornerstone of the project is the involvement of 15 senior women, appointed as CRA–W Distinguished Professors, who actively participate as role models, mentors, and advisers. The project hopes to accelerate the successful promotion of associate professors by providing them with mentoring, leadership training, encouragement, and ongoing peer-support activities. The first workshop was held in April 2004 and the second occurred in June 2005.

ANSWERS TO POST-HEARING QUESTIONS

Responses by F. Thomson Leighton, Chief Scientist and Co-founder, Akamai Technologies

Questions submitted by Chairman Sherwood L. Boehlert

Q1. What kind of computer science research isn't DARPA supporting that you think it should? Is it just a matter of more funding or are there programs that are of a lower priority that should be cut?

A1. I am most concerned by DARPA's reduction of support for university-led research in computer science. This is not a problem limited to a particular research area within the discipline per se. Rather, it is a trend across the spectrum of computer science. While there may be examples of areas, such as the cognitive computing effort mentioned during the hearing, where DARPA is still funding basic research in computer science, university funding has been greatly reduced or eliminated in many important areas.

The Defense Science Board noted this trend in February 2005 in their examination of DOD's efforts to maintain an adequate supply of High Performance Microprocessors (incidentally, an area in which DSB concluded DOD—primarily DARPA—was "no longer seriously involved in. . .research to enable the embedded processing proficiency on which its strategic advantage depends"). The DSB recognized the crucial payoff gained by DOD—and ultimately the Nation—from DARPA's prior significant involvement in university-led IT R&D:

> "From the early 1960's through the 1980's, one tremendously successful aspect of the DOD's funding in the information technology space came from DARPA's unique approach to the funding of Applied Research (6.2 funding), which hybridized university and industry research through a process that envisioned revolutionary new capabilities, identified barriers to their realization, focused the best minds in the field on new approaches to overcome those barriers and fostered rapid commercialization and DOD adoption. The hybridization of university and industry researchers was a crucial element; it kept the best and the brightest in the university sector well informed of defense issues and the university researchers acted as useful 'prods' to the defense contractors, making it impossible for them to dismiss revolutionary concepts whose feasibility was demonstrated by university-based 6.2 efforts that produced convincing 'proof of concept' prototypes.
>
> Recently, DARPA has further limited university participation, especially as prime contractors, in its Computer Science 6.2 programs, which were by far its most significant investments in university research (vastly outstripping 6.1 funding). These limitations have come in a number of ways, including non-fiscal limitations, such as the classification of work in areas that were previously unclassified, precluding university submission as prime contractors on certain solicitations, and reducing the periods of performance to 18–24 months."

For FY 2005, DARPA reported to the National Coordination Office for IT Research and Development that it planned to make *no* investment in the High Confidence Software and Systems research area. This area includes several important topics, such as cyber security R&D.

As Director Tether's testimony before the Committee indicated, DARPA is funding *classified* research efforts in the cyber security space. Because the work is classified, however, the amount and nature of the work can't be shown in the NCO's budget supplement. More importantly, the university research community is largely unable to participate in the research, and constraints on the dissemination of the results of the work limit the community's ability to drive further innovation based on it.

In its March 2005 review of federal cyber security R&D, the President's Information Technology Advisory Committee (PITAC) noted that this trend stands to disadvantage both the civilian and military sectors. As an example, PITAC cited the potential impact of the increased use of classification on DOD's planned Global Information Grid (GIG)—a multi-layered network to link weapons, intelligence, and military personnel for "network enhanced" warfare:

> "The Defense Department intends the most sensitive portions of the GIG to be self-contained, reducing the military's potential exposure to the insecurities associated with the public IT infrastructure. However, some less sensitive portions of the GIG are expected to connect to the Internet, at least part of the time. Vulnerabilities are introduced whenever highly sensitive defense networks and

civilian networks intersect, giving both communities a significant stake in cooperating to improve the security of the civilian IT infrastructure. Also, economic realities dictate that today's military networks and tomorrow's GIG use civilian commercial hardware and software, exposing those networks to the security vulnerabilities of such products. Thus, the success of the GIG as a secure IT infrastructure of the future—and the near-term success of today's military networks—depends in part on improvements in the security of the civilian IT infrastructure. Yet because the civilian R&D community has access only to the results of unclassified research, reduced support for this community will have a harmful impact on its ability to generate the fundamental discoveries upon which future generations of security products and practices will be based."

PITAC identified 10 specific priority areas, listed below, in computer science of "paramount importance" to securing the national IT infrastructure. DARPA's support for unclassified research in these areas would likely prove enormously beneficial to DOD and the Nation:

1. Authentication Technologies
2. Secure Fundamental Protocols
3. Secure Software Engineering and Software Assurance
4. Holistic System Security
5. Monitoring and Detection
6. Mitigation and Recovery Methodologies
7. Cyber Forensics
8. Modeling and Testbeds for New Technologies
9. Metrics, Benchmarks and Best Practices
10. Research into Human and Organizational Aspects of IT Infrastructures.

There are other areas in which DARPA's efforts are under supported (or absent completely). DARPA's unclassified efforts in Software Design and Productivity, for example, have also been discontinued, according to the FY 2005 plan and FY 2006 request. Low power computation models, improved mesh & grid computing methods, easy-to-learn and use HCI, fault tolerance and replication for portable computing, and federated database management and integration, are all example areas of computing research where advances could help the warfighter, as well as the civilian population, homeland defense and the economy.

DARPA's mission is to support the warfighter and DOD future needs. DARPA research has, in the past, often met those needs by "pushing the envelope" such that advances were adopted in the civilian sphere, thus making them available in quantity, and at lower cost, to the military as "commodity" computing items. By not pursuing research in this realm, or by classifying it, the commoditization and the synergy produced by mixing both university and industrial talent, are missing.

But as the DSB report alluded, DARPA's key role in promoting innovation in IT—innovation that has honed America's war fighting capability, fueled the new economy, and revolutionized health care and the conduct of the sciences—wasn't just its support for particular research areas. It was its unique approach (and commitment) to developing communities of researchers in both industry and academia focused on problems in computer science. DARPA continues to maintain a focus on some of those important problems, but its growing failure to support the university elements of that community is altering the innovation ecosystem in an increasingly negative way. And worse yet, no other mission agency has yet picked up the mantle, leaving NSF to bear the bulk of support for university-led fundamental computer science research.

In summary, I do not believe that the problem necessarily results from a lack of money, but rather from a change in prioritization. Whereas overall funding for computer science has increased over the last several years at DARPA, DARPA funding for basic research at universities in computer science has dropped significantly.

Q2. At the hearing, Dr. Tether mentioned several times his agency's work on cognitive computing as an example of long-range research underway at DARPA. Is that the kind of long-range computer science research that you believe DARPA should be doing? Why or why not?

A2. I am not directly familiar with DARPA's program in cognitive computing, but I do believe that research in this area is worthwhile. However, it is only one area of computer science and will not address many needs of the warfighter and the Nation. For example, research in this area will probably not be relevant to the area of cyber security.

Q3. What criteria should we be using to determine if federal support for fundamental research in computer science in general and cyber security in particular is adequate?

A3. "How much should we spend?" is always a difficult question when it comes to funding basic research. The reason is that the benefit derived from the research generally is not realized until many years later. And, basic research is a high-risk endeavor. Not every idea pans out. Indeed, fundamental research, by its very nature, should be expected to have many failures. Risk-averse research simply does not lead to fundamentally new ways of thinking or to breakthroughs in the most important problems.

That said, there are measures that one can use to determine if the levels of funding are inadequate. First, the success rates of qualified grant proposals can be examined and compared across disciplines. As was noted in prior testimony, the success rate of qualified proposals in computer science at NSF lags far behind the NSF-wide average. The success rate in the area of cyber security is even smaller, a factor of three smaller than the NSF-wide average. These statistics indicate that there is good research that is going unfunded in computer science and that the lack of funding in computer science is out of proportion with other disciplines.

Second, one can look at the historical return on investment for research expenditures in a particular field. As was noted in prior testimony, the return on investment for academic computer science research over the last several decades has been extraordinary. Not only has the research led to the creation of numerous billion-dollar industries, but it has led, in part, to our nation's preeminence in technology as a whole. If history is any guide, we should be spending far greater sums on fundamental research in computer science than we do today.

Third, one can turn to experts for advice. PITAC was one such body of experts in information technology and they have made it very clear that our under-investment in basic cyber security research poses a significant threat to our national well being. PITAC had planned to study the adequacy of our overall investment in IT R&D but their term has expired and no renewals have been announced.

Questions submitted by Representative Bart Gordon

Q1. What efforts are now being made and what mechanisms exist to transition the results of federally funded cyber security research to commercial products and methods, and do you have recommendations for additional federal efforts in this area?

A1. As was noted in the PITAC report "Cyber Security: A Crisis of Prioritization," "current cyber security technology transfer efforts are not adequate to successfully transition federal research investments into civilian sector best practices and products."

PITAC recommended that "the Federal Government should strengthen its cyber security technology transfer partnership with the private sector. Specifically, the Federal Government should place greater emphasis on the development of metrics, models, data sets, and testbeds so that new products and best practices can be evaluated; jointly sponsor with the private sector an annual interagency conference at which new cyber security R&D results are showcased; fund technology transfer efforts (in cooperation with industry) by researchers who have developed promising ideas or technologies; and encourage federally supported graduate students and postdoctoral researchers to gain experience in industry as researchers, interns, or consultants."

In its discussion, PITAC noted that "technology transfer enables the results of federally supported R&D to be incorporated into products that are available for general use. There has been a long and successful history of federally funded IT R&D being transferred into products and best practices that are widely adopted in the private sector."

"The diffusion of federally supported IT R&D into products and practices benefits both consumers and developers:

- Consumers have benefited from faster hardware, faster networks, better software that is easier to use, and more frequent time- and labor-saving upgrades.
- IT research often results in new ideas and prototypes that can be rapidly developed into new or improved commercial products. The developers of such innovations are free to carry their innovative ideas into the marketplace, benefiting all consumers."

"Unlike other IT products, cyber security's benefits are measured by the absence of problems in IT systems. Because the market for these benefits has historically been small, interest is limited among both start-ups and large companies."

PITAC believes that, "given the value and difficulty of technology transfer, the Federal Government should support programs to transform existing and future cyber security research results into commercial products or operational best practices. Specifically, the Federal Government should:

- Strengthen the development of metrics, models, data sets, and testbeds so that new products and best practices can be evaluated.
- Jointly sponsor with the private sector an annual interagency conference at which new cyber security R&D results, especially those conducted or sponsored by the Federal Government, are showcased.
- Require grant proposals to describe the potential practical utility of their research results and have the coordinating body identified in Recommendation 4 of the PITAC report collect and publish these descriptions. (While fundamental research is usually undertaken without any direct transition path envisioned, cyber security research is often undertaken in the context of recognized problems, and documenting logical connections with real world problems is worthwhile.)
- Establish a fund to support technology transfer efforts by researchers who have developed promising ideas or technologies. This fund could also help researchers cooperate with industry to bring products or enhancements rapidly to market.
- Establish and maintain a national database of results from federally funded cyber security research, allowing vendors to identify ideas that can be incorporated into commercial products.
- Encourage federally supported graduate students and postdoctoral researchers to gain experience in industry as researchers, interns, or consultants.
- Encourage agency investment in technology transfer of cyber security R&D results through the Small Business Innovation Research (SBIR) and Small Business Technology Transfer (SBTT) programs of the Federal Government.

"The Federal Government and the private sector, by working together, can effectively and efficiently transfer federally funded cyber security research results into commercial products and build an innovative cyber security workforce, and by doing so can help our society realize the potential benefits of this research."

Q2. The President's Information Technology Advisory Committee report on cyber security finds that the academic research community in cyber security research is below critical mass.

Q2a. To what extent would this be corrected simply by increasing the amount of research funding available?

Q2b. Are there other impediments to bringing more researchers to this field aside from the availability of research funding?

A2a,b. As PITAC notes in its report, increasing the level of funding for basic research in cyber security is required to increase the size of the academic research community in cyber security. But it is not sufficient. The long-term stability of the funding is also important, and it is critical that the university research not be classified.

I do not mean to imply that all cyber security research should be unclassified. Indeed, classified research in the area of cyber security is certainly a worthwhile endeavor. However, if most or all research in cyber security is classified, then university researchers (with whom much of our nation's networking and computer science expertise resides) will not be able to contribute to the discovery of the breakthroughs that are so badly needed in this area. Moreover, the technology transfer needed to convert breakthroughs into products and best practices will also be seriously impeded.

Questions submitted by Representative Sheila Jackson Lee

Q1. While I am unsatisfied by the status of computer science research being conducted on the federal level, I am also disturbed by the lack of female and minority representation in the field of computer science. The statistics show that women and minorities are not being proportionally represented in academia when it comes to computer science. In 2003, women represented barely over 20

percent of the computer science doctoral degrees granted. The same statistics show that in 2003, the White population made up about 70 percent of the doctoral degrees granted to U.S. citizens and permanent residents. At the same time, Asian/Pacific Islanders made up about 20 percent of the doctoral degrees granted, but Blacks, Hispanics, and American Indian/Native Alaskans made up less than five percent of the doctoral degrees granted. These statistics are very discouraging and show that we are not reaching out to our entire population. Indeed, the problem starts in the classroom, where many under-privileged youth do not have nearly the same access to computers and the Internet. If they don't have this background at an early age, its not surprising that they don't pursue the field in higher education and later in life. What are we doing to reach women, minorities, and the under-privileged in our society?

A1. Although I am painfully aware of lack of female and minority representation in the field of computer science (as well as related fields such as mathematics), I do not have sufficient expertise to provide a good answer to this question.

I do know that National Science Foundation's CISE Directorate is continually experimenting with innovative programs to improve this situation, including the new 'Broadening Participation in Computing' program *(http://www.nsf.gov/pubs/2005/nsf05562/nsf05562.htm).* Ensuring continued and increased funding for this program and others like it is important.

In addition, two years ago, computer scientists established the National Center for Women in Technology *(http://www.ncwit.org)* to coordinate a number of national efforts aimed at increasing the participation of women and minorities in the field.

Q2. Your committee's report on cyber security recommends an increase to NSF's budget for cyber security research to $90 million per year and "substantial" increases in civilian cyber security R&D at DARPA and the Department of Homeland Security.

Q2a. Why is there a recommendation for a specific increase for NSF, but not for the other agencies?

Q2b. Did your committee consider the need for funding increases at NIST or other federal agencies?

A2a,b. NSF is the only agency for which we had enough credible data on research funding in order to make a specific recommendation for funding levels. That said, a comparable amount of funding for basic non-classified research at DARPA and DHS would certainly be in the Nation's interest. As was noted in prior testimony, DARPA has shifted a significant amount of funding away from universities in cyber security in favor of more directed and/or classified work, and DHS (which is tasked with the Nation's cyber security) spends only a tiny fraction of its large S&T budget on cyber security. The failure of the Department of Homeland Security to invest significantly in cyber security R&D was of particular concern to PITAC. DHS has an overall Science & Technology budget of roughly $1.3 billion dollars, of which $18 million dollars is devoted to cyber security. For FY06, the DHS budget decreases this amount to $17 million. Of these amounts, less than $2M is devoted to basic research.

NIST, NIJ, DHS, DOE and other agencies should all re-examine the role they play in cyber security research. It is probably in the Nation's interest to increase funding at each of these agencies. However, without better data, a clear understanding of how the money would be spent at those agencies, and some kind of national strategy, the committee was unable to formulate specific recommendations—especially at a time when there are such large federal deficits.

Appendix 2:

Additional Material for the Record

JOINT STATEMENT OF THE COMPUTING RESEARCH COMMUNITY

Thank you, Chairman Boehlert and Ranking Member Gordon, for convening this hearing and for your committee's continued support of information technology research and development. The American Society for Information Science and Technology (ASIS&T), Coalition for Academic Scientific Computing (CASC), Computing Research Association (CRA), Electrical and Computer Engineering Department Heads Association (ECEDHA), Society for Industrial and Applied Mathematics (SIAM), and U.S. Public Policy Committee of the Association for Computing Machinery (USACM) join in endorsing this testimony because we believe the health of the computing research enterprise to be crucial to the Nation's future economic competitiveness, our national defense and homeland security, the health of our citizens, and further discovery in the sciences.

The United States, in both the public and private sectors, has done a remarkable job in forging a leadership role in information technology, due in large part to a healthy fundamental computing research enterprise. That leadership role has paid great dividends to the country and the world. However, we are concerned that the U.S. is in danger of ceding leadership if current trends continue. Fortunately, the U.S. remains in good position to reverse those trends if we act soon.

Our testimony examines how the U.S. came to assume its dominant position in IT and the benefits that role conveys to the Nation. We also examine why the changing landscape for federal support of computing research imperils U.S. leadership in IT, and in turn, U.S. economic performance in the coming decades. Finally, we outline what we believe should be done to shore up that leadership.

We commend the Committee for its interest in this topic and hope this "view from the community" provides you a valuable perspective on the critical importance of IT on national prosperity, and how changes to the federal research portfolio impact the IT sector.

The Impact of New Technologies

The importance of computing research and computational science in enabling the new economy is well documented. The resulting advances in information technology have led to significant improvements in product design, development and distribution for American industry, provided instant communications for people worldwide, and enabled new scientific disciplines such as bioinformatics and nanotechnology that show great promise in improving a whole range of health, security, and communications technologies. Federal Reserve Board Chairman Alan Greenspan has said that the growing use of information technology has been the distinguishing feature of this "pivotal period in American economic history." Recent analysis suggests that the remarkable growth the U.S. experienced between 1995 and 2000 was spurred by an increase in productivity enabled almost completely by factors related to IT. "IT drove the U.S. productivity revival [from 1995–2000]," according to Harvard economist Dale Jorgenson.

Information technology has also changed the conduct of research. Innovations in computing technologies are enabling scientific discovery across every scientific discipline—from mapping the human brain to modeling climatic change. Researchers, faced with research problems that are ever more complex and interdisciplinary in nature, are using IT to collaborate across the globe, simulate experiments, visualize large and complex data sets, and collect and manage massive amounts of data.

The Information Technology Ecosystem that Gives Birth to New Technologies

A significant reason for this dramatic advance in IT and the subsequent increase in innovation and productivity is the "extraordinarily productive interplay of federally funded university research, federally and privately funded industrial research, and entrepreneurial companies founded and staffed by people who moved back and forth between universities and industry," according to a 1995 report by the National Research Council. That report, and a subsequent 1999 report by the President's Information Technology Advisory Committee (PITAC), emphasized the "spectacular" return on the federal investment in long-term IT research and development.

The 1995 NRC report, *Evolving the High Performance Computing and Communications Initiative to Support the Nation's Information Infrastructure,* included a compelling graphic illustrating this spectacular return. The graphic was updated in 2002 and is included with this testimony. (See Figure 1.)

It is worth a moment to consider the graphic. The graphic charts the development of technologies from their origins in industrial and federally-supported university R&D, to the introduction of the first commercial products, through the creation of billion-dollar industries and markets. The original 1995 report identified nine of these multi-billion-dollar IT industries (the categories on the left side of the graph-

ic). Seven years later, the number of examples had grown to 19—multi-billion-dollar industries that are transforming our lives and driving our economy.

The graphic also illustrates the dynamic interplay between federally-supported university-based research and industrial R&D efforts. In some cases, such as reduced instruction set computing (RISC) processors (a chip architecture that forms the basis for processors used by Sun, IBM, HP, and Apple, and has significantly influenced all microprocessor design) and RAID disk servers ("redundant arrays of inexpensive disks"), the initial ideas came from industry, but government-supported university research was necessary to advance the technology. In other cases, such as timesharing, graphical user interfaces, and the Internet, the ideas originated in the universities long before they matured to a point where subsequent research by industry helped move the technologies towards commercialization. In each example, the industry/university research relationship has been complementary. University research, focused as it is on fundamental questions and long-term problems, does not supplant industry research and development. And industry, which contributed $190 billion in 2002 (down from $198 billion in 2001) in overall R&D geared primarily towards short-term development, does not supplant university research.

This is an important point that bears some development. The great majority of industry-based research and development is of a fundamentally different character than university-based research. Industry-based research and development is, by necessity, much shorter term than the fundamental research performed in universities. It tends to be focused on product and process development, areas which will have more immediate impact on business profitability. Industry generally avoids long-term research because it entails risk in a couple of unappealing ways. First, it is hard to predict the outcome of fundamental research. The value of the research may surface in unanticipated areas. Second, fundamental research, because it is published openly, provides broad value to all players in the marketplace. It is difficult for any one company to "protect" the fundamental knowledge gleaned from long-term research and capitalize on it without all players in the marketplace having a chance to incorporate the new knowledge into their thinking.

Those companies that do make significant fundamental research investments tend to be the largest companies in the sector. Their dominant position in the market ensures that they benefit from any market-wide improvement in technology basic research might bring. But, even with that advantage, the investment of companies like Microsoft and Intel in fundamental research remains a small percentage of their overall IT R&D investment (in Microsoft's case, it's estimated at around five percent of the company's R&D budget), and many companies of equivalent size (Oracle, Dell, Cisco) don't invest in long-term R&D at all.

The chart also illustrates one other important characteristic of the IT R&D ecosystem—it is very interdependent. Note that the arrows that show the flow of people and ideas move not only between industry, university and commercial sectors, but between subfields as well, sometimes in unanticipated ways. Developments in Internet-working technologies led to the development of the Internet and World Wide Web (and the rise of Yahoo and Google), but also to developments in Local Area Networking and Workstations. Work on timesharing and client and server computing in the 1960s led to the development of e-mail and instant messaging. In addition, this interdependence increasingly includes subfields beyond traditional IT, helping enable whole new disciplines like bioinformatics, opto-electronics, and nanotechnology.

Perhaps the most noteworthy aspect of the graphic is its illustration of the long incubation period for these technologies between the time they were conceived and first researched to the time they arrived in the market as commercial products. In nearly every case, that lag time is measured in decades. This is the clearest illustration of the results of a sustained, robust commitment to long-term, fundamental research. The innovation that creates the technologies that drive the new economy today is the fruit of investments the federal government made in basic research 10, 15, 30 years ago. Essentially every aspect of information technology upon which we rely today—the Internet, web browsers, public key cryptography for secure credit card transactions, parallel database systems, high-performance computer graphics, portable communications such as cell phones, broadband last mile. . .essentially every billion-dollar sub-market—is a product of this commitment, and bears the stamp of federally-supported research.

One important aspect of federally-supported university research that is only hinted at in the flow of arrows on this complex graphic is that it produces people—researchers and practitioners—as well as ideas. This is especially important given the current outlook for IT jobs in the coming decade. Despite current concerns about offshoring and the end of the IT boom times, the U.S. Bureau of Labor Statistics this year released projections that continue to show a huge projected shortfall in IT

workers over the next 10 years. As Figure 2 illustrates, the vast majority of the entire projected workforce shortfall in all of science and engineering is in information technology. These are jobs that require a Bachelor's level education or greater. In addition to people, university research also produces tangible products, such as free software and programming tools, which are heavily relied upon in the commercial and defense sectors. Continued support of university research is therefore crucially important in keeping the fires of innovation lit here in the U.S.

But the impact of IT research on enabling of innovation resonates far beyond just the IT sector. IT has played an essential—many argue *the* essential—role in the economic growth of the U.S. in the past 20 years. Most of the actual economic value of IT does not come directly from fundamental discoveries in electronics, computers, software, communications, or algorithms—these are inputs to larger processes of product and service innovation, most of which happens in the private sector and in competitive markets. Nevertheless, the seeds of this economic growth are in the fundamental discoveries, most of which are pre-competitive and occur in the Nation's universities and research laboratories. The economic growth would not happen without these discoveries. Our concern is on the precarious state of research that primes the pump of economic growth, and that puts the U.S. in jeopardy.

The Changing Landscape for Computing

The landscape for computing research funding has changed significantly since PITAC began its review of the federal IT R&D effort in 1997. Since the early 1960s, the federal agencies arguably most responsible for supporting computing research, the development of the field and much of the innovation that has resulted are the National Science Foundation, the Defense Advanced Research Projects Agency, and the Department of Energy. At the time PITAC began its review, NSF and DARPA bore a leading and nearly equal share of the overall federal investment in IT R&D. In FY 1998, DARPA funding constituted 30 percent of federal IT R&D spending, compared to NSF's 27 percent share.

However, as the overall investment has increased, DARPA's share of the research—both as a percentage of the overall effort and in absolute dollars—has declined. While NSF's $795 million investment in IT R&D in FY 2005 represents 35 percent of overall federal IT R&D (an increase in its total share since FY 1998), DARPA's $143 million in FY 2005 represents just six percent of the overall IT R&D budget, a significant decrease in its share since FY 1998.

We are concerned about DARPA's diminished role in supporting computing research and the impact that it will have on the field, DARPA's mission, and the Nation as a whole. Central to these concerns is the idea that the field—and hence, the Nation—benefited greatly by having different approaches to funding computing research represented by the NSF model and the DARPA model. While NSF has primarily focused on support for individual investigators at a wide range of institutions—and support for computing infrastructure at America's universities—DARPA's approach has varied over the years. Historically, DARPA program managers could fund individual researchers, or even "centers of excellence"—typically university research centers—with useful and critically important flexibility. DARPA program managers had great discretion in funding projects they believed to be promising. In this way, DARPA was able to create and nourish communities of researchers to focus on problems of particular interest to the agency and to the Department of Defense, with great success.

The combination of the different approaches has proven enormously beneficial to the Nation, we argue, and to DARPA's overall mission of assuring that the U.S. maintains "a lead in applying state-of-the-art technology for military capabilities and [preventing] technological surprise from her adversaries." DARPA-supported research in computing over a period of over four decades, beginning in the 1960s, has laid down the foundations for the modern microprocessor, the Internet, the graphical user interface, single-user workstations, and a whole host of other innovations that have not only made the U.S. military the lethal and effective fighting force it is today, but have driven the new economy and enabled a whole range of new scientific disciplines.

However, through a series of policy changes, including the use of "go/no-go" decisions applied to critical research at 12 to 18 month intervals and the increasing classification of research sponsored by the agency,[1] DARPA has shifted much of its

[1] There are, of course, important reasons for classifying federal research, especially when it is clear that the research might reveal our defense capabilities or vulnerabilities. However, it should also be understood that there are real costs—including that the research is unavailable for public dissemination and scrutiny, and that many university researchers, arguably some of the best minds in the country, are no longer able to contribute to the work. In the case of

focus in IT R&D from pushing the leading edge of computing research to "bridging the gap" between basic research and deployable technologies—in essence relying primarily on other agencies such as NSF and Department of Energy's Office of Science—to fund the basic research needed to advance the field.

These changes at DARPA have discouraged university participation in research, effectively reducing DARPA "mindshare"—the percentage of people working on DARPA problems—at the Nation's universities. This is borne out by a review of DARPA's support for IT R&D at universities. While DARPA's overall funding for IT R&D across the agency increased from $543 million in FY 2001 to $586 million in FY 2004 (in unadjusted dollars), DARPA IT research funding for universities dropped by nearly half—from $214 million in FY 2001 to $123 million in FY 2004—according to numbers the agency provided in response to questions from the Senate Armed Services Committee.

The research community is not alone in noting the potential impact. A DOD Defense Science Board Task Force report on High Performance Microprocessors in February 2005, noted that DOD—primarily DARPA—"is no longer perceived as being seriously involved in—or even taking steps to ensure that others are conducting—research to enable the embedded processing proficiency on which its strategic advantage depends. This withdrawal has created a vacuum where no part of the U.S. Government is able to exert leadership, especially with respect to the revolutionary component of the research portfolio." The report continues in a remarkable footnote:

> This development is partly explained by historic circumstances. Since World War II, the DOD has been the primary supporter of research in university Electrical Engineering and Computer Science (EECS) departments, with NSF contributing some funds towards basic research. From the early 1960's through the 1980's, one tremendously successful aspect of the DOD's funding in the information technology space came from DARPA's unique approach to the funding of Applied Research (6.2 funding), which hybridized university and industry research through a process that envisioned revolutionary new capabilities, identified barriers to their realization, focused the best minds in the field on new approaches to overcome those barriers and fostered rapid commercialization and DOD adoption. The hybridization of university and industry researchers was a crucial element; it kept the best and the brightest in the university sector well informed of defense issues and the university researchers acted as useful "prods" to the defense contractors, making it impossible for them to dismiss revolutionary concepts whose feasibility was demonstrated by university-based 6.2 efforts that produced convincing "proof of concept" prototypes. As EECS grew in scale and its scope extended beyond DOD applications, a "success disaster" ensued in that EECS essentially "outgrew" the ability of the DOD to be its primary source of directional influence, let alone funding. Furthermore, DOD never developed a strategy to deal with this transition. With pressures to fund developments are unique to the Defense (e.g., military aircraft, tanks, artillery, etc.), the DOD withdrew its EECS research leadership. Recently, DARPA has further limited university participation, especially as prime contractors, in its Computer Science 6.2 programs, which were by far its most significant investments in university research (vastly outstripping 6.1 funding). These limitations have come in a number of ways, including non-fiscal limitations, such as the classification of work in areas that were previously unclassified, precluding university submission as prime contractors on certain solicitations, and reducing the periods of performance to 18–24 months.
>
> *High Performance Microchip Supply,* Defense Science Board, February 2005, Appendix D, p. 87–88.

Unfortunately, the other mission agencies have not yet stepped in to fill the gap created by DARPA's withdrawal. As PITAC members Edward Lazowska and Dave Patterson noted in a recent *Science Magazine* editorial, the Department of Homeland Security spends less than two percent of its Science and Technology budget on cyber security, and only a small fraction of that on research. NASA is downsizing computational science, and IT research budgets at the Department of Energy and the National Institutes of Health are slated for cuts in the President's FY 2006 budget. In effect, the national commitment to fundamental research in IT has waned. Ironically, this began at about the same time the economists began to understand the huge benefit that such research provided for economic growth.

DARPA's cyber security research, there is another significant cost to bear as well. The military (and the government overall) has a huge dependence on our nation's commercial infrastructure, but classifying the research in information security means that it is largely unavailable for use in protecting this commercial infrastructure.

This fact, combined with an overall growth in the number of researchers in the field and an increase in the breadth of the discipline, has placed a significant burden for funding basic IT R&D on NSF. The agency reports that in FY 2004, NSF supported 86 percent of federal obligations for basic research in computer science at academic institutions—and the agency's Computing and Information Science and Engineering directorate (CISE) is beginning to show the strain. In FY 2004, the funding rate for competitive awards in CISE fell to a decadal low of 16 percent, lowest of any directorate at NSF and well below the NSF average. Programs in critical areas like information security and assurance are experiencing even lower success rates—NSF's CyberTrust program reported an 8.2 percent success rate for FY 2004. Other fundamental areas, where long-term advances are critical to broad research advances, are also suffering neglect. In particular, computational science, which was the raison d'etre for the entire Federal High-Performance Computing and Communications (HPCC) Program, has become an expanding area for all sciences, however, it has been without any focal point in the overall Federal HPPC Program (now renamed as NITRD). Moreover, even at NSF, support for mathematics and computing sciences—which underlie the health of computing research—has been declining in real terms since FY 2004. Such budget and program management decisions, we argue, are harmful to the field and to the Nation as a whole.

To be clear, our concern is not just with the impact of changes at a single agency. Rather, our concern is that the total level of national investment in fundamental IT research rise to the need that our economy requires in an increasingly competitive world.

As Lazowska and Patterson note: "At a time when global competitors are gaining the capacity and commitment to challenge U.S. high-tech leadership, this changed landscape threatens to derail the extraordinarily productive interplay of academia, government, and industry in IT. Given the importance of IT in enabling the new economy and in opening new areas of scientific discovery, we simply cannot afford to cede leadership."

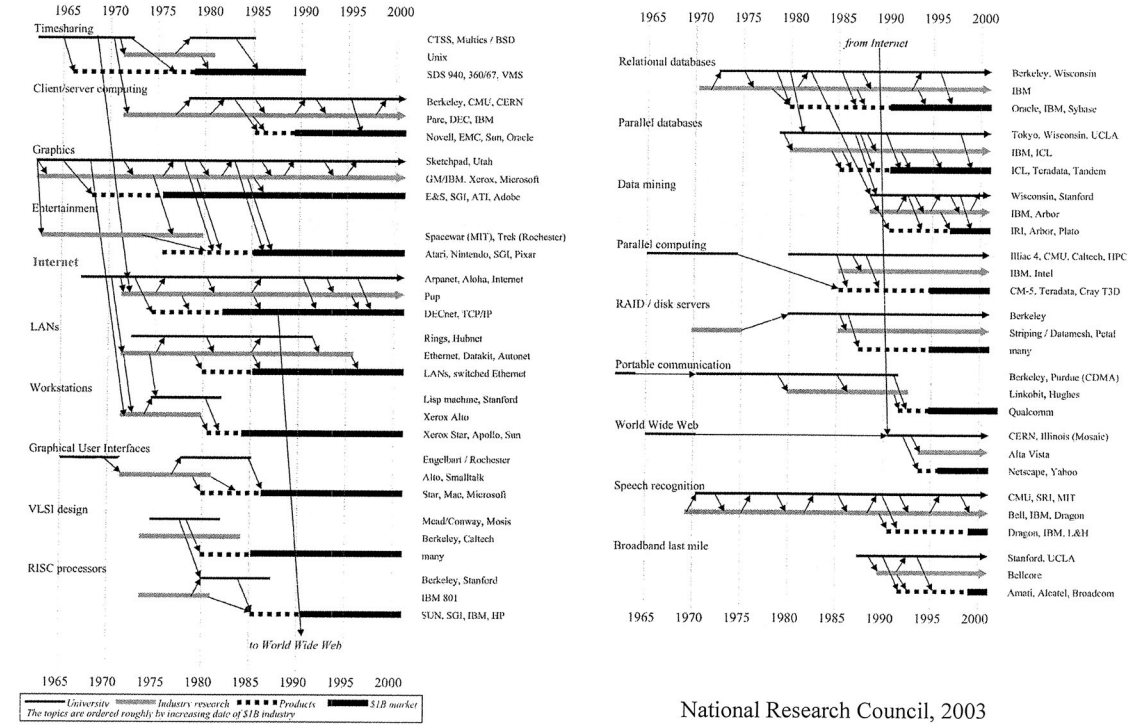
Maintaining Leadership

The U.S. still has the world's strongest capability in fundamental research in IT, and the most experience in how to leverage that capability toward economic growth. This is a robust system that can take stresses from decreased funding for a short time as we determine our strategy. But we run a grave risk in letting the uncertainty about funding for fundamental IT research go on too long. The first causalities are the brilliant young people, many of them from other countries, who come to the U.S. to learn from and contribute to our global lead in this area. Already, tightened visa rules and a perception of a more hostile environment in the U.S. encumber our ability to attract many of these brilliant minds. Without support, they will go to Canada, Europe, Australia and other countries that are actively courting them. Those other countries know the value the U.S. has realized from its system of fundamental research—and want it for themselves. Even with their own economic difficulties, those countries are increasing their investments in such research.

The U.S. took a critical step some years ago in doubling the Nation's investment in health research, and, at the urging of your committee, agreeing to double its investment in other areas of research, including IT research. We believe that was the right decision. The current delays in that process of doubling are understandable, but the costs of delaying too long are very high. We taught the rest of the world how to grow from such investment and they learned the lesson well.

That federal investment helps fuel the innovation that insures the U.S. remains the world leader in business, that we have the strongest possible defense, and that we continue to find ways to live longer, healthier lives. To keep the fires of innovation lit, we should continue to boost funding levels for fundamental IT R&D. We should insure that NSF, DARPA, and the Department of Energy have broad, strong, sustained research programs in IT independent of special initiatives. And we should work to maintain the special qualities of federally-supported university research.

Interplay of university research, industrial research, and development for IT in the US (A)



National Research Council, 2003

Figure 1

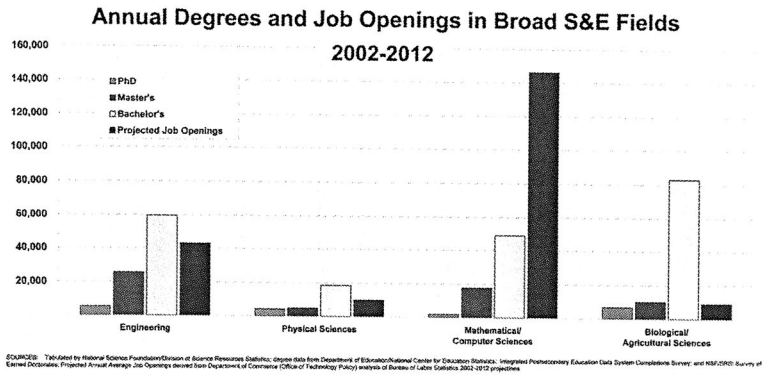

Annual Degrees and Job Openings in Broad S&E Fields
2002-2012
160,000
140,000
120,000
100,000
80,000
60,000
40,000
20,000
PhD
Master's
Bachelor's
Projected Job Openings
Engineering
Physical Sciences
Mathematical/
Computer Sciences
Biological/
Agricultural Sciences

Figure 2

Appendix A

What others are saying:

Council on Competitiveness, *Innovate America* report on the *National Innovation Initiative,* released December, 2004. Available online at: *http://www.compete.org*

To Out-Compete Is to Out-Compute

Few areas of technology hold more promise for stimulating innovation and propelling competitiveness than high performance computing. Along with theory and experimentation, modeling and simulation with high performance computers has become the third leg of science and path to competitive advantage. There's now in vivo, in vitro and in silica. A recent survey by the Council on Competitiveness of U.S. chief technology and chief information officers revealed that nearly 100 percent consider high performance computing tools essential to their business survival. And they are realizing a range of strategic competitive benefits from using this technology, such as shortened product development cycles and faster time to market (in some cases more than 50 percent faster), all of which improve a company's bottom line.

But we are only beginning to reap the potential innovation and competitive benefits that use of this technology promises. With dramatically more powerful systems, companies can extract trillions of dollars in excess cost through business enterprise transformation. We can revolutionize manufacturing through advanced modeling and simulation of the entire process from raw resource to finished product. We can dramatically accelerate the drug discovery process, and substantially increase oil recovery rates by modeling entire oil fields. By shrinking "time to insight" and "time to solution" through the use of high performance computing, companies in virtually every sector will be able to accelerate the innovative process in ways simply not seen in the past, resulting in new capabilities and revolutionary products and services that capture and cement global market share. As Robert Bishop, CEO of Silicon Graphics, notes, "In the 21st century, to out-compete is to out-compute." *[Page 47]*

Because of the IT revolution—especially in software—a major component of manufacturing is service-based. As the U.S. Congress Office of Technology Assessment noted: "Software is. . .a marriage of manufacture and service, since it has the character of both a good (it can be stored and shipped) and a service (computer programs are not immutably fixed)." But, we classify software as a service, not a manufacture. Consider how it is being applied:

- Manufacturers like Xerox are installing service capabilities in their machines—diagnostic software that is capable of signaling to the manufacturer when a part is nearing the end of its useful life, before the problem is ever visible to the customer.
- In 1985, when Ford Motor Company wanted safety data on its vehicles, it spent $60,000 to slam a vehicle into a wall. Today, that frontal crash is performed virtually on high performance computers—at a cost of around $10.
- To design the 777, Boeing developed a software program that allowed its engineers to "fly" in a computerized prototype of the aircraft and iterate the design in virtual space.
- Wal-Mart has installed miniature tracking devices on its products, enabling computerized inventory tracking and controls. *[Page 15–16]*

Goal No. 1 Revitalize Frontier and Multi-disciplinary Research

Nowhere is the need for new multi-disciplinary approaches clearer than in the area of emerging "services science"—the melding together of the more established fields of computer science, operations research, industrial engineering, mathematics, management sciences, decision sciences, social sciences and legal sciences that may transform entire enterprises and drive innovation at the intersection of business and technology expertise. *[Page 30–31]*

A 21st Century Infrastructure

In the late 19th and 20th centuries, the United States pioneered the world's most advanced infrastructure in transportation (railroads, highways, air travel), telecommunications, energy, water and waste management.

Even the Internet, the marvel of modern communications, needs an upgrade. In 1985, the Internet connected 2,000 computers. Today, there are more than 233 million Internet hosts and more than 812 million users. The Internet of the fu-

ture must be able to connect billions of information appliances, like computers, portable devices, wireless modems, GPS locators and sensors. The current infrastructure was not designed to support this explosion of users and devices—and much more investment will be needed to transform the technology and support innovation. *[Page 50]*

Task Force on the Future of American Innovation, *The Knowledge Economy: Is The United States Losing Its Competitive Edge?,* released February, 2005. Available on-line at *http://futureofinnovation.org*

Federal support of science and engineering research in universities and national laboratories has been key to America's prosperity for more than half a century. A robust educational system to support and train the best U.S. scientists and engineers and to attract outstanding students from other nations is essential for producing a world-class workforce and enabling the R&D enterprise it underpins. But in recent years federal investments in the physical sciences, math and engineering have not kept pace with the demands of a knowledge economy, declining sharply as a percentage of the gross domestic product. This has placed future innovation and our economic competitiveness at risk.

It is essential that we act now; otherwise our global leadership will dwindle, and the talent pool required to support our high-tech economy will evaporate. *[Page 1–2]*

U.S. Commission on National Security/21st Century (Hart-Rudman Committee), *Road Map for National Security: Imperative for Change. Phase III,* January 2001. Available online at: *http://govinfo.library.unt.edu/nssg/PhaseIIIFR.pdf*

. . .[T]he U.S. Government has seriously underfunded basic scientific research in recent years. . . [T]he inadequacies of our systems of research and education pose a greater threat to U.S. national security over the next quarter century than any potential conventional war that we might imagine. American national leadership must understand these deficiencies as threats to national security. If we do not invest heavily and wisely in rebuilding these two core strengths, America will be incapable of maintaining its global position long into the 21st century. *[Page ix]*

About the Endorsing Organizations

American Society for Information Science and Technology *(http://www.asist.org)*—Since 1937, the American Society for Information Science and Technology (ASIS&T) has been the society for information professionals leading the search for new and better theories, techniques, and technologies to improve access to information.

ASIS&T brings together diverse streams of knowledge, focusing what might be disparate approaches into novel solutions to common problems. ASIS&T bridges the gaps not only between disciplines but also between the research that drives and the practices that sustain new developments.

ASIS&T counts among its membership some 4,000 information specialists from such fields as computer science, linguistics, management, librarianship, engineering, law, medicine, chemistry, and education; individuals who share a common interest in improving the ways society stores, retrieves, analyzes, manages, archives and disseminates information, coming together for mutual benefit.

Coalition for Academic Scientific Computing *(http://www.casc.org)*—CASC is a nonprofit organization of supercomputing centers, research universities and federal laboratories that offer leading edge hardware, software, and expertise in high-performance computing resources and "advanced visualization environments." Founded in 1989, CASC has grown into a national association representing 42 centers and programs in 28 states.

Coalition members complement traditional methods of laboratory and theoretical investigation by using high-performance computers to simulate natural phenomena and environmental threats, handle and analyze data and create images—all at performance levels not available from smaller computers. By applying advanced technology, CASC members help extend the state-of-the-art to achieve the scientific, technical, and information management breakthroughs that will keep the U.S. in the forefront of the 21st century information technology revolution.

Computing Research Association *(http://www.cra.org)*—The Computing Research Association (CRA) is an association of more than 200 North American academic departments of computer science, computer engineering, and related fields; laboratories and centers in industry, government, and academia engaging in basic computing research; and affiliated professional societies.

CRA's mission is to strengthen research and advanced education in the computing fields, expand opportunities for women and minorities, and improve public and policy-maker understanding of the importance of computing and computing research in our society.

Electrical and Computer Engineering Department Heads Association *(http://www.ecedha.org)*—The Electrical and Computer Engineering Department Heads Association is composed of heads or chairs of departments offering accredited programs in electrical and/or computer engineering.

The purposes of ECEDHA are threefold: help advance the field, help members exchange ideas, and improve communication with the profession, industry, government, and others.

ECEDHA membership is open to the official leaders (whether called head, chair, or some other title) of U.S. university departments offering ABET-accredited electrical and/or computer engineering (or similarly named) programs. Of about 300 departments offering such programs, almost 90 percent are currently represented in ECEDHA.

Society for Industrial and Applied Mathematics *(http://www.siam.org)*—SIAM has grown from a membership of few hundred in the early 1950s to over 10,000 members today. SIAM members are applied and computational mathematicians, computer scientists, numerical analysts, engineers, statisticians, and mathematics educators. They work in industrial and service organizations, universities, colleges, and government agencies and laboratories all over the world. In addition, SIAM has over 400 institutional members-colleges, universities, corporations, and research organizations.

U.S. Public Policy Committee of the Association for Computing Machinery *(http://www.acm.org/usacm)*—USACM is the U.S. Public Policy Committee of the Association for Computing Machinery, which is widely recognized as the premier organization for computing professionals, delivering resources that advance the computing as a science and a profession, enabling professional development, and promoting policies and research that benefit society. ACM is the world's first edu-

cational and scientific computing society with almost 80,000 members worldwide. USACM members include leading computer scientists, engineers, and other professionals from industry, academia, and government.