DEFINING FEDERAL INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT: WHO? WHERE? WHAT? WHY? AND HOW MUCH?

HEARING

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS

OF THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

JULY 7, 2004

Serial No. 108–251

Printed for the use of the Committee on Government Reform

Available via the World Wide Web: http://www.gpo.gov/congress/house
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

97–999 PDF 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 GOVERNMENT REFORM

TOM DAVIS, Virginia, *Chairman*

DAN BURTON, Indiana	HENRY A. WAXMAN, California
CHRISTOPHER SHAYS, Connecticut	TOM LANTOS, California
ILEANA ROS-LEHTINEN, Florida	MAJOR R. OWENS, New York
JOHN M. McHUGH, New York	EDOLPHUS TOWNS, New York
JOHN L. MICA, Florida	PAUL E. KANJORSKI, Pennsylvania
MARK E. SOUDER, Indiana	CAROLYN B. MALONEY, New York
STEVEN C. LATOURETTE, Ohio	ELIJAH E. CUMMINGS, Maryland
DOUG OSE, California	DENNIS J. KUCINICH, Ohio
RON LEWIS, Kentucky	DANNY K. DAVIS, Illinois
JO ANN DAVIS, Virginia	JOHN F. TIERNEY, Massachusetts
TODD RUSSELL PLATTS, Pennsylvania	WM. LACY CLAY, Missouri
CHRIS CANNON, Utah	DIANE E. WATSON, California
ADAM H. PUTNAM, Florida	STEPHEN F. LYNCH, Massachusetts
EDWARD L. SCHROCK, Virginia	CHRIS VAN HOLLEN, Maryland
JOHN J. DUNCAN, Jr., Tennessee	LINDA T. SANCHEZ, California
NATHAN DEAL, Georgia	C.A. "DUTCH" RUPPERSBERGER, Maryland
CANDICE S. MILLER, Michigan	ELEANOR HOLMES NORTON, District of Columbia
TIM MURPHY, Pennsylvania	JIM COOPER, Tennessee
MICHAEL R. TURNER, Ohio	BETTY McCOLLUM, Minnesota
JOHN R. CARTER, Texas	
MARSHA BLACKBURN, Tennessee	BERNARD SANDERS, Vermont (Independent)
PATRICK J. TIBERI, Ohio	
KATHERINE HARRIS, Florida	

MELISSA WOJCIAK, *Staff Director*
DAVID MARIN, *Deputy Staff Director/Communications Director*
ROB BORDEN, *Parliamentarian*
TERESA AUSTIN, *Chief Clerk*
PHIL BARNETT, *Minority Chief of Staff/Chief Counsel*

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS

ADAM H. PUTNAM, Florida, *Chairman*

CANDICE S. MILLER, Michigan	WM. LACY CLAY, Missouri
DOUG OSE, California	STEPHEN F. LYNCH, Massachusetts
TIM MURPHY, Pennsylvania	
MICHAEL R. TURNER, Ohio	

EX OFFICIO

TOM DAVIS, Virginia	HENRY A. WAXMAN, California

BOB DIX, *Staff Director*
URSULA WOJCIECHOWSKI, *Professional Staff Member*
JULIANA FRENCH, *Clerk*
ADAM BORDES, *Minority Professional Staff Member*

CONTENTS

DEFINING FEDERAL INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT: WHO? WHERE? WHAT? WHY? AND HOW MUCH?

WEDNESDAY, JULY 7, 2004

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,
INTERGOVERNMENTAL RELATIONS AND THE CENSUS,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:30 a.m., in room 2154, Rayburn House Office Building, Hon. Adam Putnam (chairman of the subcommittee) presiding.

Present: Representatives Putnam and Clay.

Staff present: Bob Dix, staff director; John Hambel, senior counsel; Ursula Wojciechowski, professional staff; Juliana French, clerk; Felipe Colon, fellow; Michelle Ash, minority senior legislative counsel; Adam Bordes, minority professional staff member; and Cecelia Morton, minority office manager.

Mr. PUTNAM. A quorum being present, this hearing of the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census will come to order.

Good afternoon and welcome to the subcommittee hearing on "Defining Federal Information Technology Research and Development. Who? Where? What? Why? and How much?" the purpose of this hearing is to examine the extent of Federal funding for and the leveraging of information technology research and development across agencies, academia and industry.

By addressing the basic questions, this subcommittee hopes to identify the following: How many different agencies of the Federal Government are currently engaged in conducting or managing IT research and development; is there an overall strategic plan that provides an opportunity to leverage investments, both internally and externally, and to identify complementary activities in an effort to avoid duplication; how much is being spent on an annualized basis on information technology R & D; where and how these investments are actually being made; what are the outcome measurements and expectations associated with those investments; is there a defined set of goals and objectives or focus areas that are targeted by these efforts and what have been the recent results; what is the role of the academic community and the private sector, and how are these partnerships created and maintained?

The Federal Government funds research and development to meet the mission requirements of the departments and agencies. Advances in the uses of IT research and development are continuing to change the way those Federal agencies communicate, use information, deliver services and conduct business. The technology and expertise generated by this endeavor may have applications beyond the immediate goals or intent of federally funded research and development. Federal support reflects the consensus that while basic research is the foundation for many innovations, the rate of return to society as a whole generated by investments and such work is significant.

The potential benefits of federally funded R&D related to information technology are endless. Federally funded programs have played a crucial role in supporting long term research into the fundamental aspects of computing. The unanticipated results of research are often as important as anticipated results. The Internet, electronic mail and instant messaging were by-products of government funded research from the 1960's. Another aspect of government funded IT R&D is that it often leads to open standards, something that many perceive as beneficial, encouraging deployment and further investment.

Previous oversight hearings conducted by this subcommittee have identified an important missing link in the cyber security arena that requires further attention in the research and development area. We have learned that inadequate tools exist today to conduct necessary quality assurance testing of existing and emerging software and hardware products that could better identify flaws, defects and other vulnerabilities prior to deployment. With a renewed commitment on the part of software and hardware manufacturers to quality and security of the products they introduce into the marketplace, a collaborative approach to developing more mature testing tools are essential to improved protection of computer networks and the information assets they contain.

The outcomes achieved through public and private funding programs create a synergistic environment in which both fundamental and application driven research is conducted, benefiting government, industry, academia and the public. Government funding appears to have allowed research on a larger scale and with greater diversity, vision and flexibility than would have been possible without government involvement.

It is important to recognize collaborative efforts across programs and agencies and stress the importance of leveraging efforts with academia and the private sector. Universities, private companies, and Federal labs are important partners in this endeavor. It will be productive to explore new methods to encourage increased activities by other parties in the innovation process, particularly if the goal is to continue the technological advancement which has been so instrumental to this Nation's economic growth and high standard of living.

Because investments in science and technology have resulted in unparalleled economic growth as well as the standard of living and quality of life, we must emphasize the importance of supporting the efforts of IT R&D. Advances have been possible only with the support of the public and private investment in R&D, according to the

President's budgets. Yet challenges continue. There are many R&D needs vying for a limited amount of R&D dollars. Federal research and development program managers face tough choices in deciding where the money should go and how much is appropriate for information technology.

Further, it is important to ensure that Federal agencies are not pursuing conflicting goals. It is essential that agencies, universities and industry move toward a more coordinated, unified approach. Multiple Federal agencies will need to coordinate their efforts to ensure that new understanding of information technology and network security is generated and that this knowledge is transitioned into useful products. Academia will have developed and expanded degree programs to ensure that an adequate work force exists to put new tools and techniques into practice. The private sector has a critical role to play, as it will contain the developers and suppliers as well as the major purchasers of new IT technologies and services.

Government sponsorship of research, especially in universities, helps develop the IT talent used by industry, universities, and other pieces of the economy. When companies create products using the ideas and work force that results from federally sponsored research, they repay the Nation in jobs, tax revenues, productivity increases and global leadership.

We need a strong strategic plan to ensure that IT R&D is being used to maximize improvement and mission goals and performance. federally funded research and development are key endeavors within the respective agencies and in cooperation with universities in the private sector. It is essential to meet vital Federal needs and sustain global leadership in science and in the engineering of information technology.

I welcome today's distinguished panel of witnesses and look forward to their testimony and the opportunity to explore these matters in greater detail.

At this time I would like to recognize the distinguished ranking member of the subcommittee, Mr. Clay, for his opening statement. Mr. Clay.

[The prepared statement of Hon. Adam H. Putnam follows:]

ONE HUNDRED EIGHTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5074
FACSIMILE (202) 225–3974
MINORITY (202) 225–5051
TTY (202) 225–6852

www.house.gov/reform

Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census

Congressman Adam Putnam, Chairman

OVERSIGHT HEARING
STATEMENT BY ADAM PUTNAM, CHAIRMAN

Hearing topic: ***"Defining Federal Information Technology Research and Development: Who? Where? What? Why? and How Much?"***

Wednesday, July 7, 2004
1:30 p.m.
Room 2154, Rayburn House Office Building

OPENING STATEMENT

Good afternoon and welcome to the Subcommittee's hearing on "Defining Federal Information Technology Research and Development: Who? Where? What? Why? and How Much?" The purpose of this hearing is to examine the extent of Federal funding *for* and leveraging *of* information technology (IT) research and development (R&D) across agencies, academia and industry.

By addressing the basic questions, this Subcommittee hopes to identify the following: how many different agencies of the Federal government are currently engaged in conducting or managing IT research and development activities; is there an overall strategic plan that provides an opportunity to leverage investments, both internally and externally, and to identify complimentary activities in an effort to avoid duplication; how much is being spent on an annualized basis on information technology R&D, where and how these investments are actually being made, what are the outcome measurements and expectations associated with these investments; is there a defined set of goals and objectives or focus areas that are targeted by these efforts and what have been the recent results; what is the role of both the academic community and the private sector, and how are these partnerships created and maintained?

The Federal government funds research and development to meet the mission requirements of the departments and agencies. Advances in the uses of IT R&D are continuing to change the way that federal agencies communicate, use information, deliver services and conduct business. The technology and expertise generated by this endeavor may have applications beyond the immediate goals or intent of federally funded research and development. Federal support reflects a consensus that while basic research is the foundation for many innovations, the rate of return to society as a whole generated by investments in such work is significant.

The potential benefits of federally funded R&D related to information technology are endless. Federally funded programs have played a crucial role in supporting long-term research into fundamental aspects of computing. The unanticipated results of research are often as important as the anticipated results. The Internet, electronic mail and instant messaging, for instance, were by-products of government-funded research in the 1960s. Another aspect of government-funded IT R&D is that it often leads to open-standards, something that many perceive as beneficial, encouraging deployment and further investment.

Previous oversight hearings conducted by this Subcommittee have identified an important missing link in the cyber security arena that requires further attention in the research and development arena. We have learned that inadequate tools exist today to conduct necessary quality assurance testing of existing and emerging software and hardware products that could better identify flaws, defects and other potential vulnerabilities prior to deployment. With a renewed commitment on the part of software and hardware manufacturers to quality and security of the products they introduce into the marketplace, a collaborative approach to developing more mature testing tools are essential to the improved protection of computer networks and the information assets they contain.

The outcomes achieved through public and private funding programs create a synergistic environment in which both fundamental and application-driven research is conducted, benefiting government, industry, academia and the public. Government funding appears to have allowed research on a larger scale and with greater diversity, vision, and flexibility than would have been possible without government involvement.

It is important to recognize collaborative efforts across programs and agencies, and stress the importance of leveraging efforts with academia and the private sector. Universities, private companies, and federal laboratories are important partners in this endeavor. It will be productive to explore new methods to encourage increased activities by other parties in the innovation process, particularly if the goal is to continue the technological advancement, which has been so instrumental to this Nation's economic growth and high living standard.

Because investments in science and technology have resulted in unparalleled economic growth, as well as the standard of living and quality of life, we must emphasize the importance of supporting the efforts of IT R&D. Advances have been possible only with the support of both public and private investment in R&D, according to the President's budget. However, challenges continue. There are many R&D needs vying for a limited amount of R&D dollars. Federal R&D program managers face tough choices in deciding where the R&D money should go and how much is appropriate for information technology.

Furthermore, it is important to ensure that federal agencies are not pursuing conflicting R&D goals. It is essential that agencies, universities and industry move toward a more coordinated, unified goal. Multiple Federal agencies will need to coordinate their efforts to ensure that new understanding of information technology and network security is generated and that this knowledge is transitioned into useful products. Academia will have develop and expand degree programs to ensure that an adequate workforce exists to put the new tools and techniques into practice. The private sector has a critical role to play, as it will contain the developers and suppliers as well as the major purchasers of new information technologies and services.

Government sponsorship of research, especially in universities, helps develop the IT talent used by industry, universities and other parts of the economy. When companies create products using the ideas and workforce that results from federally sponsored research, they repay the nation in jobs, tax revenues, productivity increases and world leadership.

We need a strong strategic plan to ensure that IT R& D is being used to maximize improvement in mission goals and performance. Federally funded research and development are key endeavors within the respective agencies and in cooperation with academia and the private sector. It is essential to meet vital Federal needs and sustain U.S. global leadership in science and in the engineering of information technology.

######

Mr. CLAY. I thank the chairman for holding today's hearing on what is an important but often overlooked portion of our government's research and development portfolio. The Federal Government will spend approximately $60 billion on the many different components of information technology during fiscal year 2004. In contrast, the fiscal year 2004 budget only allocates $2.2 billion for the Networking and Information Technology Research and Development Program, a minimal amount considering the role of higher performance computing and technology in our mission to enhance government efficiency, accessibility and security for all citizens.

Although funding for IT research and development has increased fourfold since 1990, along with an increased coordination throughout multiple agency participants for such activity, there is a disconnect between the level of government funding and its importance in the development of a strong IT work force and premier academic institutions.

Furthermore, the government's role in IT research and development fosters the creation of common criteria and open standards that both government and private industry can utilize for their benefit. When focused, the government's investments in IT research often results in jobs, economic growth, and a higher standard of living in both quantitative and qualitative terms. Moreover, such resources permits our Nation to remain on the cutting edge of technology in vital areas, including health care, education, manufacturing, and the basic sciences.

This concludes my remarks, Mr. Chairman, and I ask that they be included in the record.

[The prepared statement of Hon. Wm. Lacy Clay follows:]

STATEMENT OF CONGRESSMAN CLAY ON FEDERAL IT RESEARCH & DEVELOPMENT (7/7)

I thank the Chairman for holding today's hearing on what is an important, but too often overlooked, portion of our government's research and development portfolio.

The federal government will spend approximately $60 billion on the many different components of information technology during fiscal year 2004. In contrast, the FY 2004 budget only allocates $2.2 billion for the Networking and Information Technology Research and Development program—a minimal amount considering the role of high-performance computing and technology in our mission to enhance government efficiency, accessibility, and security for all citizens.

Although funding for IT research and development has increased four-fold since 1990, along with an increased coordination throughout multiple agency participants for such activities, there is a disconnect between the level of government funding and its importance in the development of a strong IT workforce and premier academic institutions.

Furthermore, the government's role in IT research and development fosters the creation of common criteria and open standards that both government and private industry can utilize for their benefit.

When focused, the government's investments in IT research often results in jobs, economic growth, and a higher standard of living in both quantitative and qualitative terms. More, such resources permits our nation to remain on the cutting edge of technology in vital areas including health care, education, manufacturing, and the basic sciences.

This concludes my remarks, Mr. Chairman, and I ask that they be included in the record.

Mr. PUTNAM. Without objection, they will be included in the appropriate place in the record.

At this time we will move to the administration of the oath. If our witnesses would please rise and raise your right hands.

[Witnesses sworn.]

Mr. PUTNAM. Note for the record that all the witnesses responded in the affirmative, and we will move to our first panel's testimony. I would ask that all of our panelists adhere to the 5-minute rule for your opening statements and we will have successive rounds of questions from the panel to get to all of your issues.

Our first witness is Dr. David Nelson. Dr. Nelson is the Director of the National Coordination Office for IT Research and Development and a member of the Senior Executive Service. He is responsible for the coordination of planning, budget and assessment activities for the Federal networking and information breakthrough that advance the science of IT.

Dr. Nelson is cochair of the Interagency Working Group for the NITRD program. Dr. Nelson joined the NCO from NASA, where he was Deputy CIO with primary responsibility for information technology security of all NASA systems and additional responsibilities in scientific computing and enterprise architecture. He previously served at the Department of Energy, which he joined from Oak Ridge National Labs, where he was research scientist working mainly in theoretical plasma physics and its applications to fusion energy. He is the author of numerous papers in theoretical plasma physics, computational science and research policy. He has twice received the President's Meritorious Rank Award for superior sustained managerial performance.

Welcome to the subcommittee. You are recognized for 5 minutes, Dr. Nelson.

STATEMENTS OF DR. DAVID NELSON, DIRECTOR, NATIONAL COORDINATION OFFICE FOR INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT (EXECUTIVE OFFICE OF THE PRESIDENT); DR. PETER FREEMAN, CO-CHAIR OF INTERAGENCY WORKING GROUP AND ASSISTANT DIRECTOR, COMPUTER AND INFORMATION SCIENCE AND ENGINEERING DIRECTORATE, NATIONAL SCIENCE FOUNDATION; DR. HRATCH SEMERJIAN, ACTING DIRECTOR, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY; AND DR. C. EDWARD OLIVER, ASSOCIATE DIRECTOR, OFFICE OF ADVANCED SCIENTIFIC COMPUTING RESEARCH, U.S. DEPARTMENT OF ENERGY

Dr. NELSON. Thank you, Mr. Chairman and members of the subcommittee. I have submitted my written testimony to the subcommittee and ask that it be entered into the record, and I will limit my oral testimony to a brief summary of four points.

Let me start by saying that I agree with many of your opening comments, both from the majority and the minority side, with regard to the importance of information technology research and development, and I think that agreement will be shown through my oral testimony.

First, I would like to discuss the Networking and Information Technology Research and Development Program. This program derives from authorization in the High Performance Computing Act of 1991.

For fiscal year 2005 the President's budget requests slightly over $2 billion for the program in 13 participating agencies. The program supports long-range research as well as research infrastructure, such as research computer centers and research networks. Performers include universities, Federal research centers and laboratories, national laboratories and federally funded research and development centers, private companies, and nonprofit organizations. Research is funded by the participating agencies through grants, cooperative agreements, contracts, and other authorities. The agencies work together under the program to identify research needs, plan research programs, and review progress.

I brought along one copy of planning research needs. This is in the high confidence software and systems research area and was developed by one of the coordinating groups under the program.

Agencies may coordinate their selection of research performers through joint solicitations and coordinated proposal reviews. The program interacts with stakeholders through workshops and other meetings and disseminates research results through publications, reports and presentations. Often activities under the program are conducted jointly with other Federal programs that benefit from information technology.

Historical accomplishments include the High Performance Computing and Communications Initiative in the early 1990's that helped create modern computational science, parallel supercomputers, the modern Internet and Mosaic, the first graphical Web browser. The Next Generation Internet Initiative in the late 1990's helped to create the technology for today's high bandwidth optical networks and demonstrated the basis for today's high performance network computing.

The program receives advice and guidance from the President's Information Technology Advisory Committee, which was authorized in the High Performance Computing Act. Members of the committee are drawn from the private sector, and I believe Dr. Ed Lazowska, cochair of the committee, is testifying before the subcommittee today.

Let me turn to my second main point. This concerns the value of the government's historical investment in information technology research. In 1995, the National Research Council documented the return on this investment. The study cited numerous examples of information technologies whose roots lay in federally funded research or that were nurtured through critical development periods by Federal research. Examples include network technology in the Internet, the Web browser, computer windowing, computer graphics, reduced instruction set computers, design of very large scale integrated circuits, data storage technology, and parallel computing architecture.

In 1999, the National Research Council extended its 1995 conclusions, citing additional contributions to technology and to the economy. Federal information technology research also returns value directly to government operations through at least two pathways, the first through government purchase of commercial off-the-shelf information technology products that have been invented or improved through Federal research. The second pathway is through the development of special information technology needed for government missions. This is clearly shown in the government's research and development programs, where many of the specialized information technologies have been invented or developed by the Networking and Information Technology R&D Program, often in direct partnership with the program intending to use those technologies.

Let me turn to my third point. This concerns the value of current Federal investments in IT research. The Networking and Information Technology R&D Program is currently working in areas such as improving the quality and reliability of software, improving the security of operating systems, applications and networks, making it easier and more productive for humans to interact with computer systems, including access by individuals with disabilities, managing resources distributed over the Internet, applying computer modeling and simulation to scientific and engineering fields, detecting and responding to natural or man-made threats, managing information intensive dynamic systems and supporting lifelong learning.

Of perhaps special interest to this subcommittee is research in information security. Federal agencies are funding applied research to better enable us to cope with security weaknesses in the architecture of operating systems, networks and applications, as well as fundamental research, investigating ways to improve the intrinsic security of these architectures. The President's Information Technology Advisory Committee is currently studying this area and will issue recommendations regarding Federal research investments.

A specific example of the value of current Federal investment concerns Google, and it may serve to illustrate the value of this research generally. The Digital Libraries Initiative is an ongoing part of the program that has been sponsored by NSF, NASA, DARPA, and NIH. A recent article points out that Google, the search engine company that is about to issue a very significant initial public offering of stock, owes its technology directly to a Digital Libraries Initiative grant to Stanford University. Under this grant the cofounders of Google invented, developed and tested their search algorithms.

My final point concerns the management of IT research. Federal research programs have benefited from talented research managers in the agencies and in funded projects. Because research deals directly with the unknown and unanticipated, it must be managed deftly. Often research failure becomes success, as intractable obstacles point the way to alternative approaches. Both Federal program managers and researchers must have good instincts regarding when to continue the proposed research and when to abandon or modify it.

Structures for managing and overseeing federally funded research should allow program managers to alter projects in midcourse in response to preliminary results and need to recognize that research projects can produce valuable results even if they do not achieve their original objectives. Failure to manage deftly risks stifling creativity and innovation. The history of information technology research demonstrates the benefits of a flexible approach, and this approach is consistent with the administration's R&D investment criteria.

This concludes my remarks. I thank the committee for the opportunity to testify.

[The prepared statement of Dr. Nelson follows:]

Statement of Dr. David B. Nelson
Director, National Coordination Office for
Information Technology Research and Development
to the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census of the Committee on Government Reform,
U.S. House of Representatives
On Federal Information Technology Research and Development
July 7, 2004

Mr. Chairman and members of the Subcommittee, I am pleased to meet with you to discuss federal information technology research and development.

I am the Director of the National Coordination Office for Information Technology Research and Development under the National Science and Technology Council (NSTC), and I co-chair, with my colleague Dr. Peter Freeman of the National Science Foundation, the Interagency Working Group for Networking and Information Technology Research and Development (NITRD). The NITRD program includes unclassified research and development activities of thirteen federal agencies, organized in seven Program Component Areas. It derives from authorization in the High Performance Computing Act of 1991 (Public Law 102-194), as amended.

The NITRD Program

For Fiscal Year 2005 the President's Budget requests $2.008 billion for the NITRD Program.[1] Detail at the level of Program Component Area is not yet available for Fiscal Year 2005. This level of detail is available for Fiscal Year 2004 and is presented in Table 1, which summarizes the NITRD Program activities and requested funding for Fiscal Year 2004. This table is taken from *Networking and Information Technology Research and Development: Supplement to the President's Budget for Fiscal Year 2004*, often referred to as the "Blue Book."[2] The total request of $2.147 billion for the FY 2004 NITRD program is an allocated or "crosscut" amount, rather than an aggregate of line items, because agencies describe their projects with differing terms. Table 1 also gives the names and requested funding for each of the seven Program Component Areas. Additional information regarding the NITRD program is contained in congressional testimony[3] recently presented by Dr. John H. Marburger, III, Director, White House Office of Science and Technology Policy.

The NITRD Program supports long-range research as well as research infrastructure such as computer centers and research networks. Research is performed at universities, federal research centers and laboratories, national laboratories and federally funded research and development centers, and private companies and non-profit organizations.

---

[1] http://www.ostp.gov/html/budget/2005/FY05NITRDfinal.pdf
[2] http://www.itrd.gov/pubs/blue04/index.html
[3] http://www.house.gov/science/hearings/full04/may13/marburger.pdf

Historical accomplishments of the NITRD Program and its predecessors include the High Performance Computing and Communications (HPCC) Initiative in the early 1990s and the Next Generation Internet (NGI) Initiative in the late 1990s. The HPCC initiative helped to create modern computational science and today's parallel supercomputers, demonstrated the intimate link between computing and networks, and created the graphical web browser. The NGI initiative helped to create the technology for today's high-bandwidth optical networks and demonstrated the value of distributed computing using high-bandwidth networks, forming the basis for today's grid computing.

Agencies participating in NITRD work together to identify research needs, plan research programs, and review progress. Often agencies coordinate their selection of research performers through joint or coordinated announcements and mutual assistance in proposal review. The program includes numerous interactions with stakeholders through workshops and other meetings and wide dissemination of research results through publications, reports, and presentations. Often activities under the NITRD Program are conducted jointly with other research programs to enhance knowledge and technology transfer.

The President's Information Technology Advisory Committee (PITAC), authorized by the High Performance Computing Act, provides advice and guidance to the NITRD Program. PITAC is governed by the provisions of the Federal Advisory Committee Act; its members are drawn from the private sector. The current PITAC Co-Chairs are Dr. Ed Lazowska, professor of computer science at the University of Washington, who is testifying before the Subcommittee today, and Marc Benioff, Chief Executive Officer of Salesforce.Com. At its next meeting, scheduled for June 17, 2004, PITAC will consider draft recommendations for the contribution of information technology research and development to health care and will discuss the preparation of recommendations in the two areas of cyber security research and computational science.

A notable example of the processes used by the NITRD Program is the recently published *Federal Plan for High-End Computing: Report of the High-End Computing Revitalization Task Force.*[4] This plan was developed during a year of planning under the auspices of the NSTC by more than sixty federal research managers, including representatives from fields of science and engineering that use high-end computing. Input from stakeholders was obtained through a major workshop organized by the Computing Research Association[5], white papers solicited as part of the workshop, and non-disclosure briefings by companies involved in high-end computing. Participating agencies are now working together to incorporate planned activities into their programs. An early result is the High-End Computing University Research Activity,[6] sponsored by the Defense Advanced Research Projects Agency (DARPA), The Department of Energy Office of Science (DOE/SC), and the National Science Foundation (NSF) and solicited through two coordinated research announcements. This activity supports long-lead academic research necessary to revitalize high-end computing.

---

[4] http://www.itrd.gov/pubs/2004_hecrtf/20040510_hecrtf.pdf
[5] http://www.cra.org/Activities/workshops/nitrd/
[6] http://www.itrd.gov/hecrtf-outreach/hec-ura/index.html

Another closely related example is the High Productivity Computing Systems (HPCS) Program led by DARPA. The HPCS Program precedes development of the *Federal Plan for High-End Computing* and is key to its success. This program seeks to improve productivity of technical computers that might be available in the mid-term, a need shared by all NITRD agencies. Several agencies participate in planning and assessing progress of the HPCS Program and have adjusted their own programs to complement the HPCS Program.

Two examples illustrate how the NITRD Program works with other programs and communities to invent and apply advances in information technology. The first example is the Information Technology Research (ITR) Program of NSF, which has funded projects under its several science and engineering directorates to advance and incorporate information technology into science and engineering. This program specifically aims at rapid transfer of advances in information technology to disciplines that benefit from them. The Digital Government Program is perhaps of interest to this Subcommittee, because it funds research cooperatively with other branches of government specifically to improve government effectiveness through advanced information technology. The second example is the Scientific Discovery through Advance Computing (SciDAC) Program in DOE/SC. This program directly links information technology research with the other research programs of the Office of Science to quickly recognize and apply opportunities for information technology to improve effectiveness of the sciences.

Agencies participate in NITRD activities according to their mission needs. Research agencies such as NSF and DARPA tend to focus their NITRD work on longer term research and underlying technology. Mission agencies such as the National Institutes of Health (NIH), the Agency for Healthcare Research and Quality, the National Oceanic and Atmospheric Administration, and the Environmental Protection Administration focus more on applying basic NITRD advances to their mission activities, such as biomedicine, health care, climate, weather, and the environment. Other mission agencies such as the National Aeronautics and Space Administration, the National Institute of Standards and Technology, and DOE/SC participate both in underlying research and applications of that research. Defense agencies such as the Department of Defense and DOE's National Nuclear Security Administration participate through open, unclassified research and apply results to their classified national security missions.

A few agencies, such as the Federal Aviation Administration, the Food and Drug Administration, and the General Services Administration, associate with the NITRD Program as observers, contributing research needs and incorporating research advances into their operations.

Value of Historical Federal Investments in Information Technology Research and Development

"Success has many fathers,"[7] yet studies attest to the unique role of Federal information technology research and development investments in creating the information age. In

[7] Attributed to Philip Caldwell

1995 the National Research Council concluded in a Congressionally chartered study[8] of the HPCC Initiative that "Federal investment in information technology research has played a key role in the U.S. capability to maintain its international lead in information technology." The study cited numerous examples of information technologies whose roots lay in Federally funded research or that were nurtured through critical development periods by Federal research funds. These include network technology and the Internet, the Web browser, windowing, computer graphics, reduced instruction set computers, very large scale integration design, storage technology known as RAID,[9] and parallel computing architecture.

In 1999 the National Research Council studied the role of Federal investment in information technology research and development.[10] The study concluded that "Federal funding not only financed development of most of the nation's early digital computers, but also has continued to enable breakthroughs in areas as wide ranging as computer time-sharing, the Internet, artificial intelligence, and virtual reality as the industry has matured. Federal investment also has supported the building of physical infrastructure needed for leading-edge research and the education of undergraduate and graduate students who now work in industry and at academic research centers." The study also stated that, "The effects of federal support for computing research are difficult to quantify but pervasive. Patent data, although a limited indicator of innovation, provide strong evidence of the links between government-supported research and innovation in computing. More than half of the papers cited in computing patent applications acknowledge government funding."

The 1999 National Research Council Study pointed out that information technology has had profound implications, stating:

> "The computer revolution is not simply a technical change; it is a sociotechnical revolution comparable to an industrial revolution. The British Industrial Revolution of the late 18th century not only brought with it steam and factories, but also ushered in a modern era characterized by the rise of industrial cities, a politically powerful urban middle class, and a new working class. So, too, the sociotechnical aspects of the computer revolution are now becoming clear. Millions of workers are flocking to computing-related industries. Firms producing microprocessors and software are challenging the economic power of firms manufacturing automobiles and producing oil. Detroit is no longer the symbolic center of the U.S. industrial empire; Silicon Valley now conjures up visions of enormous entrepreneurial vigor."

Of course, these words were written before the bursting of the dot-com bubble, but the growth of the information technology industry continues, and the use of information technology has recently led to significant productivity increases in broad sectors of the U.S. economy.

U.S. companies have unquestionably led the information technology revolution, and Federal research funding has built the basis for many of these companies through idea

[8] *Evolving the High Performance Computing and Communications Initiative to Support the Nation's Infrastructure*, National Academy Press, Washington, D.C., 1995
[9] RAID is an acronym for redundant arrays of inexpensive disks.
[10] *Funding a Revolution: Government Support for Computing Research*, National Academy Press, Washington, D.C., 1999.

generation and training of future entrepreneurs. As the 1999 study points out, "Many of these entrepreneurs had their early hands-on computer experience as graduate students conducting federally funded university research." Fortune favors the company that is first to market with new technology through higher margins, greater market share, and a stronger role in standards. It is no surprise then that most of the world's largest and most successful information technology companies are American and that most information technology standards are based on American technology.

The NITRD Program returns value directly to government operations through at least two pathways. The first is through Government purchase of commercial off the shelf (COTS) information technology products – hardware, software and services – that have been invented or improved through federal research. Today the government uses mostly COTS information technology, and even when custom development is undertaken, the development tools are usually COTS. The second pathway is the development of special information technology needed for Government missions. This is clearly shown in the Government's research and development programs, where many of the specialized information technologies have been invented or developed by the NITRD Program, often in direct partnership with the program intending to use these technologies, as described earlier in this testimony.

Value of Current Federal Investments in Information Technology Research and Development

The value of today's research in the NITRD Program can only be based on prediction, and "predicting is difficult, especially about the future."[11] Nonetheless, if we extrapolate from the past, we can be confident that today's investments will have large payoff. The NITRD Program is working in areas such as

- Improving the quality and reliability of software
- Improving the security of operating systems, applications, and networks
- Making it easier and more productive for humans to interact with computer systems, including facilitating access by individuals with disabilities.
- Managing resources distributed over the Internet
- Developing and applying computer modeling and simulation to fields as diverse as medicine, manufacturing, energy, environment, climate and weather, and nanotechnology
- Detecting and responding to natural or man-made threats
- Managing information-intensive dynamic systems
- Supporting life-long learning

Each of these areas has application to important economic, social, and/or national security needs. Of perhaps special interest to this Subcommittee is research on information security, because of its importance to Government operations. Federal agencies are funding applied research to better enable us to cope with security weaknesses in the basic architectures of operating systems and networks, as well as fundamental research investigating ways to improve the intrinsic security in the architecture of information systems and networks. The value of the latter is that if

[11] Attributed to Yogi Berra.

successful it would eliminate the security weaknesses of current architectures. The difficulty is that even if methods to improve intrinsic security are found, they must be compatible with legacy technology and protocols. An example of this research is the NSF Cyber Trust Program, whose awards will soon be announced.

Two examples may serve to illustrate the value of current research programs. The first is the return on the Digital Libraries Initiative, an ongoing part of the NITRD Program that has been sponsored by NSF, NASA, DARPA, and later NIH. A recent article[12] points out that Google, the search engine company that is about to issue a very significant initial public offering of stock and whose name has entered the vocabulary as a verb, owes its technology directly to a Digital Libraries Initiative grant. As the article states,

> "Google was founded by Larry Page and Sergei Brin – two computer science graduate students at Stanford University. Stanford was one of a number of universities that received funding under the "Digital Libraries Initiative" – supported by the National Science Foundation, NASA, and the Defense Advanced Research Projects Agency… The goal of the initiative, launched in 1994, was to 'dramatically advance the means to collect, store, and organize information in digital forms, and make it available for searching, retrieval, and processing via communication networks - all in user-friendly ways.' Larry Page was funded under the DLI as a graduate student researcher, and Sergei Brin was supported with an NSF graduate student fellowship. Page and other Stanford researchers created an algorithm called PageRank. It ranks the importance of each Web page based on the number and importance of other Web pages that link to it. This technological advance enabled Page and Brin to develop a search engine that found useful and relevant information, which was critical to Google's popularity. Google was also prototyped on equipment paid for by the federal government's Digital Library Initiative."

The second example is the ongoing NITRD work on grid computing, supported by several agencies in close collaboration with other research communities. The goal of grid computing is to make it easy to manage and use large-scale computing and data storage resources located anywhere on the network. Among the problems to be solved are the efficient transport of large data sets, synchronization of distributed data bases, access to and management of distributed information technology resources, security and privacy provisions that work across disparate organizations, simple user interfaces that hide the complexity of underlying protocols, and compatibility with legacy technology. Even though the initial applications are to scientific research, commercial information technology applications can also benefit from grid technology. Not surprisingly, several computer companies including IBM, Hewlett Packard, Microsoft, and Oracle are working closely with the grid computing research community and are already offering commercial products and services based on this technology. They are also providing feedback to the research community regarding the practicality of the grid services being developed.

Managing Federal Information Technology Research and Development

The NITRD Program has benefited from talented research leaders and managers in the participating agencies and supported organizations. Because research deals centrally with the unknown and unanticipated, it must be managed deftly. Often research "failure" becomes success, as intractable obstacles point the way to alternative approaches. Both

[12] http://www.americanprogress.org/site/pp.asp?c=biJRJ8OVF&b=71217

Federal program managers and researchers must have good instincts regarding when to continue the proposed research and when to abandon or modify it. Milestones and benchmarks are helpful in some types of project but can be stultifying in others, especially when they mandate following unproductive paths. The 1999 National Research Council study referenced previously[8] provides cogent recommendations regarding successful management of information technology research:

> "Scientific and technological research explores the unknown; hence, its outcomes cannot be predicted at the start--even if a clear, practical goal motivates the work.... Moreover, even research projects that do not achieve their original objectives can produce meaningful results or generate valuable knowledge for guiding future research efforts.... Other projects show meaningful returns only after a long time because their applications are not immediately recognized or other technological advances are needed to make their usefulness evident....
>
> "Such difficulties frustrate attempts to meaningfully measure the performance of research and also highlight the need for ensuring flexibility in the management and oversight of federally funded research programs. Researchers need sufficient intellectual freedom to follow their intuition and to modify research plans based on preliminary results.... Building such flexibility into federal structures for managing research requires both skilled program managers--who understand, articulate, and promote the visions of researchers--and an organizational culture that accepts and promotes exploratory efforts....
>
> "Clearly, there are limits to the flexibility that researchers and program managers can be allowed. In development-oriented programs, for example, program managers must ensure that specific objectives are met. In exploratory research, program managers must ensure that research funds are used prudently. But such accountability must be balanced against the unpredictability of research. Structures for managing and overseeing federally funded research need to allow program managers to alter programs midcourse in response to preliminary results and need to recognize that research projects can produce valuable results even if they do not achieve their original objectives. Failing to do so risks stifling creativity and innovation. The history of computing demonstrates the benefits of a flexible approach."

The experience of the NITRD program managers has shown that these are valuable recommendations, and that following them has contributed to the success of the NITRD Program. These concepts are also consistent with the R&D Investment Criteria,[13] which the Administration uses to guide all federal R&D programs.

Conclusion

Thank you for giving me the opportunity to testify before the Subcommittee. I would be pleased to answer any questions that you might have.

---

[13] http://www.whitehouse.gov/omb/memoranda/m03-15.pdf

Agency NITRD Budgets by Program Component Area

FY 2003 Budget *Estimates* and FY 2004 Budget Requests (dollars in millions)

Agency	High End Computing Infrastructure and Applications (HEC I&A)	High End Computing Research and Development (HEC R&D)	Human Computer Interaction and Information Management (HCI & IM)	Large Scale Networking (LSN)	Software Design and Productivity (SDP)	High Confidence Software and Systems (HCSS)	Social, Economic, and Workforce (SEW)	Totals
NSF (2003) estimates	*211.7*	*76.0*	*128.8*	*109.0*	*53.4*	*63.8*	*65.9*	*708*
NSF (2004) requests	218.1	97.9	125.3	103.4	55.0	59.9	74.0	734
NIH	*77.1*	*37.8*	*93.1*	*128.8*	*6.8*	*3.7*	*12.1*	*359*
NIH	87.6	41.7	99.0	132.2	9.2	3.7	12.2	386
NASA	*35.2*	*26.0*	*40.8*	*12.6*	*55.8*	*34.7*	*4.2*	*209*
NASA*	45.9	34.6	67.1	28.9	59.2	24.2	6.7	267
DARPA		*109.9*	*42.9*	*47.6*	*58.6*	*3.2*		*232*
DARPA		108.5	78.4	18.2	13.3	4.0		222
DOE Office of Science	*98.4*	*37.3*	*16.2*	*28.7*			*3.5*	*184*
DOE Office of Science	88.9	51.3	16.4	30.0			3.5	190
AHRQ			*6.4*	*5.2*				*12*
AHRQ			32.0	25.0				57
NSA		*51.3*		*2.1*		*28.1*		*82*
NSA		21.3		1.9		28.1		51
NIST	*3.5*		*6.2*	*3.2*	*7.5*	*2.0*		*22*
NIST	3.5		6.2	3.2	7.5	2.0		22
NOAA	*13.5*	*1.8*	*0.5*	*2.8*	*1.5*			*20*
NOAA	13.5	1.8	0.5	2.8	1.5			20
EPA	*1.6*		*0.2*					*2*
EPA	1.6		0.2					2
ODDR&E		*3.6*	*2.0*	*4.7*	*1.0*	*0.7*		*12*
ODDR&E								
Subtotals	*441.0*	*343.6*	*337.1*	*314.6*	*184.6*	*136.2*	*85.6*	[illegible]
Subtotals	459.1	357.1	425.1	345.5	145.7	122.0	96.4	1,951
DOE/NNSA	*40.5*	*37.5*		*13.5*	*31.3*		*4.4*	*127*
DOE/NNSA	41.5	37.3		14.4	32.8		4.4	130
DISA						*6.1*		*6*
DISA			46.2	13.2		6.1		66
TOTALS[b]	*481.5*	*381.1*	*337.1*	*328.1*	*215.9*	*142.3*	*90.0*	*1,976*
TOTALS[b]	500.6	394.4	471.3	373.3	178.5	128.1	100.8	2,147

Notes:

[illegible] NASA FY 2004 budget reflects full cost.

[b] These totals include discrepancies from what appears in the President's FY 2003 and FY 2004 budgets due to a combination of rounding and shifts in program estimates.

Table 1. Fiscal Year 2004 NITRD Program and Budget Request

Mr. PUTNAM. Thank you very much. I would ask the remaining witnesses to please try to adhere to our 5-minute rule and check the lights on the table.

Our next witness is Dr. Peter Freeman. Dr. Freeman is the assistant director for the Computer and Information Science and Engineering Directorate. He was previously at Georgia Institute of Technology as professor and founding dean of the College of Computing since 1990. From 1987 to 1989 he served as division director for computer and computational research at the National Science Foundation and helped to formulate the High Performance Computing and Communications Initiative of the Federal Government. In addition to his many activities as dean at Georgia Tech, he headed an NSF-funded national study of the IT worker shortage, started an active group for deans of IT and computing, and published several papers relating to future directions of the field. He received his Ph.D. in computer science from Carnegie Mellon, his M.A. in mathematics and psychology from UT Austin, and his B.S. in Physics from Rice. His research and technical expertise has focused on software systems and their creation.

We welcome you to the subcommittee. You are recognized.

Dr. FREEMAN. Thank you, Chairman Putnam, Ranking Member Clay. Good afternoon. It is a pleasure to be here this afternoon and to have the opportunity to testify before you and to discuss information technology R&D. Let me begin by clarifying some terms that I think we will all be using this afternoon.

It is important to understand that the subject of today's hearing, IT R&D, is open to multiple interpretations that can lead to misunderstandings and to differences in reported activity levels. For example, it is often reported that a company spends a huge sum on IT R&D, but a closer examination almost always reveals that the vast majority of that sum is actually spent on development, not research. In the past, the term "information technology" was usually taken to refer to data processing activities such as payroll, accounting or inventory, not the full range of work to which the term now often refers. I would note that the Federal R&D community primarily uses the more general meaning of the term "information technology."

Definitions of research and development are notoriously overlapping and often lumped together. In the technical community, research generally refers to activities that produce new knowledge, while development refers to the use of existing knowledge to produce new systems, products or practices. Even these very general definitions are open to much interpretation and practice. An important distinction, however, is that research is usually targeted more broadly to longer term and must be provided a very broad and loose type of oversight, while development usually has very specific targets, has a shorter timeframe, and requires a project management type of oversight.

Let me now outline two frameworks for discussing Federal activity in this area. The first separates IT from its usage. Very simply, it is often useful to differentiate between IT activity and IT-enabled activity. For example, a research project we are currently supporting at NSF, an assessment of voting technology and ballot design, seeks to provide an assessment of information technologies relative to on-line voting and ballot design. This is certainly IT research. It may lead to some IT development of, for example, better e-voting systems, but use of those systems would certainly be IT-enabled activity.

The second framework that I would note is the one we use to report Federal activity in this area. The major research emphases of the NITRD effort are called program component areas, and those are spelled out in what we call the Blue Book, our annual supplement to the President's budgets.

Let me now turn to the questions expressed in your letter of invitation. The first question was who is doing IT research and development? I believe, as Dr. Nelson has already indicated, at least 13 agencies or major subareas of larger agencies report work in the NITRD program that is self-identified as research. Non-U.S. Government personnel perform the majority of that work, as Dr. Nelson has indicated. There is undoubtedly additional IT research supported by the government and of course a very large amount of development, as Ranking Member Clay's opening statement made note of.

The second question was where are these investments being made. I think it is fair to say that there is some amount of investment in every State, in every research university and essentially every company capable of providing research service to the U.S. Government.

Your third question is what is government gaining from these investments. In general, government is gaining directly from the technical base used by our military and for streamlined governmental operations and indirectly by fostering the continuing economic revolution that provides the innovation, productivity and economic vigor for our Nation as a whole.

Your fourth question was why should government continue to make those investments. I can only add that as industry often and publicly stresses, it is because federally funded research is essential to the continued advancement of IT technology.

Your final question, how much is being spent by the Federal Government? I believe that within the stated caveats, the crosscuts listed in our annual Blue Book provide a good compilation of Federal research activity in this area.

In conclusion, let me thank you for the opportunity to appear before you today. I would ask that my fuller written statement be entered into the record. I will be glad to respond to your questions.

[The prepared statement of Dr. Freeman follows:]

Testimony of
Dr. Peter A. Freeman
Assistant Director, National Science Foundation
for
Computer and Information Science and Engineering (CISE)
and
Co-Chair, Interagency Working Group on NITRD

Before the U.S. House of Representatives
Committee on Government Reform
Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census

July 7, 2004

Good afternoon, Mr. Chairman and members of the Committee. I am Dr. Peter Freeman, NSF's Assistant Director for Computer and Information Sciences and Engineering, and Co-Chair of the Interagency Working Group (IWG) on Networking and Information Technology Research and Development (NITRD).

INTRODUCTION

I am glad to have the opportunity to testify before you this afternoon and to discuss the topic "*Defining Federal Information Technology Research and Development: Who? Where? What? Why? and How Much*?" As you know, information technology (IT) is vital to all operations of the government and is an essential component of the U.S. economy. I am always appreciative of the opportunity to help key decision makers understand this area better and the key role that government-funded research plays in making sure our Nation remains in a strong leadership position.

In the spirit of your letter of invitation "to provide the Subcommittee with a better understanding" of the scope of IT R&D and its impact on the Federal government, and because others on the panels today will also address your questions, I will first focus my testimony on some general issues that I believe will assist you in developing that deeper understanding. I will then address your specific questions directly. I will be glad to amplify these remarks in response to follow-up questions at the hearing.

TERMS AND A FRAMEWORK FOR DISCUSSION

It is important to understand that the subject of today's hearing is open to different interpretations, both abstractly and in practice. This can lead to misunderstandings and differences in reported activity levels.

For example, it is often reported in industry that a particular company spends a huge sum on IT R&D, sometimes specifically in an organization labeled "research." Closer examination, however, always reveals that the vast majority of that sum is spent on development, not research, even though it may be carried out in an organization with "research" in its title. The same confusion, of course, often occurs in discussing governmental activities.

Thus, let me begin by explicating the terms of the hearing subject, as I believe they are in current use, and by describing the framework used within the Federal research community for discussing them. This will then permit me to respond to your specific questions more effectively.

What is Information Technology?

"Information technology," until perhaps the past decade, was usually taken to refer to data processing as done by large organizations such as the government (in the sense of payroll, accounting, inventory, and other such systems), not the full range of computer- and communications-enabled work to which the term now often refers. This transition in usage is still underway, but for some time, the Federal R&D community has primarily used the more general definition as can be seen in the title of the IWG for NITRD itself.

Distinction Between "Research" and "Development"

Definitions of "research" and "development" are notoriously overlapping and often lumped together in a single category of "R&D." In the technical community, "research" generally refers to activities that produce new knowledge (or technology) while "development" refers to the use of existing knowledge (and technology) to produce new artifacts (systems, products, practices). Even these very general definitions are open to much interpretation in practice, however, since one can often find descriptions of a "research project" which is primarily focused on discovering *new knowledge not currently known to a particular organization*, even though it may have been known to others for a long time.

An important distinction at the core, however, is that research is usually targeted more broadly, is longer-term, and must be provided a broad type of oversight, while development usually has very specific targets, has a shorter time frame, and requires a project-management type of oversight. A related, practical distinction is that research is done by people who view themselves (and are viewed by their peers) as "researchers", while development is done by "developers." For example, NSF/CISE has initiated the Cyber Trust emphasis area this year which will fund about $30M of basic research aimed at improving the security and predictability of computer systems even when they are under cyber attack, at assuring that sensitive information flowing in public computer systems is consistent with public policies about where that information may flow, and at expanding the workforce competent to build and operate such systems. We expect a variety of research results to flow from this work so that perhaps three to five years from now specific development projects can be initiated that will utilize some of these results to build more secure information systems for the government on a specific timetable.

Who Does IT R&D?

This example illustrates another reality. "Federal" activity in IT R&D is not only, or even primarily in the case of research, done by Federal employees. While two of today's panelists represent organizations that perform some amount of IT R&D "in-house," the bulk of "Federal" IT research is performed in non-US-Government organizations, notably universities. Likewise, while the government employs thousands of IT developers, much of the government's development work is done by outside contractors. A notable recent example is the recent DHS award of a multi-billion IT system development contract to a commercial organization. While I am not conversant with the technical details of this project, based on my experience with other large government systems, I believe it is fair to say that essentially no research will be done on that project but that it will be based almost entirely on the results of research over many years, much of which were supported in part or entirely by Federal funds.

Inclusion of Networking, Separation of Chip Technology

Two final definitions need to be made. First, while "networking" is specifically named in the title of the IWG, it generally is included in the term IT since modern networking depends heavily on the IT component of a network. This is a fairly recent (past twenty years perhaps) usage since communications networks (telephone, radio) not based on computers pre-date the modern computer age. Second, as one peels back the layers of a modern IT system, one eventually reaches the underlying hardware such as computer chips. Integrated circuit technology is, of course, a fundamental driver of and part of IT technology, but for the most part the R&D essential to its advancement is considered a separate topic.

IT Activity Differentiated from IT-Enabled Activity

Let me turn now to two frameworks for discussing Federal activity in IT R&D. The first separates IT from its usage. In a study[1] I co-authored several years ago, we found it very useful to differentiate between IT activity and *IT-enabled* activity. Thus, a research project currently supported by NSF/CISE, "An Assessment of Voting Technology and Ballot Design[2]" seeks to provide an "assessment of information technologies relative to on-line voting and ballot design." This is certainly "IT research," which may lead to some "IT development" of better e-voting systems, but electronic voting would be an "IT-enabled" activity. Similarly, *research* into new computer architectures might enable future *development* of specialized computers, but their usage for weather prediction (or other tasks) would be *IT-enabled activity.*

---

[1] *The Supply of Information Technology Workers in the United States,* http://www.cra.org/reports/wits/cra.wits.html

[2] http://www.digitalgovernment.org/projectHighlight/149.pdf

NITRD Program Component Areas (PCA's)

The second is the framework[3] used by the IWG for NITRD to report Federal activity in this area. Despite the fact that NITRD includes a D for *development*, it is important to note that in practice the NITRD focus is primarily on research i.e. the creation of new IT knowledge not currently known to any organization.

The major *research* emphases of the NITRD effort are called Program Component Areas (PCA's):

- High End Computing Infrastructure and Applications
- High End Computing Research and Development
- Human Computer Interaction and Information Management
- Large Scale Networking
- Software Design and Productivity
- High Confidence Software and Systems
- Social, Economic, and Workforce

The work of each PCA is guided by a Coordinating Group (CG) of agency program managers. These groups, which report to the IWG, meet monthly to coordinate planning and activities of the multi-agency projects in their specialized research areas. The PCA's evolve in response to changing research needs. Overall, NITRD accounts for an approximate annual US Government investment in IT research of $2B.

My co-chair, Dr. David Nelson, and I initiated a thorough review of the definitions of these PCA's last year by the various Coordinating Groups. Their assessment after several months of study and discussion was that in the main these areas still describe the current structure of the field. There is, of course, overlap and some amount of interpretation of just where a specific activity might appear.

For example, in September 2002, NSF organized a workshop entitled: "New Vistas in CIP Research and Development: Secure Network Embedded Systems." The focus was on interdependencies of critical infrastructure systems, the need for integral security, and the increasingly distributed nature of these systems. Implications were considered for SCADA and air traffic control. Just from this short description, one can see that subject matter covered by several PCA's was involved, as well as IT-enabled activity (air traffic control); and for that matter, should a workshop devoted to identifying needed research be classified as "research" at all?

In spite of these definitional issues, the PCA's continue to provide a useful framework for developing a comprehensive, cross-cutting look at Federal and Federally-supported research activity in IT. They do not, however, address the issue of development of IT systems in the operational sense.

[3] See http://www.nitrd.gov/iwg/program.html for a fuller description.

Let me now turn to the questions expressed in your letter of invitation.

SPECIFIC QUESTIONS

Given the above discussion, my particular responsibilities on the IWG, and as head of the largest funder of Federal IT research, I will succinctly address your questions in the context of the NITRD program. The annual "Blue Book" supplement to the President's budget[4] provides comprehensive examples and budgetary crosscuts.

"Who is doing IT research and development?"

At least thirteen agencies or major sub-areas of larger agencies report work in the NITRD program that is self-identified as *research* in the main. Non-US Government personnel, largely at universities and contractors, perform the majority of this work. Given the size of the Federal government and the looseness of definitions, there is undoubtedly additional research supported by the government. For example, it is well known that the Armed Services support some amount of IT research and that is most likely not accounted for in our crosscuts. Again, as noted above, the focus of the NITRD program is on research, so that development projects (such as the DHS project mentioned above) are not included.

"Where are these investments being made?"

Given the breadth of some of the funding programs, especially at NSF and NIH, it is fair to say that there is some amount of investment in every state, every research university (over 200), many colleges, and essentially every company capable of providing research service to the US Government.

"What is government gaining from these investments?"

The annual Blue Book referenced above provides numerous, well-illustrated examples of the results of this research and how, in many cases, they directly address the requirements and programs of the US Government. Many studies have been published of the value of IT research to the Nation and to the government, such as one[5] chaired by one of today's panel members, Dr. William Scherlis, and an earlier report[6] that addressed some of the research needs for a national information infrastructure which has now become essential to the operation of government. In general, the government is gaining directly from the technical base that underlies our military might and governmental operations, while enabling in ways that industry cannot a continuing economic revolution that provides the innovation, productivity, and economic vigor for our Nation.

---

4 http://www.nitrd.gov/pubs/blue04/index.html
5 http://books.nap.edu/html/itr_e_gov/
6 http://www.nap.edu/catalog/4948.html)

"Why should the government continue to make these investments?"

I believe that my answer to the previous question largely addresses this. I would only underscore the point that as industry repeatedly and publicly stresses (for example, the CEO of Intel[7]) Federally-funded research is essential to the continued advancement of IT technology because it produces the basic ideas, innovations, and workforce development that industry cannot in general afford to do.

"How much is being spent by the Federal government and how many projects exist?"

As noted above, I believe that within the stated caveats the crosscuts listed in the annual Blue Book provide a good compilation of Federal research activity in this area. It is important to note that for a complex activity of this magnitude (approximately $2 billion in FY2004) and for which definitions are subject to so much interpretation, it is inevitable that reports done at different times and with differing definitions will produce different results.

CONCLUSION

Thank you for the opportunity to appear before you today. I will be glad to respond to your questions.

7 http://www.computerworld.com/managementtopics/management/itspending/story/0,10801,92552,00.html?nas=AM-92552)

Mr. PUTNAM. Thank you very much.

Our next witness is Dr. Hratch Semerjian, who is serving as Acting Director of NIST. He has served as the Deputy Director of NIST since July 2003. In this position Dr. Semerjian is responsible for overall operation of the institute, including financial management, human resource management facilities and information technology systems, effectiveness of NIST technical programs and for interactions with international organizations.

Dr. Semerjian received his Master's and Ph.D. Degrees in engineering from Brown in 1977. He joined the National Bureau of Standards, now known as NIST, where he served as director of the Chemical Science and Technology Laboratory from April 1992 through July 2003. He has received countless awards and we welcome him to the subcommittee today.

You are recognized for 5 minutes.

Dr. SEMERJIAN. Thank you, Chairman Putnam and Ranking Member Clay. Thank you for the opportunity to testify about NIST's contributions to Federal information technology research and development.

The impacts of information technology on the United States and the world economy are certainly well known. NIST plays a critical role in building trust and confidence in information technologies and development of secure, reliable and interoperable IT systems. NIST's programs help to ensure that the U.S. industry maintains the competitive advantage vis-a-vis the rest of the world while ensuring that U.S. Government information technology assets remain secure.

Twenty-first century science is being pushed by continuing progress in computing information and communication technology and pulled by the expanding complexity, scope and scale of today's technological challenges. Information technology is providing the potential for the research community to build new types of scientific and engineering knowledge and to pursue research in new ways and with increased efficacy. The key to these breakthroughs is achieving the necessary functionality, interoperability, usability, confidence and data protection within the IT systems that will lead the way.

NIST is at the forefront of these developments. I'd like to give you just a few highlights from our information technology program which will give you a flavor of the wide array of expertise that exists at NIST. For example, NIST ensures the security, confidentiality, integrity and availability of information by providing standards and guidelines, testing methodologies, and other Federal Information Processing Standards [FIPS], in compliance with legislation such as the Computer Security Act, the Federal Information Security Management Act and the Cyber Security Research and Development Act.

NIST helps mitigate the cost of inadequate software testing, which is estimated to be around $60 billion, by developing test methodologies for software assurance and conformity to IT standards.

NIST develops tests and measurement technology that keys the implementation, robust operation, and continuity of operations of the Nation's core networking infrastructure, especially to assure the robustness of the systems under various failure and recovery scenarios.

NIST enables efficient access, manipulation, and exchange of complex information through advances in human language technology that enhances context extraction, question answering and speech-to-text capabilities.

And NIST provides analytical, statistical and computational tools for solving scientific and engineering problems. Some of these tools, for example, are currently being used in the analysis of the World Trade Center collapse. We are also collaborating with the semiconductor industry to create a Web-based electronic handbook of statistical methods.

Through these efforts, NIST has developed world class competencies in cyber security, software, networks information access, mathematics, statistics and interoperability. This bundle of competencies, combined with Nobel prize winning expertise in the physical sciences, places NIST in a unique position to create an enormous impact on the economy and innovation enterprise in the United States. It is precisely this unique capability that attracts industry and other Federal agencies to collaborate with NIST. And let me highlight some of these specific efforts where NIST's expertise is being put to direct use.

For example, NIST works with industry to ensure the interoperability of technology specifications. Interoperability is essential to productivity and competitiveness of many industries because efficient design and manufacturing require the coordination of many different participants and processes that rely on a digital representation of the product. To mitigate the billion dollar annual cost just to the automotive supply chain, NIST has initiated the NIST manufacturing business-to-business operability test beds, for example.

NIST assists government and industry in protection of the U.S. borders through the development of biometrics evaluation systems, standards and research. Two recent laws recognize this expertise and provide specific requirements for NIST, the U.S. Patriot Act and the Enhanced Border Security and Visa Reform Act.

NIST enhances trust and confidence in voting systems. The Help America Vote Act provides NIST with mandates in the areas of security, hardware and software interoperability and human factors issues. Under HAVA, NIST just recently released a study on human factors which will be used to improve the performance and reliability of voting machines.

And looking more into the future, NIST makes revolutionary advances in quantum communications and computing. This is really important for the future of the country, because quantum communications offers the promise of perfectly protected messages, while quantum computing offers the promise of dramatically increased computing power.

NIST also utilizes information technology for knowledge management. I think we have a knowledge-based economy, and both the creation and dissemination of knowledge is a very important part of what we do at NIST.

NIST works with other Federal agencies, academia and industry to develop and promote openness and interoperability of information technology. We work with other agencies to provide expertise in our own unique areas of research to DOD, DHS, HHS, DOJ and others. We also participate in the Interagency Working Group on Information Technology R&D, and we also cooperate with industry on integrating information-based manufacturing systems and development of the measurement and standards infrastructure needed for the application of intelligence systems in manufacturing, defense and homeland security.

In fiscal year 2004, the NIST Information Technology Laboratory received about $48 million in appropriated funds. In addition, ITL received about $17 million from other agencies on a reimbursable basis. These are the words with M, not the B. The President's 2005 budget request has an increase of $7 million for the NIST IT budget.

In conclusion, NIST takes its roles in maintaining the vitality of the U.S. information technology industry seriously in providing unique expertise to the rest of the government and in sharing with industry, government and universities the basic science and technology that comes from its measurement and standards research. These brief examples of our work and accomplishments illustrate NIST's commitment to these roles. They also demonstrate the base upon which NIST continues to build.

This concludes my prepared remarks. Thank you.

[The prepared statement of Dr. Semerjian follows:]

Statement of

Dr. Hratch G. Semerjian
Acting Director

National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Before the

House of Representatives
Committee on Government Reform
Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census

"Defining Federal Information Technology Research and Development: Who? Where? What? Why? and How Much?"

July 7, 2004

Chairman Putnam and Members of the Committee, thank you for this opportunity to testify today about the contributions of the National Institute of Standards and Technology (NIST) to Federal information technology research and development. I would like to address the questions you asked in your invitation to testify and tell you about some of the important activities currently underway at NIST.

The benefits that information technology has had on the United States and world economy are well known. NIST plays a critical role in building trust and confidence in information technologies and the continued development of secure, reliable, usable and interoperable IT with ground-breaking studies on technology performance, development of state-of-the art automated testing techniques, guidelines and standards for securing systems, and leadership of international standardization programs. NIST's programs help to ensure that U.S. industry maintains the competitive advantage vis-à-vis the rest of the world while ensuring that U.S. government information technology assets remain secure.

Our mission is to develop and promote measurement science, standards, and supporting programs in information technology in order to enhance productivity, facilitate trade, and improve the quality of life. We work in partnership with industry, academia, government—civilian and military, and consortia to develop and demonstrate tests, test methods, reference data sets, proof-of-concept implementations, and other information infrastructure technologies. Our goal is to enable the information technology industry in the United States to produce high quality reliable, interoperable, and secure products and services. Nowhere else in the world is there a laboratory dedicated to understanding the metrics of information technologies, and the development of tools and tests to enable industry and users to build better systems through the understanding of these metrics. Nowhere else in the federal government is there an organization dedicated to working with U.S. industry to improve the trust and confidence of IT, particularly scientific systems that are crucial to the continued competitive advantage of the United States in the international community.

A new age is dawning for scientific and engineering research, pushed by continuing progress in computing, information, and communication technology, and pulled by the expanding complexity, scope and scale of today's challenges. These information technology advancements provide the potential for the research community to build new types of scientific and engineering knowledge environments and organizations and to pursue research in new ways and with increased efficacy.[1] The acknowledged key to these breakthroughs is achieving the necessary functionality, interoperability, usability, confidence, and data protection within the IT systems that will lead the way.

NIST is at the forefront of this new age. The information technology research at NIST is focused on building the trust and confidence in today's and tomorrow's systems. Trust and confidence covers the range of IT systems: advances in modeling and simulation to complement the advances in the physical sciences; secure, robust, quality software; agile, resilient, robust networks that continue to operate under catastrophic conditions; and integrity, availability, interoperability and reliability of the systems, data and networks. We have a unique collection of scientists working collaboratively from computer scientists to chemists, electrical and

[1] *Revolutionizing Science and Engineering Through Cyberinfrastructure*, NSF, March 2003.

mechanical engineers and physicists striving to meet the challenge of trust and confidence in IT in the nanoscale revolution and beyond.

I would now like to mention some highlights from our major Information Technology program areas which will give you a flavor of the wide array of expertise and effort resident at NIST:

NIST ensures the security, confidentiality, integrity, and availability of information. NIST has a long-standing, highly successful role in working with Federal agencies and industry to ensure the protection of information technology and systems through standards and guidelines, testing methodologies, conformity assessment and complementary supporting research. These activities emanated from necessity and were formalized in legislation such as the Computer Security Act, the Federal Information Security Management Act, and the Cyber Security Research and Development Act. These efforts, often codified in Federal Information Processing Standards (FIPS), have led to increased protection of government information. NIST is also leading global efforts to develop secure smart card technologies and travel documents, and to achieve consensus on various electronic authentication strategies.

NIST mitigates the $59.5 billion cost of inadequate software testing. NIST is the world leader in development of test methodologies for software assurance and conformity to IT standards. NIST maintains a robust program in software that is fundamental to the continued growth of the IT industry. We facilitate electronic commerce through development of XML tests, while also developing test methods and registries to improve the interoperability, quality, conformance, and correctness of healthcare information data transfer. Our expertise in software extends to the field of computer forensics; a program which enables the detection of computer crime and successful prosecution of terrorists and other criminals.

NIST develops test and measurement technology that keys the implementation, robust operation, and continuity of operations of the nation's core networking infrastructure. We have the premier capability in the world for modeling and simulating the performance of large networks under various failure and recovery scenarios, which enables more consistent service of the internet. Our broad ranging program also works with the public safety community and industry to develop modern, interoperable communication and networking standards for first responders.

NIST enables intuitive, efficient access, manipulation, and exchange of complex information. NIST continues to make strides in improving our customers' ability to use information technology and the underlying information. These efforts have brought advances to human language technology that enhances content extraction, question answering, and speech-to-text capabilities. Tremendous strides have also occurred in the usability and accessibility of information through the testing of NIST labs.

NIST is a world leader in analytical, statistical, and computational methods for solving scientific and engineering problems. We continue to provide technical leadership in state-of-the-art analytical and computational methods for the scientific and engineering world. The mathematics program develops, analyzes, and solves mathematical models of physical phenomena; develops highly efficient parallel computational models to enable scientific advancement; develops and distributes mathematical software tools and tests; and continues development of the Digital Library of Mathematical Functions, a comprehensive, authoritative web-based interactive reference on the special functions of applied mathematics. NIST also continues to provide the statistical underpinnings that strengthen scientific research through formulation and development of statistical theory and methodology for metrology. The program develops new statistical methods for the design and analysis of Key Comparisons forming the basis of international trade; develops statistical methods to evaluate IT performance in networks, biometrics, and computer forensics; and characterizes complex instruments, systems, and processes in mathematical terms, including the analysis of the World Trade Center collapse. In cooperation with Sematech, NIST created the popular Web-based e-Handbook of Statistical Methods, which is a fundamental global reference.

NIST works to ensure the interoperability of technology specifications. Interoperability is essential to productivity and competitiveness of many industries because efficient design and manufacturing require the coordination of many different participants and processes that rely on a digital representation of the product. To mitigate the $1 billion annual cost to members of the automotive supply chain, NIST has initiated the NIST Manufacturing B2B Interoperability Testbed to address the needs for demonstration and testing of B2B standards. The testbed is an on-going effort to mobilize software vendors, manufacturers, standards organizations, and other stake-holding parties to enhance the capability for on-demand demonstration and testing of interoperability of enterprise application in a B2B setting.

Through these efforts NIST has developed world-class competencies in security, software, networks, information access, mathematics, statistics, and interoperability. This bundle of competencies, combined with Nobel prize winning expertise in the physical sciences places NIST in a unique position to create an enormous impact on the economy and scientific research. It is precisely this unique capability that attracts funding from other agencies. We continually leverage our expertise and this funding to protect this Nation and position the US as a leader in the information technology and scientific arenas. I would like to again highlight some specific NIST efforts:

NIST assists government and industry in protection of the US border through the development of biometrics evaluation systems, biometrics standards, and biometrics research. Working with the biometric community, NIST has long been recognized as an expert in the use of biometric information. Two recent laws recognized this expertise and provided specific requirements for NIST, the USA PATRIOT Act and the Enhanced Border Security and Visa Entry Reform Act. Under these laws, NIST has refined programs in fingerprint testing, face testing, multimodal biometrics evaluation, multimodal system design, and standards.

NIST enhances trust and confidence in voting systems. The core of democracy is the voting system. The Help America Vote Act seeks to increase trust and confidence in the voting system, in part by providing NIST with mandates in the areas of security, hardware/software interoperability, and human factors issues. Under HAVA, NIST recently released a study titled: "Improving the Usability and Accessibility of Voting Systems and Products" which established a roadmap for voting constituencies, vendors and users to achieve increased trust and confidence that the voting system accurately reflects the will of the electorate.

NIST makes revolutionary advances in quantum communications and computing. Quantum communications offers the promise of perfectly protected messages while quantum computing offers the promise of dramatically increased computing power. NIST is developing the measurements and standards infrastructure to enable future development of information systems based on the principles of quantum physics. NIST's two Nobel Laureates are focused on this effort.

NIST utilizes information technology to find knowledge in large data sets. NIST has the most comprehensive array of chemical, physical, and engineering measurements data of any group worldwide working in science and technology. NIST cost-effectively manages this data by developing accessible IT resources, including web-based data dissemination and single-portal access to all these databases, while using statistical and mathematical methodology to make sense of the data.

NIST works with partners in other Federal agencies, academia, and industry to develop and promote openness and interoperablility in information technology. It works with other agencies not only on a bilateral basis, where it furnishes expertise in its unique areas of research to the DoD, HHS, NIH, DOJ and others, but also through support and cooperation within the Interagency Working Group on Information Technology Research and Development. Examples of NIST IT cooperation with industry include electronic commerce and various aspects of U.S. manufacturing. One focus is on integrating information-based manufacturing systems. Another effort is aimed at developing the information-based measurement and standards infrastructure needed for the application of intelligent systems in manufacturing, defense, and homeland security. In a related effort, the NIST Combinatorial Methods Center develops methods that lead to innovations in materials science faster, cheaper, and better. Developing these methods requires a significant emphasis on IT research, as strategies for managing and analyzing the overwhelming amount of data generated are a critical problem for the Center and its industrial partners.

Providing security to supervisory control and data acquisition (SCADA) systems-- systems that monitor and control power flows in the electric power grid –involves significant IT research, as SCADA systems are increasingly IT-based. NIST is evaluating the performance of a number of promising security systems under development to ensure security while not compromising the performance of the power grid. In a similar way, cybernetic building systems involve information handling at many different levels of building services (e.g., fire detection, security and transport systems, energy management, and utilities). The NIST program which includes a full-scale demonstration of cybernetic building systems, involves a significant amount of IT research to develop a standards-based information infrastructure.

NIST is careful to utilize its unique attribute of being an unbiased, neutral third-party to best enhance the efforts of industry where it is needed most. The impact of NIST programs on the IT industry, the Federal government, the security of IT infrastructure, and security of the American people is broad and deep. The standards, tests and measures that NIST enables are also key to the continued competitive advantage of the United States. NIST's efforts in information technology measurement, standards, and interoperability provide a unique contribution to the advancement of IT that would not otherwise be performed.

NIST received FY 2004 appropriated funding of $48.6 million, which is supplemented by a number of other agencies by $17 million. In addition, now before the Congress is the President's FY 2005 budget request that includes a proposed increase of $7 million for NIST to address key national needs in cyber security and accelerate solutions to critical cyber security issues ($6 million) and to address the biometric requirements of the USA Patriot Act by developing the standards for testing the accuracy of biometric technologies ($1 million). This specifically includes working with the Department of Homeland Security through its Science and Technology Directorate, as well as the Information Analysis and Infrastructure Protection Directorate's National Cyber Security Division to enhance collaborative efforts begun in 2003. This proposed expansion of NIST's current program will allow for additional deliverables in FY 2005 and a critical start to long-term work in key areas including:

- Enhancing security, critical infrastructure application, and communication protocols;
- Expanding the NIST Cryptographic Toolkit to include limited power, small-sized computing environments;
- Improving broken wireless security standards by identifying, prioritizing, and accelerating approaches to securing wireless devices;
- Developing metrics to understand, express, and improve our ability to build secure networks and systems from individually understood components; and
- Developing advanced means to cost-effectively control access of individuals and automated services to information and other automated services.

In conclusion, NIST takes its roles in maintaining the vitality of the U.S. information technology industry seriously, in providing unique expertise to the rest of the government, and in sharing with industry, government and universities the basic science and technology that comes from its measurement and standards research. These brief examples of our work and accomplishments illustrate NIST's commitment to these roles. They also demonstrate the base upon which NIST continues to build.

This concludes my prepared remarks. I will be pleased to answer your questions.

Mr. PUTNAM. Thank you very much.

Our final witness for this panel is Dr. Carl Edward Oliver. Dr. Oliver is the Associate Director of the Office of Advanced Computing Research for the Office of Advanced Science at the Department of Energy. He is responsible for basic research and applied mathematics, computer science and networking needs in the Office of Science. His duties include management of the Small Business Innovative Research Program.

Dr. Oliver came to DOE under the Intergovernmental Personnel Act from Sandia National Laboratories. Prior to that he was the associate laboratory director for computing robotics and education at Oak Ridge National Lab from 1995 to 2000. After receiving his Ph.D. in mathematics in 1969 as a NASA fellow from the University of Alabama, he held research and management positions at the Air Force Weapons Lab, the Air Force Office of Scientific Research and DOE.

He has also held teaching positions at six universities, been active on a national and international level organizing professional society meetings for numerous academic societies and has served on several university and Federal advisory committees and others under the auspices of the OSTP and the National Science Foundation.

Welcome to the subcommittee. You are recognized for 5 minutes.

Dr. OLIVER. Mr. Chairman, I too commend you for holding this hearing and I appreciate the opportunity to testify on behalf of the Department of Energy's Office of Science on a matter of importance to the Nation; namely, information technology research.

Dr. David Nelson and Dr. Freeman have given you some overview of the Federal IT R&D activities. I'll concentrate on those areas of the portfolio where the Office of Science focuses its efforts: High performance computing, large scale networks and software that enables scientists to use these resources as tools for scientific discovery.

Ever since the inception as part of the Atomic Energy Commission immediately following World War II, the Office of Science has blended cutting edge research and innovative problem solving to keep the United States at the forefront of scientific discovery. Since the 1940's, the Office of Science supported the work of more than 40 Nobel prize winners. Research supported by the office has made major contributions to the United States in research areas such as magnetic resonance imaging, medical isotopes, composite materials used in motor vehicles and x-ray diagnostic of computer chips and other high tech materials.

Other research investments have led to such innovations as the Nobel prize winning discovery of new forms of carbon, noninvasive detection of cancers and other diseases, improved computer models for understanding global climate change and new insights into the fundamental nature of matter and energy.

High end computing has become an indispensable tool for researchers across the Office of Science. Large multi-disciplinary teams of researchers that combine the expertise of physicists, chemists or biologists with the expertise of computer scientists and mathematicians are working on the next generation of computational science tools that will enable the discovery and design or advance of materials for the development of catalysts that dramatically reduce the energy costs and emissions and understanding of the dynamics of combustion systems. Each of these examples and many more will have a significant effect on the missions of the Department of Energy and then the missions of other U.S. Government agencies.

High performance networks play a critical role as well because they make it possible to overcome the geographical distances that often hinder science by making all the scientific resources readily available to scientists, regardless of their physical location. In this area, we work in close coordination with the National Science Foundation and university consortia such as Internet II to ensure that scientists at universities can seamlessly access unique DOE facilities and their scientific partners in DOE laboratories.

To develop these tools we also work closely with other agencies. A significant part of the coordination has been described by Dr. Nelson already. In high end computing we cochaired the High End Computing Revitalization Task Force that was put together. This task force identified our Nation's critical needs in a report released in May, and they proposed a game plan to improve U.S. computing capabilities.

The Office of Science and other Federal agencies are working to implement the recommendations of the task force report and to develop the next generation of supercomputing capability as well as networks needed to allow the broadest possible access to new systems.

On May the 12th of this year, Secretary Spencer Abraham announced that the Department of Energy will provide $25 million in this fiscal year to a team led by Oak Ridge National Laboratory to begin to build a new supercomputer for scientific research. This is an important step toward achieving our leadership goals. When complete, researchers will gain the ability to understand the natural world with the precision that could only be imagined a few years ago.

It's clear that working with our computing industry, we can build these tools. The administration has developed a clear path forward for revitalizing high end computing, and with vital support from the Congress and administration I am confident we will succeed.

Once again, thank you for the opportunity to testify before the committee on this important matter.

[The prepared statement of Dr. Oliver follows:]

Testimony of Dr. C. Edward Oliver
Associate Director, Office of Science, U.S. Department of Energy
before the
Subcommittee on Technology, Information Policy,
Intergovernmental Relations and the Census
Committee on Government Reform
U.S. House of Representatives

July 7, 2004

Mr. Chairman and members of the Committee: I commend you for holding this hearing. I appreciate the opportunity to testify on behalf of the Department of Energy's (DOE) Office of Science (SC) on a subject of importance to this Nation, Information Technology Research. I will focus today on those areas where DOE-SC directs its efforts: high-performance computing, large-scale networks, and the software that enables scientists to use these resources as tools for scientific discovery.

***

Mr. Chairman, for more than half a century, every President and each Congress has recognized the vital role of science in sustaining this Nation's leadership in the world.

Ever since its inception as part of the Atomic Energy Commission immediately following World War II, the Office of Science has blended cutting-edge research and innovative problem solving to keep the U.S. at the forefront of scientific discovery. In fact, since the mid-1940's, the Office of Science has supported the work of more than 40 Nobel Prize winners, testimony to the high quality and importance of the work it underwrites.

The Office of Science is the single largest supporter of basic research in the physical sciences in the United States, providing more than 40 percent of total Federal funding. It oversees – and is the principal Federal funding agency of – the Nation's research programs in high-energy physics, nuclear physics, and fusion energy sciences.

The Office of Science manages fundamental research programs in basic energy sciences, biological and environmental sciences, and computational science. In addition, the Office of Science is the Federal Government's largest single source of funds for materials and chemical sciences, and it supports unique and vital parts of U.S. research in climate change, geophysics, genomics, life sciences, and science education.

The Office of Science manages this research portfolio through six interdisciplinary program offices: Advanced Scientific Computing Research, Basic Energy Sciences, Biological and Environmental Research, Fusion Energy Sciences, and High Energy Physics and Nuclear

Physics.

The Office of Science also manages 10 world-class laboratories, which often are called the "crown jewels" of our national research infrastructure. The national laboratory system, created over a half-century ago, is the most comprehensive research system of its kind in the world. The 10 Office of Science laboratories are: Ames Laboratory, Argonne National Laboratory, Brookhaven National Laboratory, Fermi National Accelerator Laboratory, Thomas Jefferson National Accelerator Facility, Lawrence Berkeley National Laboratory, Oak Ridge National Laboratory, Pacific Northwest National Laboratory, Princeton Plasma Physics Laboratory and the Stanford Linear Accelerator Center.

The Office of Science oversees the construction and operation of some of the Nation's most advanced R&D user facilities, located at national laboratories and universities. These include particle and nuclear physics accelerators, synchrotron light sources, neutron scattering facilities, supercomputers and high-speed computer networks. Each year these facilities are used by more than 18,000 researchers from universities, other government agencies and industry.

The Office of Science is a principal supporter of graduate students and postdoctoral researchers early in their careers. About 50 percent of its research funding goes to support research at 250 colleges, universities, and institutes nationwide.

***

The Administration recognizes the importance of high-performance computing for the Nation. A recent plan developed by the High End Computing Revitalization Task Force (http://www.itrd.gov/pubs/2004_hecrtf/20040510_hecrtf.pdf.) encourages DOE's Office of Science and other Federal agencies to work together to develop the next generation of advanced scientific computational capability for the benefit of America's scientific enterprise.

The elements of this plan include a coordinated research strategy to address critical barriers in high-performance computing for key Federal missions in science and national security as well as a strategy for providing a portfolio of high-performance computing resources for scientists and engineers in the U.S. The Office of Science invests in high-performance computing and networks to deliver the full benefit of this revolution to U.S. science. Of course in these areas of IT research DOE-SC works with other Federal agencies to deliver the science and the facilities the nation needs. To the maximum possible degree, access to these resources should be open to all U.S. researchers--whether they work for the government, universities, or industry--on a competitive, peer reviewed basis.

Advanced scientific computing is central to DOE's missions. It is essential to simulate and predict the behavior of nuclear weapons and aid in the discovery of new scientific knowledge. The importance of advanced scientific computing and networks to DOE is underscored in the DOE strategic plan (http://strategicplan.doe.gov/full.pdf)

> Strategy 6: Significantly advance scientific simulation and computation, applying new approaches, algorithms, and software and hardware combinations to address the critical science challenges of the future.

And Goal 6 of the Office of Science Strategic Plan (http://www.science.doe.gov/Sub/Mission/Strategic_Plan/Feb-2004-Strat-Plan-screen-res.pdf)

> Deliver forefront computational and networking capabilities to scientists nationwide that enable them to extend the frontiers of science, answering critical questions that range from the function of living cells to the power of fusion energy.

In fact, in fulfilling its mission over the years, the Office of Science has played a key role in scientific computation and networking. Consider some of the innovations and contributions made by DOE's Office of Science:

- helped develop the Internet;
- pioneered the transition to massively parallel supercomputing in the civilian sector;
- began the computational analysis of global climate change;
- developed many of the computational technologies for DNA sequencing that have made possible the unraveling of the human genetic code;
- simulated combustion reactions with the goal of reducing emissions.

***

Computational modeling and simulation rank among the most significant developments in the practice of scientific inquiry in the latter half of the 20th century and are now a major force for discovery in their own right. In the past century, scientific research was extraordinarily successful in identifying the fundamental physical laws that govern our material world. At the same time, the advances promised by these discoveries have not been fully realized, in part because the real-world systems governed by these physical laws are extraordinarily complex. Computers help us visualize, test hypotheses, guide experimental design, and most importantly determine if there is consistency between theoretical models and experiment. Computer-based simulation provides a means for predicting the behavior of complex systems that can only be described empirically at present. Since the development of digital computers in mid-century, scientific computing has greatly advanced our understanding of the fundamental processes of nature, e.g., fluid flow and turbulence in physics, molecular structure and reactivity in chemistry, and drug-receptor interactions in biology. Computational simulation has even been used to explain, and sometimes predict, the behavior of such complex natural and engineered systems as weather patterns and aircraft performance.

Within the past two decades, scientific computing has become a contributor to essentially all scientific research programs. It is particularly important to the solution of research problems that are (i) insoluble by traditional theoretical and experimental approaches, e.g., prediction of future climates or the fate of underground contaminants; (ii) hazardous to study in the laboratory, e.g., characterization of the chemistry of radionuclides or other toxic chemicals; or (iii) time-consuming or expensive to solve by traditional means, e.g., development of new materials, determination of the structure of proteins, understanding plasma instabilities, or exploring the limitations of the "Standard Model" of particle physics. In many cases, theoretical and experimental approaches do not provide sufficient information to understand and predict the behavior of the systems being studied. Computational modeling and simulation, which allow a description of the system to be constructed from basic theoretical principles and the available experimental data, are keys to solving such problems.

We have moved beyond using computers to solve very complicated sets of equations to a new regime in which scientific simulation enables us to obtain scientific results and to perform discovery in the same way that experiment and theory have traditionally been used to accomplish those ends. We must think of computation as the third of the three pillars that support scientific discovery, and indeed there are areas where the only approach to a solution is through high-end computation.

High performance networks play a critical role as well in allowing researchers to overcome the geographical distances that often hinder science. The Office of Science maintains a state-of-the-art high-speed Energy Science network, ESnet, which ensures that scientific resources are readily available to scientists around the world. DOE-SC works closely with the National Science Foundation and university consortia such as Internet 2 to ensure that scientists at universities can seamlessly access unique DOE facilities and their scientific partners in DOE laboratories.

***

To develop systems capable of meeting the challenges faced by DOE, universities, and industry, the Office of Science invests in several areas of computation: high-performance computing, large-scale networks, and the software that enables scientists to use these resources as tools for discovery. The FY 2005 President's Request for the Office of Science includes $204 million for ASCR for IT R&D and approximately $20 million in the other Offices to support the development of the next generation of scientific simulation software for SC mission applications.

As a part of this portfolio the Office of Science supports basic research in applied mathematics and the computer science needed to underpin advances in high-performance computers and networks for science.

In FY 2001 the Office of Science initiated the Scientific Discovery through Advanced Computing (www.science.doe.gov/SciDAC/) effort to leverage our basic research in mathematics and computer science and integrate this research into the scientific teams that extend the frontiers of science across DOE-SC. We have assembled interdisciplinary teams and collaborations to develop the necessary state-of-the-art mathematical algorithms and software, supported by appropriate hardware and middleware infrastructure, to use terascale computers effectively to advance the fundamental scientific research at the core of DOE's mission.

All of these research efforts, as well as the success of computational science across SC, depend on a portfolio of high-performance computing facilities and testbeds and on the high-performance networks that link these resources to scientists across the country. Since the early 1950s, DOE and the Office of Science have been leaders in testing and evaluating new high performance computers and networks and turning them into tools for scientific discovery. The Office of Science established the first national civilian supercomputer center, the Magnetic Fusion Energy Computer Center, in 1975. We have tested and evaluated early versions of computers ranging from the first Cray 1s to the parallel architectures of the 1990s, to the Cray X1 at ORNL. Our current facilities and testbeds include:

- The Center for Computational Sciences (CCS) at Oak Ridge National Laboratory, which has been testing and evaluating leading edge computer architectures as tools for science for over a decade. The latest evaluation, on a Cray X1, formed the basis for ORNL's successful proposal to begin developing a new supercomputer. In his remarks announcing the result of this competition, Secretary of Energy Spencer Abraham stated, "This new facility will enable the Office of Science to deliver world leadership-class computing for science," and "will serve to revitalize the U.S. effort in high-end computing." This supercomputer will be open to the scientific community for research.

- The National Energy Research Scientific Computing Center (NERSC) at Lawrence Berkeley National Laboratory, which provides leading edge high-performance computing services to over 2,000 scientists nationwide. NERSC has a 6,000 processor IBM SP3 computer with a peak speed of 10 Teraflops. We have initiated a new program at NERSC, Innovative and Novel Computational Impact on Theory and Experiment (INCITE), to allocate substantial computing resources to a few, competitively selected, research proposals from the national scientific community. Last year, the Office of Science selected three proposals were selected for INCITE. One of these has successfully simulated the explosion of a supernova in 3-D for the first time.

- The ESnet, which links DOE facilities and researchers to the worldwide research community. ESnet works closely with other Federal research networks and with university consortia such as Internet 2 to provide seamless connections from DOE to other research communities. This network must address facilities that produce millions of gigabytes of data each year and deliver these data to scientists across the world.

We have learned important lessons from these testbeds. By sharing our evaluations with vendors we have enabled them to produce better products to meet critical scientific and national security missions. Our spending complements commercial R&D in IT which is focused on product development and on the demands of commercial applications which generally place different requirements on the hardware and software than do leading edge scientific applications.

***

To accomplish its goals the Office of Science works closely with other agencies. In the areas where DOE –SC focuses its research, High-End Computing and Large-Scale Networking, DOE-SC cochairs the relevant coordinating group. In addition to this mechanism, DOE-SC has engaged in a number of other joint planning and coordination efforts.

- DOE-SC participated in the National Security community planning effort to develop an Integrated High-End Computing plan.
- DOE-SC and DOD cochaired the HECRTF.
- DOE-SC and NSF cochair the Federal teams that coordinate the engineering of Federal research networks and the emerging GRID Middleware.
- DOE-SC is a partner with DARPA in the High Productivity Computing Systems project, which will deliver the next generation of advanced computer architectures for critical science and national security missions through partnerships with U.S. industry.
- DOE-SC works closely with NNSA on critical software issues for high performance computing.
- DOE-SC, DOE-NNSA, DOD-ODDR&E, DOD-NSA, and DOD-DARPA have developed a Memorandum of Understanding to jointly plan our research in high performance computing. This MOU will enable us to better integrate our substantial ongoing collaborative projects.

***

Mr. Chairman, high-performance computing provides a new window for researchers to understand the natural world with a precision that could only be imagined a few years ago. Federal investments in advanced scientific computing equip researchers to advance knowledge and help solve the most challenging scientific problems facing the Nation. These national research investments might also provide current and prospective benefits to American industry, enabling it to use leading edge computational tools and simulation to develop new, more efficient, higher quality products for the U.S. consumer and greater competitiveness for the U.S. economy. Opportunities range from innovative design and engineering to materials development, all of which may serve to increase efficiency and safety while potentially reducing environmental effects.

Computing is an important tool in carrying out Federal agency missions in science and technology, but the government high-end computer market is simply not large enough to divert computer industry attention from the much larger and more lucrative business computing sector. The Federal Government must continue our research and prototype development on the next generation of computers, if we are to effectively carry out our scientific mission in the future.

With the continued support of this Committee, the Congress and the Administration, we in the Office of Science hope to continue to play an important role in the world of scientific supercomputing. Thank you very much.

Mr. PUTNAM. Thank you very much, Dr. Oliver. I want to thank all of you for your opening statements. Your full statement is to be included in the record, and we will begin with questioning.

Among these two dozen or so agencies that are coordinating or, excuse me, are engaged in Federal research, is there some collaboration across those agencies to pursue an overall strategic framework for research? Do they communicate with one another to avoid duplication or to buildupon the successes that are being found? Does the left hand know what the right hand is doing?

Dr. Freeman, you're nodding. We'll let you answer first.

Dr. FREEMAN. That's fine. Thank you sir, and I think that my cochair of the NITRD working group, David Nelson, will add to whatever I may have to say.

I think the answer to your question is a very definite yes in terms of coordination, in terms of knowing what each other is doing. In some cases that results in joint solicitations. For example, in the high performance computing area, we are currently coordinating, or I should say collaborating with DARPA for a jointly funded research program. We have several others in other areas already in place with DARPA. We are putting one in place with NIH, so there are a number of examples of that sort.

The Interagency Working Group as a whole meets every 3 months at which representatives from all 13 of those agencies are present to review budgets, to review strategic directions and, in general, to coordinate. There are then the program coordination areas that both Dr. Nelson and I mentioned. Those smaller, more narrowly defined groups; for example, in the area of human computer interface or in the area of high confidence or secure systems, those smaller groups of program directors and program managers typically meet on a monthly basis, in some cases even on a weekly basis, because many of the primary agencies are located physically adjacent to each other.

So there is a high degree of communication and collaboration there.

Mr. PUTNAM. Dr. Nelson.

Dr. NELSON. I agree with the comments of Dr. Freeman and would just add a couple of things. First, I refer to the Interagency Working Group, which Dr. Freeman and I cochair, as our board of directors. It sets the general directions and identifies special topics. About a year ago, Peter and I commissioned a study of whether the program components areas and the groups that implement them were properly constituted, and the answer that came back from them, and the Interagency Working Group has blessed it, is that in general they are, but in particular we need to focus more on security. And so we have started as a cross-cutting topic looking at how security aspects of all of our work need to be better done. It's, as you know, an extremely difficult topic.

The other thing that I would add is that there's always an open door to the involvement by additional agencies and additional programs in the work of the—and I will use the acronym here—the NITRD program. So for example, we have the Federal Aviation Administration, Food and Drug Administration as observers. They don't have much research, but they do want to use what the research program produces. And we also are discussing with the Department of Homeland Security its entry in the program. So the door is always open. Information Technology Research and Development has an awful lot of small pieces. And so as Peter has said, much of the detailed work is done putting those pieces together.

I mentioned before an example of research needs assessments. That's usually the first step. That's one. Another example of research needs assessment is the document that Peter just referred to, which is the Federal Plan for High-End Computing, which involved about 60 Federal managers from 12 agencies for about a year. After research needs assessments is research planning. Peter gave one example. There are many others.

The agencies share reviewers: They coordinate the solicitations; and then they jointly review progress and, where necessary, make changes and of course then go through another cycle of research needs, research planning, research implementation, research review.

Mr. PUTNAM. OK. Dr. Freeman, you said that they meet periodically to review strategic direction. Who sets the strategic objective, and could you summarize what the strategic objective is currently for Federal IT research and development.

Dr. FREEMAN. I don't think that I or anyone is really capable of saying what the objective is. As Dr. Nelson just indicated, there is a fairly elaborate process of trying to understand the needs for future research. He mentioned some of those activities. Let me share another one with you that perhaps will illustrate the process and thereby how the overall objectives are ultimately set.

Another activity that Dr. Nelson and I initiated, oh, probably a year and a half ago now, was an effort by the members of our working group to look at what are the major challenges, often called grand challenges, that would involve information technology, not on the research but at the usage end; for example, being able to seamlessly access the medical records of any citizen anywhere with appropriate privacy security, etc. It was put forth as a possible grand challenge, because we don't really know how to do that today. That working group, which worked for, oh, 6, 8 months, ultimately came back with a set of these grand challenges that, if achieved, would have great benefit for our society and for our economy. Taking those grand challenges, they then backed up and said, so what research should we be doing? So for example, security was something that was seen to be a critical component of essentially every one of those grand challenges.

So, through this process, our members, the various agencies, and through other processes that are not a part of the interagency activity, because each agency has its own internal processes to bubble up these research needs, prioritization then of those research objectives will depend upon the individual agencies, upon their missions, and upon their judgments as to which of, as Dr. Nelson has indicated, the many, many objectives that one could name.

So, in sum, what we wind up with is not a single strategic objective or even a coherent set of a small number. Obviously, we can boil those up to a high level and certainly security is a current high objective, I believe, of all of our members. High performance computing is another objective that is very important to many of the agencies. Ease of access to large data stores is a third objective.

But I would not characterize those as forming a strategic plan in the same way that an individual company or an individual agency might have.

Mr. PUTNAM. Dr. Oliver, a lot of attention has been paid to the fact that Japan now has the fastest supercomputer, the Earth simulator, which I believe has led the United States to reassess its high end computing R&D plans. Given where we now stand, are the existing Federal efforts appropriately targeted to deal with the challenge of positioning the United States as a leader in IT R&D, or are we losing our leadership position in this area?

Dr. OLIVER. I think that the formation of the High End Computing Revitalization Task Force last summer was the right step at the right time for us to articulate as a group of Federal agencies and departments how to address this problem. There were lots of meetings that were held and the report was written, and I think the implementation plan is pretty much in place or will be soon. So I think fully supporting that plan will lead us to a leadership position again. There is no doubt about it.

Mr. PUTNAM. Mr. Clay.

Mr. CLAY. Thank you, Mr. Chairman. Dr. Nelson, according to the recent report on Federal R&D released by RAND, total R&D funding for colleges and universities grew from approximately $70 billion in fiscal year 1996 to $96 billion in fiscal year 2004. Yet only $2.2 billion is dedicated specifically to IT research and development through the NITRD program.

Can you tell us why it is such a small percentage of the total allocation, and have no concerns with cyber security and national defense caused your office to reevaluate its support for IT R&D funding?

Dr. NELSON. Yes, Congressman Clay, the priorities for research, as for any other Federal program, go through many steps and have many masters. And so addressing a question like why IT R&D is only $2 billion is almost impossible. One could equally ask why is it as big as it is. And I think, as you pointed out, it has grown substantially in recognition of its importance.

I would suggest though, and I think Dr. Freeman has also mentioned this, that much of other research has information technology components. The term that's used often is it's embedded in that research, and it is almost impossible to tease out how much of that other research is information technology. But we know there is a lot there. In other words, the amount of information technology research is higher than the numbers might suggest.

The second thing that I would say is I believe the RAND study pointed out that much of that increase went to medical schools and was a direct result of the doubling of the National Institutes of Health budgets, and of course that has been a national and bipartisan priority. It is good to note that much of the improvement in health care research has come about from better usage of information technology, and bioinformatics is now a thriving field.

So again it's hard to tease out, and the bottom line I can give you is that there probably isn't a direct answer. We can all hope that those good research ideas are funded and that they appropriately impact our economy and way of life.

But the process for arriving at it is probably beyond that of any one person to comprehend.

Mr. CLAY. Then another question, Doctor. Tell me about, compare the 2004 budget for Federal IT R&D to 2005. It's been reduced by about $200 million, from $2.2 billion to $2.0. Can you tell us why the amount requested was reduced?

Dr. NELSON. Yes. I would like, if I could, to answer that for the record. And I will tell you why. We have a total for 2005, but because the—and I will use the term NITR&D, that's Networking and Information Technology R&D—program is what we call a crosscut, you can't get there by aggregating line items. And, therefore, it takes judgment and allocation to come up with either the total or with the subcomponents. We do not yet have the 2005 numbers for those subcomponents.

And before I could address why that $200 million is approximately about 10 percent down, I would have to have a better idea of how it matches up with the program component areas that Dr. Freeman referred to, and therefore what the change is. I would be happy to respond for the record, but it may take a few weeks before we get back to you.

Mr. CLAY. That's fine. Thank you for that response.

And Dr. Freeman, I am concerned that a large proportion of Federal R&D funds are being limited to the life sciences. Can you tell us if the IT needs of the medical and biological research communities are being met through the current formula for Federal R&D funding?

Dr. FREEMAN. Congressman Clay, I'm afraid in the specifics, I am not competent to answer that question. Obviously, someone from NIH or the medical community should address it. I would note that through the interagency working group and our budget reviews, we are aware that NIH is spending large sums on information technology usage, more on the development and usage side of the ledger than on the underlying research. But I will have to defer to their judgment as to whether there is sufficient IT research being done in the country to support those medical efforts.

Mr. CLAY. OK. Then I guess asked another way. Can you cite for us what other Federal R&D needs would rival the need for life science research?

Dr. FREEMAN. Well, certainly based on the demand through the proposal submission process at NSF, there is a very large unmet need for additional research. Let's take the cyber security area. My program director in this area is just in the process this week and next of making final decisions on something like 150 proposals that were submitted by a deadline a few weeks ago for funding specifically in the cyber security area. I have not seen the final results, but based on previous competitions, probably at least 30 to 35 percent, about a third of those proposals would be ranked by their scientific peers as worthy of funding, that is, scientifically valid. We will be lucky if we can fund 10 percent of those submitted proposals. So there is an overhang there of good ideas in the cyber security area that we are simply not going to be able to fund. I suspect that my colleague from NIST has a similar experience in that area.

Mr. CLAY. I will get to him. Thank you for your response. You know, you guys have long responses and long opening statements, and they give us a limited amount of time. But I appreciate your effort.

Dr. Oliver, in what ways can the Office of Science collaborate with the private sector on R&D initiatives in order to find solutions to problems facing our Nation and the international community, such as environment and educational issues?

Dr. OLIVER. Well, we have had a long history of collaborating with the computing vendor industry in high-end computing and network and so forth. And, you know, we have cooperative research and development agreements with many of the individuals who have funding from us, especially in the DOE laboratories. And so that has tremendous benefit in many ways with the computing industry. And the wave goes out from there. We get in machines. We have often bought serial one of every high-end machine in the Department of Energy from the beginning of time. There are a few exceptions.

So we get them when they are raw. They don't necessarily work. We invest in operating systems to help make this work. We do this in cooperation with other agencies, DARPA and 1–Ks or NSF in another. And so we help make a machine viable. We then put on applications software like a structural analysis code and make it work on the machine. That makes it attractive to the aerospace companies and so forth.

So there is a dramatic effect like that where we work with industry, you know, to help in the economic sense. And, but we do it to serve our own needs. I mean, we have to make these machines work in order to meet the missions of the Office of Science to do science.

Mr. CLAY. Thank you. And, finally, Dr. Semerjian. Are there specific areas of IT R&D that the government is currently not pursuing but merit consideration in future strategic plans?

Dr. SEMERJIAN. Well, that is a very broad question. Probably some of my colleagues are better prepared to answer that. But just from our own point of view, the kind of things that we do at NIST, I think I agree with Dr. Freeman that cyber security issues I think really need to be addressed. Because in every application area that we look at, whether it's the medical records or whether it's communication issues and national security issues, cyber security continues to be at the top of the list of issues, which is clearly underfunded.

And I think we are very pleased that the President's budget proposes to increase the NIST part of that. But that is only a drop in the bucket. I am sure there are many other security-related issues in other agencies which need to be addressed.

Mr. CLAY. Thank you for your response. I thank the panel for their indulgence. Thank you, Mr. Chairman.

Mr. PUTNAM. Thank you, Mr. Clay. I just want to followup a bit on the coordination line of questioning. To what degree are the classified and unclassified research initiatives coordinated? If you take cyber security, for example, it's certainly broader than NIST and NSF. You have an alphabet soup of agencies within the intelligence community who are also doing work. Do they share some of their direction on research as well, or is that a world unto itself?

Dr. Nelson.

Dr. NELSON. I can speak to the relationship between the classified world and the unclassified. I personally have high security clearances, but the NITRD program is totally unclassified. Now, I believe there is reasonably good coordination between the classified side and the unclassified. And I will say how that occurs. Several of the agencies that participate in the NITRD program, in particular the National Security Agency, the National Nuclear Security Agency, and the Defense Advanced Research Projects Agency, bring their unclassified research to the table and work closely with agencies like NSF, NIST, DOE science, and so on to get the best bang for the buck out of that. Now, clearly, they take those results back into the classified side, and the NITRD program does not see those.

I am aware that there are coordinating groups that deal with classified research, in particular, the Infosec Research Council. But I do not know whether that is broadly the case. I could mention another agency or two that interacts with us on an informal basis, the Central Intelligence Agency, and as I said earlier, we are talking seriously with the Department of Homeland Security about their joining the program. So, indeed, there is coordination. As it comes through the boundary between classified and unclassified, I'm less knowledgeable about what goes on behind the classification screen.

Mr. PUTNAM. So Homeland Security is not currently a part of this NITRD program?

Dr. NELSON. That's correct.

Mr. PUTNAM. And what is it that needs to be decided to allow them to participate?

Dr. NELSON. As you know, they have been forming up. And bringing all those subagencies together has been a monumental task. So the short answer is they are still working on their research agenda. They are still getting staffed up to carry out that research agenda. And I fully expect that as soon as they have people who are able to work—coordination takes time, it takes people—that they will join.

Mr. PUTNAM. Well, I certainly expect them to get ramped up and be a part of it as soon as possible. They are an important piece, and they are a relatively new agency, but they are no longer a new agency and that excuse only carries you so long.

Dr. NELSON. Yes, sir.

Dr. SEMERJIAN. If I could add on the classified versus unclassified issue. We do have a close working relationship with NSA. It is formally recognized that NIST provides the standards for the unclassified world, so to speak, and NSA for the classified. And we do work closely with them, since some of the technologies are utilized on both sides of the fence. So at least in terms of standard issues, cyber security-related standards, we have a very good working relationship with NSA.

Mr. PUTNAM. Good. I want to give all of you the opportunity, because we were cut short on the opening statements, but we have another panel that we need to move to. I want to give any or all of you, if you have something that you wish to add to this conversation, something you wish you had been asked, now is the time. So we will begin with Dr. Oliver, work backward, and then we will seat the second panel. Dr. Oliver, anything to add?

Dr. OLIVER. Nothing to add.

Dr. SEMERJIAN. (Shaking head.)

Mr. PUTNAM. Dr. Freeman.

Dr. FREEMAN. A former professor always has another word. One topic we have not discussed today is the issue of education. That is one that, of course, NSF has a key responsibility in. And I would note that it is also a key element in both the research and certainly the development aspects of information technology, to say nothing of the utilization of it. I think that your opening statement, Congressman Clay's opening statement very aptly recognize the importance of information technology in essentially every element of our life today. And I would only add that we must keep in mind that educating all of our citizens at all levels of the work force, all the way down to kindergartners, in the usage of that technology is a key challenge that we need to keep in sight.

Mr. PUTNAM. Let me followup on that and ask you, as someone who has come out of the academic world. Many of us are familiar with and very concerned about the decline in math and science skills among America's young people, the number of degrees being awarded to Americans in a number of these sensitive fields. I am not asking you for a silver bullet, but what are the steps that we can begin to take to turn that around and produce more math and science graduates?

Dr. FREEMAN. I'm glad you didn't ask for the silver bullet, because I certainly don't have it and I'm not sure that I have all of the steps. But it is something, and the reason I bring it up here is it is a topic that I believe we must first and foremost always keep in mind. So it is important, of course, to look at funding levels at the substance of the research, but we must be mindful that we have to have the educated people to carry out that research, for example. So I think the attention of committees such as yours to the educational issues, the attention of all of us as citizens is certainly a first and a very necessary step to take.

Mr. PUTNAM. Dr. Oliver, I believe in some of your responsibilities at the Department of Energy, do you have a hard time filling slots in the Office of Science? Do you have a hard time recruiting good people who want to work for the government doing this type of research?

Dr. OLIVER. You have done your homework. Yes, it is, in many areas, very difficult to get program managers to come and work in D.C., though I tout the city as the greatest place to live in the country in opportunities and everything. I mean, I think we have a terrific, you know, organization. And the jobs are truly exciting. And I find that it's just getting more and more difficult in our area and I don't know why.

Maybe industry salaries are high, academic salaries are very high for people in computer science, applied math, that know about high-end computing, in tremendous demand, and I think maybe the pool is a little small. I mean, it's the supply and-demand situation. Anyway, it's very difficult for us to get people in the Office of Science. And we have a very important challenge facing us because I think we are an aging group, not just in information technology, but throughout the program management staff. And it's something we are aware of and that we are trying to address, and we are looking at all of the things that you can do, knobs you can turn. But it is indeed a challenge. So we have a lot of people with a lot of dual jobs, dual-hatted, but they rise to the occasion.

Mr. PUTNAM. Thank you.

Dr. Nelson, final comment?

Dr. NELSON. Yes. Just one footnote in the planning and management area. We can always do a better job of strategic planning, no question of that. But we have to remember that in research, it's often the least planned and the least unexpected that yields the biggest dividends. Who would have thought that the high performance computing program would produce the Mosaic browser, and yet it was the NSF program at the University of Illinois that did just that. Who would have thought that an early program to link academic computers would have produced the Internet? But it did just that. And so in research we always look for the revolutionary change, the things that really improve the economy in the country. It's hard to plan those.

And, as I mentioned in my testimony, management of those activities has to be very deft and sensitive. It's very easy to stamp out the revolutionary and it's very hard to encourage it.

Mr. PUTNAM. Thank you very much. And I want to thank the entire panel. And, with that, the subcommittee will stand in recess while we arrange for panel two. And if you would be seated as soon as possible. Thank you, gentlemen, very much for your contributions to this hearing.

If the second panel could please take their seats, we will begin. The subcommittee will reconvene. And if you would please rise, and anyone accompanying you who will assist you in answering the questions please rise for the administration of the oath.

[Witnesses sworn.]

Mr. PUTNAM. Note for the record that all of our witnesses responded in the affirmative. And we will move to the testimony. You will note the lights on your table. Green light means talk away. Yellow light means bring it in for a landing. Red light means bring it to a close.

Our first witness is Dr. Donna Fossum. Dr. Fossum is a senior scientist and legal policy analyst in the RAND Resource Management Department, and is program manager of the RaDiUS Project. Prior to joining RAND, Dr. Fossum served as the legal counsel and technology specialist of the Committee of Government Operations here in the House of Representatives. Dr. Fossum has also served as the deputy associate administrator of the Office of Federal Procurement Policy in OMB, where she devoted much of her time to advising the administrator for Federal procurement policy on matters involving the defense industrial base. Most recently, she served as the senior adviser for science resources development at NSF.

Dr. Fossum's work for the institute has centered on developing a comprehensive data base of the R&D activities sponsored by the Federal Government known as RaDiUS, to facilitate the management and content assessment of the Federal R&D portfolio. Much of her time is also devoted to working with OSTP and other Federal agencies as well as numerous nonFederal entities to identify and evaluate Federal activities in every conceivable field of R&D. Welcome to the subcommittee. You are recognized for 5 minutes.

STATEMENTS OF DONNA FOSSUM, MANAGER, RADIUS PROJECT, RAND CORP.; EDWARD LAZOWSKA, CO-CHAIR, PRESIDENT'S INFORMATION TECHNOLOGY ADVISORY COMMITTEE AND CHAIR, DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING, UNIVERSITY OF WASHINGTON; WILLIAM SCHERLIS, PROFESSOR, SCHOOL OF COMPUTER SCIENCE AT CARNEGIE MELLON; AND STEPHEN SQUIRES, CHIEF SCIENCE OFFICER, VICE PRESIDENT, HEWLETT-PACKARD

Dr. FOSSUM. Thank you. Thank you very much. I have submitted a long statement for the record, so I will make it very short and summarize it. First I want to express my sincere appreciation for the hearing today, because this is a topic that often gets overlooked and, yet it is at the heart of everybody's life and becoming more so.

Let me explain a little bit about the RaDiUS program and why it even came to be. In 1992, we were supporting the work of the White House in science and technology, and discovered that the data that everybody wanted or needed to find out what was going on in the world of Federal R&D and on various topics, we didn't have at the right level of granularity. It was at the program level, which wasn't adequate to answer their questions. For instance, they wanted to know what was going on in electronics, preventing violence in youth, automotive-related technologies, global positioning, aviation safety, etc.

And this is where RaDiUS was born. RaDiUS systemically tracks all the R&D dollars that are identified by Federal agencies as being R&D and tracks them through the layers of the bureaucracy down to where they are actually spent—where I say "the rubber hits the road." And this is where the R&D is actually conducted. Courtesy of the RaDiUS data system, we now have a capability that is used extensively by many of the agencies in the Federal Government many Federal contractors, universities, and others all over the world to learn what R&D is being supported by the USG. Actually we have discovered there is very little duplication of R&D in the Federal Government, but there are many, many opportunities where leveraging of Federal R&D dollars is not happening.

Agencies in the same red area don't even know it, but through RaDiUS, they can find out they are working in the same field and can leverage their dollars more effectively.

RaDiUS, in 1998, was declared a "best practice" of the U.S. Government by the General Accounting Office. Courtesy of RaDiUS, RAND has been able to produce two reports. "Discovery & Innovation" has been called a chest crusher by one of our colleagues. What it provides is the first compendium ever of all the Federal R&D activities by State and city in the country. Where is it happening and what are they doing? This was done in 2000. It's time to be updated but a whole lot of it has not changed all that much. Where it's happening has not changed.

I will leave a copy of it with you. And already today this report that came out a couple of months ago has been cited, "Vital Assets." It contains the first really accurate assessment of where all the Federal dollars are going to universities around the country. This kind of capability has been developed, courtesy of RaDiUS.

But that's not what the topic of today's hearing is. You have gone through a wonderful list of questions to which we would all like the answers, but the one question that has been hinted at briefly by some of the people here that I want to focus on, which is a pivotal question in this area, is "What is IT R&D?"—because IT itself has evolved so tremendously in the last 30 to 40 years, and the R&D associated with it has evolved right with it. For instance, initially IT was just physical components. We were building hardware. We were looking at the mathematical equations that could be used for pulling data together and manipulating it. At the beginning, that was IT R&D—physical components. And there's still a lot of that R&D work going on. As it evolved over time, IT R&D got into new applications and the new infrastructures. This is where you started spawning software and other applications like data bases. Once you put it together with infrastructure, applications, design, and development, what you have are all kinds of ramifications and potentials that had never been thought of in the very early days.

So what I've provided in my written testimony is a template of essentially four definitions of IT R&D. One is very narrow, which is physical components. And another is quite broad, as it includes information technology functionalities, information technology applications and infrastructure, and the capabilities enabled by information technology. And since we are the data people, we wanted to give you some hard numbers to grab on to. So what is the Federal Government spending in IT R&D?

If you take a narrow definition of IT R&D as physical components, and run it through the RaDiUS data system, we come up with the fact that there was about $1.5 billion of IT R&D. And this is a very conservative estimate. This is for just the physical components. If you broaden the definition to include everything, all four aspects, again, very conservatively, it's over $11 billion. That's about 12 percent of the Federal R&D budget. By the way, we are only talking about the "Conduct of R&D" when we talk about this information. Keep in mind that one of the biggest sources of confusion when we talk about R&D numbers in the Federal Government is often they include "R&D facilities" as well as "R&D equipment." That doesn't get you the "conduct of R&D." So in RaDiUS we only focus on the actual conduct of R&D work. That's what these numbers are.

So you have a narrow definition and a broad one.

What we cannot tell you is whether this is valuable research. We can tell you what it is and if it is meeting objectives of the Federal agencies. We can give you information on it. We can tell you what's going on. Let me give you a hint about some of this. Keep in mind, the major agency doing R&D in IT is DOD by far. In the narrow definition, the No. 2 agency is DOE. In the broad definition, it's HHS. You have all kinds of players here. NASA is a major player. You have NSF, and the Department of Agriculture. Every part of the Federal R&D community is working somehow in IT-related activities.

Let me give you a little idea of who is doing what.

Mr. PUTNAM. If you would, if you could summarize it. We have a vote at 3:15, and I want to get through testimony before they ring the bells.

Dr. FOSSUM. OK. You've got it. I will just submit this to the record. But let's suffice it to say that people are working at DOD on everything from dealing with strike aircraft to virtual battlefields. At HHS, they are doing R&D on wireless EKG chips. They are doing all kinds of R&D all over the government dealing with IT. And we are here as the tool that can tell you what's going on where and help to better coordinate it. Thank you so much.

[The prepared statement of Dr. Fossum follows:]

TESTIMONY

Identifying Federally Funded Research and Development on Information Technology

DONNA FOSSUM

CT-229

July 2004

Testimony presented to the House Committee on Government Reform July 7, 2004.

Statement of Donna Fossum, JD, PhD[1]
Manager of the RaDiUS Program at RAND

Before the Committee on Government Reform
United State House of Representatives

IDENTIFYING FEDERALLY FUNDED RESEARCH AND DEVELOPMENT ON INFORMATION TECHNOLOGY

July 7, 2004

Mr. Chairman and Members of the Subcommittee, I appreciate the opportunity to testify here today on this most important topic. To support the work of the White House Office of Science and Technology Policy, the RAND Corporation began in 1992 to systematically gather information on all of the research and development (R&D) activities that are funded each year by the United States federal government. While this effort initially gathered information only on the R&D programs of federal agencies, it quickly became clear that the most readily available information on federal R&D activities was too aggregate to be of use in answering the many questions that were of greatest concern to the federal government.

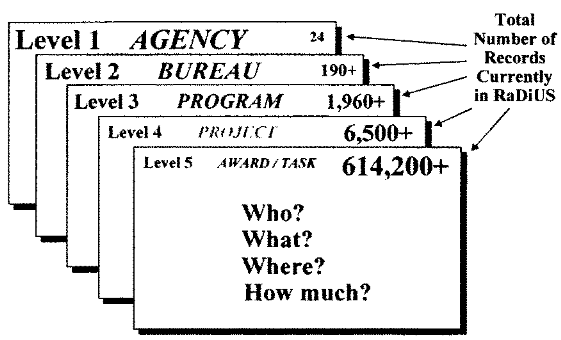
Specifically, various agencies and offices of the executive and legislative branches of the federal government wanted to know how many federal R&D dollars were being spent on electronics, global positioning technology, preventing violence among at-risk youth, automotive-related technology, aviation safety, education technology, environmental

[1] The opinions and conclusions expressed in this testimony are the author's alone and should not be interpreted as representing those of RAND or any of the sponsors of its research. This product is part of the RAND Corporation testimony series. RAND testimonies record testimony presented by RAND associates to federal, state, or local legislative committees; government-appointed commissions and panels, and private review and oversight bodies. The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

change, and a host of other topics. To answer such focused questions, the RAND Corporation created the RaDiUS Database, which is the most comprehensive and detailed collection of information assembled on the R&D activities funded by the federal government.

The RaDiUS Database uses OMB's definition of R&D to systematically track the funds that federal agencies devote each year to R&D through the various bureaucratic levels of each agency to the point where they are actually spent to conduct R&D. As noted in the chart below, each increasingly detailed level of the RaDiUS Database provides users with information on who, what, where, and how much regarding federally funded R&D.

The Structure and Contents of the RaDiUS Database



Users of RaDiUS can search the database with any descriptive term(s) of their choosing to identify federally funded R&D activities in every field of science and engineering. In 1998, the General Accounting Office declared the RaDiUS Database to be a "Best Practice" of the federal government (GAO/NSIAD/RCED-98-23).

I have been the project manager of RaDiUS since its inception at RAND, and in that capacity oversaw the design and development of the RaDiUS Database a decade ago. I continue to make sure that the information in the RaDiUS Database is regularly updated and available for use. I am also the lead author of two reports that were made possible because of the existence of the RaDiUS Database. The first is "Discovery and Innovation," which was released in 2000 and which for the first time detailed all federally funded R&D activities by the state and city in which they actually occurred. In 2001, the Public Libraries Association and the American Association of School Libraries recommended that copies of "Discovery and Innovation" be included in all public and high school libraries in the nation. The second report is "Vital Assets," which was released just three months ago (in April). It details the federal R&D funds that went to every university and college in the nation in FY 2002. Among the notable findings presented in "Vital Assets" is the fact that only 80 of the more than 1,825 four-year accredited and professional degree-granting universities and colleges in the nation received 71 percent of all the federal R&D funds provided to such institutions in FY 2002. It also found that the nation's126 medical schools received 45 percent of all federal R&D funds provided to universities and colleges in FY 2002.

Today, the focus of this hearing is on information technology (IT) R&D. Specifically, the Subcommittee has asked the following questions:

- Which federal agencies fund IT R&D?
- How many federal dollars are spent on IT R&D?

- In what areas of IT are federal R&D investments being made?
- Who receives federal IT R&D funds and how much do they get?
- What is the federal government gaining from its investment in IT R&D?
- Why should the federal government continue to make these investments?

While I will draw upon the RaDiUS Database to provide answers to many of these questions, before I do so, I would first like to address an additional question – namely, to what are we referring when we use the term "IT R&D"?

What is IT R&D?

From the development of the transistor in the 1940's until today, the meaning of the term IT has changed dramatically, most especially in the past decade. And as the capabilities and pervasiveness of IT have expanded throughout society, the range and scope of IT R&D have also grown.

Initially, IT R&D focused on the physical components of IT, encompassing both the physical sciences, where research on hardware components was being conducted, as well as mathematics, where the foundation of rudimentary machine instructions or encoding was being laid. As research advanced our knowledge of specific physical components, new IT functionalities emerged, such as data storage, data processing, and data transfer, all of which became integral parts of computers and electronic devices. Consequently, over time, IT R&D expanded to encompass research on physical IT components, as well as research on the higher-level functionalities that were enabled by the design and engineering of the underlying physical IT components. As a result, the focus of IT R&D expanded to include the fields of engineering and computer architecture design, as well as other disciplines that sought to explore and exploit the new higher-level functionalities.

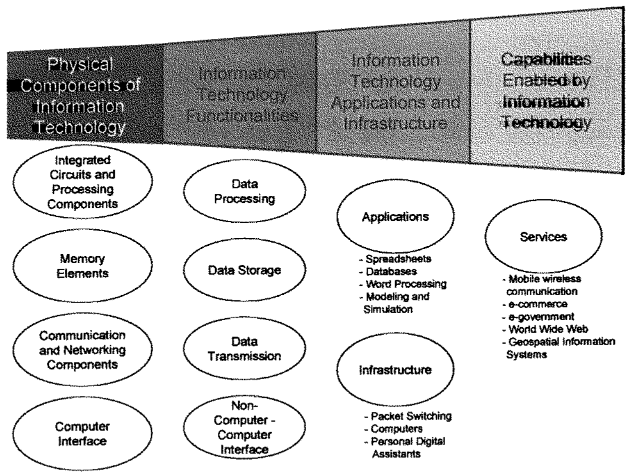
Very quickly, it was discovered that these higher-level functionalities could be combined to create new applications and new infrastructures, spawning the field of software engineering as well as the development of new tools that allowed people to handle and manipulate both data and information. This era of IT R&D produced software for word processing, spreadsheets, databases, meteorological modeling, etc. IT R&D also produced a host of infrastructures, including packet switching networks, as well as wireless base stations, cellular communication, and other similar innovations. Again, the scope of IT R&D expanded to include application and infrastructure design and development. These new IT applications and infrastructures allowed for the creation of new services, such as e-commerce, distributed computing, and the World-Wide-Web, all of which are new IT services enabled by combining IT applications and infrastructures. So the world of IT R&D expanded yet again.

In short, what began as R&D on the physical components of IT has grown to include higher-level IT functionalities enabled by combinations of physical components, IT applications and infrastructures, and IT capabilities that are built on combinations of IT applications and infrastructures. As a consequence, the challenge today of identifying what is IT R&D is not the equivalent of looking for a needle in a haystack as it was only a few decades ago. Rather it is the much harder task of identifying what is NOT encompassed by the term IT R&D, since virtually every field of science and engineering is now affected or has in some way become associated with IT. This challenge becomes even more difficult when one realizes that such seemingly non-IT fields as biology, chemistry, and optics are now viewed as having the potential for revolutionizing how basic IT systems operate.

Further complicating this challenge is the fact that, as the focus of IT R&D moved from physical components to developing new applications and services, the types of problems solved by IT also changed. That is, early on, IT R&D focused on the emerging field of electronics and electronic devices and began by replacing mechanical devices with electronic ones that merely provided an alternative method of solving simple problems. As IT R&D created new electronic devices, new combinations of IT were being discovered that allowed for new functionalities. Problems that once had to be solved by hand or mechanical devices could suddenly be solved faster and much more efficiently with the application of new IT devices. Eventually, by building on the new functionalities resulting from IT R&D, scientists and engineers began to create entirely new IT applications and infrastructures. The use of these new IT applications and infrastructures, in turn, allowed people to solve a whole new class of problems – complex problems encountered in the real world. However, to solve these real world problems using IT, it was still necessary to simplify the models of them in order for the IT to address them. Today, IT is able not only to solve the complex problems encountered in the real world with little or no simplification, but also to interact directly with the world in such a way as to influence the very problems it is addressing. Consequently, as IT R&D has evolved over the decades, it has become increasingly difficult to separate IT from the environment in which it operates.

Four Definitions of IT R&D

Based on the evolution of IT, the R&D related to IT can be defined in at least four different ways, all of which are illustrated in the chart below.



Depending on whether IT R&D is defined in terms of the physical components of IT, IT functionalities, IT applications and infrastructure, capabilities enabled by IT, or some combination thereof, one will get a different answer regarding how much the federal government is spending on IT R&D and which federal agencies are funding it.

Clearly, much of the confusion that currently exists regarding how many federal dollars are being spent on IT R&D is a direct result of the fact that there is not a standard definition of what constitutes IT R&D. While the Interagency Working Group on Information

Technology Research and Development of the National Science and Technology Council's Committee on Technology attempted to do this in its report, "Advanced Foundations for American Innovation," it does not appear to have succeeded for two reasons. First, the substantive definition of IT R&D used by the Interagency Working Group was so expansive that it encompassed virtually every field of science and engineering. Second, the inclusion of the term "fundamental" in the discussions of the Interagency Working Group appears to have been taken as a signal by at least one major federal R&D agency that only "Basic Research" was of interest to the group. This meant that the vast majority of this federal agency's IT R&D, which is "Applied Research" and "Development," was not included in this report.

Federal Funding for IT R&D

While the RaDiUS Database can answer a host of questions about IT R&D, the RaDiUS Database cannot define what IT R&D is – only people can do that. To ensure that this Subcommittee has some "hard" numbers on IT R&D, however, the RaDiUS Database was searched to identify all federally funded IT R&D using both a "narrow" and a "broad" definition of IT R&D. Specifically, searches of the RaDiUS Database were conducted when IT R&D was defined narrowly as the "Physical Components of IT" ***only***.[2] Searches of the RaDiUS Database were also conducted when IT R&D was broadly defined as the

[2] The specific terms searched were "(information technology) OR (integrated circuit%) OR (computer interface) OR (computer memory) OR (network component%) OR (processing component%)." Note that "%" is a "wildcard" that will retrieve any variation of the word specified.

"Physical Components of IT," *and* "IT Functionalities" *and* "IT Applications and Infrastructure" *and* "Capabilities Enabled by IT."[3]

Federal Agency	Narrow Definition (Estimated FY 2002 Budget Authority in thousands)	Broad Definition (Estimated FY 2002 Budget Authority in thousands)
DOD	$1,137,154	$6,869,031
HHS	$47,518	$2,181,844
NASA	$21,756	$73,702
DOE	$148,370	$1,080,827
NSF	$65,129	$628,889
USDA	$1,880	$112,155
DOC	$94,921	$227,734
Other[4]	$351	$63,225
TOTAL	$1,517,080	$11,177,408

As the table above shows, using the "Narrow" definition of IT R&D, it was found that just over $1.5 billion, or about 2%, of all federal funds devoted to the conduct of R&D in FY 2002 involved IT. Using the "Broad " definition of IT R&D, it was found that just over $11 billion, or about 12%, of all of federal funds devoted to the conduct of R&D in FY 2002 involved IT. With both definitions, the federal agency providing the most funds for IT R&D was the DOD, while the second ranked agency was DOE for the "Narrow" definition and HHS for the "Broad" definition. Under both the "Narrow" and the "Broad"

[3] The specific terms searched were "(information technology) OR (integrated circuit%) OR (computer interface) OR (computer memory) OR (network component%) OR (processing component%) OR (data processing) OR (data storage) OR (data transmi%) OR (computer modeling) OR (computer simulation) OR (word processing) OR (database%) OR (spreadsheet%) OR (packet switching) OR (computer%) OR (personal digital assistant%) OR (mobile wireless communicat%) OR (e_commerce) OR (world wide web) OR (internet) OR (gis) OR (geospatial information system) OR (e_gov%)." Note that "%" is a "wildcard" that will retrieve any variation of the word specified.
[4] DOT and DVA for both definitions, as well as DOI for the "Broad" definition only.

definitions, it was found that the vast majority of the IT R&D funds went to non-federal parties, most notably higher education institutions and private companies, where the federally funded IT R&D was actually conducted.

While there was not time before this hearing to systematically determine how many federal R&D funds were being spent on each specific IT area such as integrated circuits, processing components, packet switching, etc., the records in the RaDiUS Database revealed that a wide range of IT challenges are being addressed with the help of federal R&D funds. For example, DOD's IT R&D awards/tasks included ones focusing on reconfigurable computers to reduce the size of strike aircraft and networked virtual environments to aid battlefield awareness and management. HHS's IT R&D awards/tasks included ones focusing on informatics-based data tools to link parent-derived information directly to the care process and the development of a wireless electrocardiogram chip. NSF's IT R&D awards/tasks included ones focusing on harnessing the power of IT to manage infrastructure systems and the use of computational intelligence to solve problems that defy solutions using traditional techniques. And DOC's IT R&D awards/tasks included one focusing on exploring the use of digital signal processing techniques, such as compression and error control encoding, to improve the performance of IT applications that are carried over wireless communication systems.

Conclusion

As demonstrated above, the RaDiUS Database can tell us which federal agencies fund IT R&D, how many federal dollars are spent on IT R&D, and the areas in which federal IT

R&D investments are being made. It can also tell us who receives federal IT R&D funds and how much they get. The RaDiUS Database cannot tell us what the federal government gains from its investment in IT R&D or why the federal government should continue to make these investments, but it can provide the factual foundation on which to base an analysis of these types of questions.

Mr. PUTNAM. Thank you very much.

Our next witness is Dr. Edward Lazowska. Dr. Lazowska is professor and Chair of the Department of Computer Science and engineering at the University of Washington. He received his Ph.D. from the University of Toronto in 1977. He has been at the University of Washington since that time. His research concerns the design and analysis of distributed and parallel computer systems. He is a member of the NSF, CISE advisory committee, Chair of the Computing Research Association, and member of DARPA ISAT, and a member of the technical advisory board for Microsoft research.

He is a member of the NRC's computer, science, and telecom board, and served on the CSTB committee that produced evolving the high performance computing and communications initiative to support the Nation's information infrastructure. He is a member of the National Academy of Engineering and a fellow of the ACM and of the high Triple E. He is a leader in the Learning Federation, a group that is concerned with using information technology to improve learning at the college level. Welcome to the subcommittee. You are recognized for 5 minutes. I would ask all of you to please hold tight on the 5, because there will be a vote at 3:15. Thank you.

Dr. LAZOWSKA. Thank you very much, Mr. Putnam, and the other members of your subcommittee. It is a pleasure to be here to testify today.

As you said in your introductory remarks, much of the gains in productivity in the U.S. economy over the past decade, the really unprecedented gains throughout the 1990's, have been shown to be due to efficiencies produced through information technology. And IT and its advances are driving advances in all fields of science and engineering. So what your subcommittee is asking is, how does that happen? And the abstract answer is it's a complex ecosystem that involves companies and universities and the Federal Government. It's been working for 50 years. The United States is the world leader in innovation in information technology today because of some formula that none of us can quite get our hands around but that fundamentally seems to work. So it has been a 50-year story of success.

Every aspect of IT that we rely on today, every billion dollar subindustry, traces part of its origins to the federally funded university-based research program. You have a two-page handout of my remarks today. And on the second page is a little eye testing graph, which I won't try to describe to you now, but this is from a National Academy study that Dr. Nelson referred to. And what it shows is two dozen different billion dollar subcategories of the IT industry. And for each one, it shows the complimentary roles of university research funded by the Federal Government, industrial R&D, and product development, becoming a billion dollar industry.

So the interplays are very complex, and there have been authoritative studies of this. But the key thing for you to understand is the role that the Federal research program has played in all of these technologies.

I am fond of saying if you want to do E-commerce, you have to have a Internet, you've got to have Web browsers, you've got to have high performance data base systems, graphical user interfaces, public key cryptography for secure credit card transactions. All of those are results of the federally sponsored research program.

In planning policy—and a point that Dr. Freeman made very clearly—it is important not to confuse industry R&D with research that's looking 5 or 10 or 15 years out. And here is just a concrete example. I'm on the technical advisory board for Microsoft Research. Microsoft advertises that it will spend $6.8 billion on R&D this year. OK. Of that $6.8 billion, only a couple hundred million is Microsoft Research, the organization that I advise.

$6.6 billion is engineering the next release of Word and Excel and Power Point and Windows. This is really important. But that's done by taking ideas out of the R&D larder and putting them into products. It's engineering the next generation of the product.

Now, it sounds like I'm castigating Microsoft, but I'm not. In fact, on the contrary, Microsoft invests about 5 percent of its R&D budget in activities looking out five or 10 or 15 years. Dell, Oracle, Cisco invest essentially nothing looking more than one product cycle out. HP has a representative on this panel and HP does look more than one product cycle out in a style not unlike Microsoft. So does Intel. But many of the major IT companies don't look more than one product cycle out at all. And that's what defines our future, what makes sure that we are going to be a leader 5 and 10 and 15 years out.

You heard from Dr. Freeman that another important characteristic of the Federal research program is that it produces people. A second graph on my handout is the Department of Commerce work force projections for the next 10 years for various fields of science and engineering. And what it shows is a huge work force gap in information technology compared to any other field of science and engineering.

The Department of Commerce projects that more than three quarters of all the jobs that will have to be filled in all of science and engineering in the next 10 years are IT jobs.

Recent increases in support for IT research have been important but have fallen far short of the levels recommended by the President's Information Technology Advisory Committee. Mr. Clay observed a disconnect in funding choices made by agencies. The third graph in my materials shows the increase in the government supported R&D budget over the past 30 years. And you see that the vast majority of that is increases in the National Institutes of Health. Every other field is essentially flatlined, although IT R&D has doubled over that period, you can't see the increase on a scale that includes health and human services.

My response to your question asked of another witness about HHS IT R&D is that largely what they do is take innovations that DARPA and the National Science Foundation have funded and apply them to biomedical problems, as opposed to investing in fundamental IT research. There are exceptions, you will hear about the NIH bioinformatics program, but that's a few tens of millions of dollars new this year out of a $30-plus billion budget.

So one other point that I would make is there are, as you heard, 13 or more Federal agencies investing in IT R&D. I think if you look at the history of innovation, it is NSF and DARPA, with work from Energy in high performance computing, that have driven the lion's share of the innovations.

A couple more points and then I will conclude. The research community has concerns with the low level of funding for the NSF Computer and Information Science and Engineering directorate. That budget has gone up in recent years, but the research budget there is still only a bit more than $400 million. We have concerns about——

Mr. PUTNAM. If you could bring it in for a landing, please, sir.

Dr. LAZOWSKA. Sure. We have concerns about DHS's failure to invest in cyber security R&D. DHS began a year ago with a new $800 million research budget and proposed allocating $7 million of that to cyber security. That is simply a failure to understand the threat posed by cyber terrorism. And it's not that E-Bay goes down so you and I can't buy stuff; it is that computers are in the control loop of every element of the Nation's critical infrastructure. So if you want to attack the electric power grid, you go after the control systems. So it's a serious issue.

Summary. The track record is clear, the Federal R&D investment has stimulated America's world leadership, our economic boom, our boom in all science and engineering. Current levels of Federal investment in IT R&D continue to be dangerously low. Thank you.

[The prepared statement of Dr. Lazowska follows:]

STATEMENT OF EDWARD D. LAZOWSKA

BEFORE THE HOUSE COMMITTEE ON GOVERNMENT REFORM SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS HEARING ON

"Defining Federal Information Technology Research and Development: Who? Where? What? Why? And How Much?"

July 7, 2004

Thank you, Mr. Chairman, Ranking Member Clay, and members of the Subcommittee for holding this hearing and for the invitation to testify before you. I'm pleased to focus my testimony today on two important questions the committee posed in convening this hearing: What is the government gaining from its investments in information technology research and development, and why should the government continue to make these investments? My comments are informed by my 30-year experience in academia as a member of the computing research community, and by my involvement as the co-Chair of the Computing Research Association's (CRA) Committee on Government Affairs, as the co-Chair of the President's Information Technology Advisory Committee (PITAC), and as a member of the Technical Advisory Board for Microsoft Research since its inception in 1991. I also have served as a member of the National Research Council's Computer Science and Telecommunications Board, where I participated in two studies of how innovation occurs in information technology, and as Chair of the National Science Foundation's Advisory Committee for Computer and Information Science and Engineering. I present this testimony as an informed individual, rather than as a representative of any particular organization, although my comments have the endorsement of the Computing Research Association and the Association for Computing Machinery U.S. Public Policy Committee (USACM).

The Impact of New Technologies

The importance of computing research 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 and networking 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, visualize large and complex datasets, and collect and manage massive amounts of data.

The Ecosystem that Gives Birth to New Technologies

A significant reason for this dramatic advance in computing technology 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 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 I've included it in my testimony today. (See figure 1.)

It's 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 9 of these multibillion-dollar IT industries (the categories on the left side of the graphic). Seven years later, the number of examples had grown to 19 – multibillion-dollar industries that are transforming our lives and driving our economy.

The graphic also illustrates the complex 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 couple of unappealing ways. First, it's hard to predict the outcome of fundamental research. The value of the research may surface in unanticipated areas. Second, fundamental research, because it's published openly, provides broad value to all players in the marketplace. It's difficult for any one company to "protect" the fundamental knowledge gleaned from long-term research and capitalize on it without everyone 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 5 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 complex nature of the chart also illustrates one other important characteristic of the IT R&D ecosystem – it's 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 internetworking 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, optoelectronics, 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, I believe, 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 cellphones, 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's 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 Bachelors-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.

Important Characteristics of Federal Support

The two dominant federal agencies in the development of the discipline of computing and the resulting innovation in IT have been the National Science Foundation (NSF) and the Defense Advanced Research Projects Agency (DARPA). The fact that the agencies have had two significantly different approaches to funding IT R&D has been an overall benefit to the discipline. Historically, NSF has focused on funding smaller awards to the individual investigator; in the process ensuring a broad range of research in the field was performed. DARPA, created in response to the Soviet launch of Sputnik and charged with insuring the nation was never caught "flat-footed" by a technologically superior adversary again, has historically focused on larger awards and building communities of researchers to address critical research problems – creating centers of excellence, many of which formed the basis of some of the top computer science departments in the country. In addition, funding opportunities at other mission-oriented agencies – NASA, Department of Energy, Office of Naval Research, the Air Force Research Labs – meant university researchers had a number of possible outlets for their ideas, and consequently, many good ideas that may have otherwise gone unfunded found their way into the knowledge base.

But in addition to a diversity of funding sources, the discipline (and, by extension, the nation) has been well-served by especially visionary program managers, especially at DARPA, drawn from university and industrial research labs who knew the discipline well and were given the flexibility to take risks with the research they supported with their program funds. As the National Research Council noted in the 2002 *Innovation in Information Technology* report:

> This style of funding and management allowed researchers room to pursue new venues of inquiry. The funding style resulted in advances in areas as diverse as computer graphics, artificial intelligence, networking, and computer architecture.

> As that experience illustrates, because unanticipated outcomes of research are so valuable, federal mechanisms for funding and managing research need to recognize the inherent uncertainties and build in enough flexibility to accommodate midcourse changes.

Unfortunately, there is significant concern building within the academic computing research community that DARPA has lost much of what made it so important to the discipline by adopting policies that discourage university participation in defense-related IT R&D. Of particular concern is DARPA's recent focus on shorter-term research efforts, its implementation of a "go/no go" decision matrix for DARPA funded research projects, the classification of research on certain topics (for example, cyber security, an area in which I know this committee has been particularly active), and restrictions on the participation of foreign nationals (e.g., U.S. graduate students who are not U.S. citizens).

The idea of "scheduling" breakthroughs or demonstrable results on 12-month timelines results in research that is evolutionary instead of revolutionary, with potential grantees only proposing research they can be sure will deliver results within the shorter timeframe.

There are, of course, important reasons for classifying federal research, especially when it's clear that the research might reveal our 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 classifying Defense Department cybersecurity 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.

There are additional concerns within the computing community about the under-investment in cybsersecurity research at the Department of Homeland Security, a concern I believe this committee shares. As you know, of DHS's new R&D budget of nearly $1 billion, less than 2 percent is being invested in cybersecurity R&D. And even this shockingly low level of investment was the result of Congressional outcry – DHS originally proposed less than 1 percent. IT systems constitute the "control loop" of most other elements of our nation's critical infrastructure – the electric power grid, the air traffic control grid, the financial grid, the telecommunications grid – and constitute a significant vulnerability. With the number of cyber attacks increasing annually at an almost exponential rate, it has never been more important to focus research on reducing our exposure to this threat. I applaud the subcommittee's work to focus attention on this critical issue.

PITAC is likely to examine these concerns as we move forward with our review of the nation's cybersecurity R&D effort this year.

I'd like to share one final concern about the nation's overall research and development portfolio. While it is true that the overall federal investment in research has been increasing over the past 30 years, the vast majority of this increase has been in the biomedical fields. Compared to that, all other fields have been essentially flat. (See figure 3.) The increase in investment in biomedical fields is incredibly important to the overall health and welfare of the Nation. However, I would argue that the disproportionate funding between the life sciences and the physical sciences and engineering actually has the effect of constraining innovation and advancement in biomedical fields. Information technology, for example, has enabled huge steps forward in biomedical research and in the practice of medicine – allowing for the visualization of molecules, the modeling of cellular and physiological processes, the imaging of the human body in extraordinarily detailed ways, and the sequencing of the human genome. New disciplines like bioinformatics and nanotechnology are poised to further revolutionize the field, but are both heavily dependent upon IT research and research in the physical sciences. The federal government must take a balanced approach to funding research and development to create the environment for innovation to flourish.

The role of PITAC

PITAC is a congressionally-chartered, presidentially appointed committee charged with assessing the overall federal investment in IT R&D. The committee is comprised of 25 non-federal academic and IT industry members. I am pleased to serve as co-Chair along with Mr. Marc Benioff.

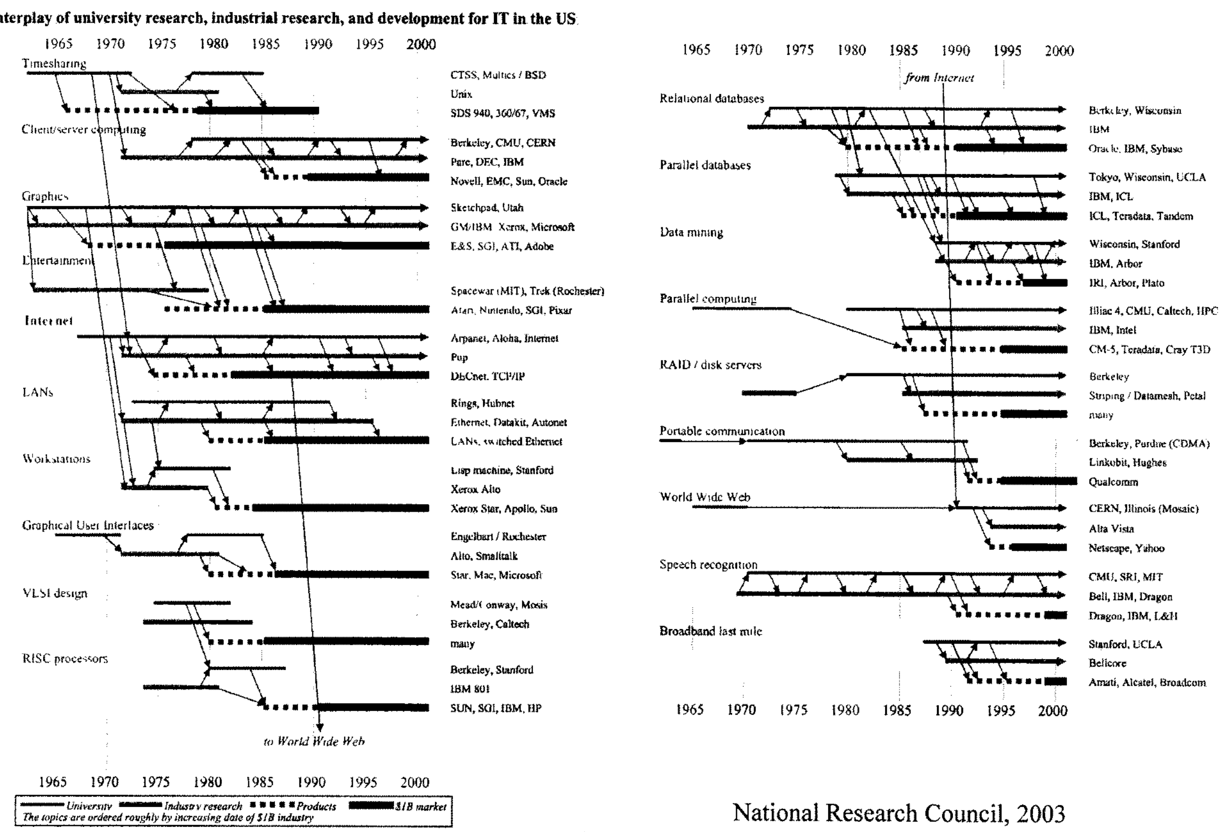
In 1997, President Clinton charged the members of his PITAC with evaluating the full breadth of the federal government's IT R&D portfolio. The resulting report, *Investing in Our Future*, released in 1999, emphasized the "spectacular" return on the federal investment in long-term IT research and development.

However, PITAC also determined that federal support for IT R&D was inadequate and too focused on near-term problems; long-term fundamental IT research was not sufficiently supported relative to the importance of IT to the United States' economic, health, scientific and other aspirations; critical problems in computing were going unsolved; and the rate of introduction of new ideas was dangerously low. The PITAC report included a series of recommendations, including a set of research priorities and an affirmation of the committee's unanimous opinion that the federal government has an "essential" role in supporting long-term, high-risk IT R&D. This opinion was buttressed by the inclusion of a recommendation for specific increases in funding levels for federal IT R&D programs beginning in FY 2000 and continuing through FY 2004 – an increase of $1.3 billion in additional funding over those five years. Actual appropriations for federal IT R&D have never reached the PITAC recommended levels, however. (See figure 4.)

The current PITAC was reconstituted in the spring of 2003 and has begun its work in three particular areas: IT and Health Care, Cyber Security, and the Current State of Scientific Computing. The first report of the Committee – on IT in Health Care – has been approved and should be released later this summer, with reports on the other focus areas to follow.

Conclusions

In my testimony today I've tried to make the case that the relatively modest federal investment in IT R&D has paid enormous dividends: changing our lives, driving our economy, and transforming the conduct of science. The 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 follow the recommendations of the NRC Computer Science and Telecommunications Board and insure that NSF and DARPA have broad, strong, sustained research programs in IT independent of any special initiatives. And we should work to maintain the special qualities of federally-supported university research.



National Research Council, 2003

Figure 1.

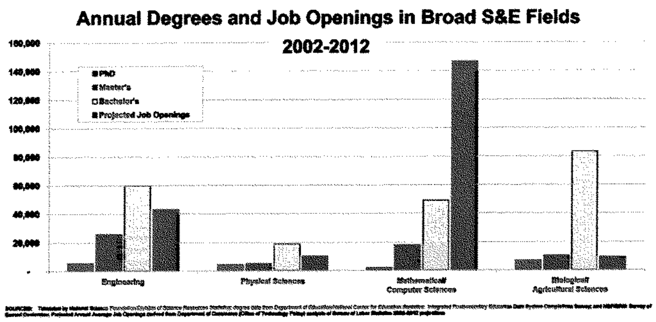


Figure 2

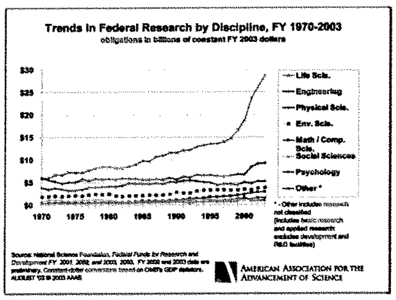


Figure 3

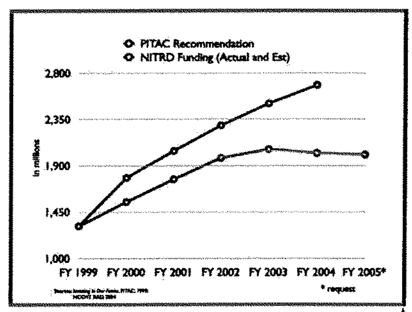


Figure 4

Mr. PUTNAM. Thank you very much. You all are really opening up some fascinating pieces for us to explore on questioning.

Our next witness is Dr. William L. Scherlis. Dr. Scherlis is a professor in the school of computer science at Carnegie Mellon and a member of CMU's International Software Research Institute. He is the founding director of CMU's Ph.D. program in software engineering. He is principle investigator of the 5-year high dependability computing project with NASA in which CMU leads the collaboration with five universities to help NASA address long-term software dependability.

His research relates to software assurance, software evolution, and technology to support software teams. He first joined the CMU faculty in 1980, after completing a Ph.D. in computer science at Stanford University and an A.B. at Harvard. He interrupted his career at CMU to serve at DARPA for 6 years, departing in 1993, as senior executive responsible for coordination of software research. While at DARPA, he had responsibility for research in strategy and computer security, high performance computing, information infrastructure, and other topics that we would be shot if we disclosed. He has served as program chair for a number of technical conferences including the ACM Foundations of Software Engineering Symposium, and he has more than 70 scientific publications. Welcome to the subcommittee. You are recognized.

Dr. SCHERLIS. Thank you very much. Mr. Chairman and members, I appreciate the opportunity to appear today to discuss R&D for information technology. I'm going to make the case to you that strategic Federal IT R&D is now more important than before, and that we need proactive leadership to move it forward. We rely on IT systems pervasively in our economy for national security, for health care, and for the operations and safety of our infrastructure. The industry and research community have made rapid progress in the capability, performance, and interconnection of IT systems. But despite this rapid progress, software and IT generally remain immature as engineering disciplines. We continue to struggle with quality challenges related to cyber security and software dependability. We do not yet know how to achieve high levels of quality in critical systems without huge sacrifices in capability and flexibility and huge costs to test and inspect.

For both cyber security and software dependability we are not in a good state. In cyber security, our stop gaps of firewalls, spam filters, intrusion detection and the like are not slowing the growth in exploits and vulnerabilities. This is a chart from the CERT that indicates the number of incidents that have been reported year over year. We are not succeeding in evaluation and validation. The Common Criteria ISO 15408, for example, does not yield guarantees regarding an absence of malicious code. In software dependability, we cannot in general make strong promises on the basis of testing and inspection. The coverage is not good enough. We supplement this by looking at how the code was developed and who did it. But these are poor proxies. We cannot, in general, fully evaluate software artifacts directly. Even when we can see every line of code, we cannot make promises about the systems we build.

It is tempting to conclude that this bad state is intrinsic to IT; that things are the way they will be—for example, that because we get e-mail, we will also get huge volumes of spam. Or, that we are at a plateau—the pace of innovation is slowing down, the 1990's are over. Or, that the sheer mass of the deployed base will inhibit any fundamental change—can we switch the entire country over to drive on the left-hand side of the road?

These conclusions are counter to the historical truth of IT for the past 40 years. There has been a constant technology revolution under the hood in operating systems, data bases, client server architectures, networking, languages, and so on. The research community, the successful IT companies and their customers all know how to handle this pace of change because they have been doing it for so long. In many areas, it is happening right now. But not in the most critical areas related to quality. We are almost complacent with our extreme vulnerability.

However, there is reason to hope for the future. There are promising research results in the pipeline that bear on these major challenges. For example, more secure network protocols and services. Improved identity and authorization management. Techniques for the direct evaluation of software. Securable architectures for resilient designs.

Given this, it's tempting to think that with the large R&D budgets the IT industry will take care of this and the government can step back. And this is wrong. Part of that historical truth of the past 40 years is that the Federal Government has consistently been an active player and leader in that process. And I'm going to give you four reasons why, and these reasons have to do with why industry does not in general look beyond more than one or two product cycles out.

First, many of the most significant research results that bear on IT quality are nonappropriable. That means that their value diffuses rapidly across the market. It cannot be retained, it becomes a public good. Only government is going to sponsor this work. Bill Gates, for example, talks about a tool that is now used to reduce the frequency of blue screens. This tool is based on technologies that were developed a decade ago by my university colleagues and sponsored by NSF and DARPA: binary decision diagrams and model checking.

Second, the early definition of standards has a particularly significant role in IT. This is the so-called prenormative work most vividly illustrated by the role of the IETF in the early days of the Internet and the role of the W3C more recently. The world of E-commerce is held together by standards such as TCP, IP, XML, HTTP, and so on.

Third, government is a major IT consumer. It needs to collaborate with its entire simply chain, just like the auto industry. Long ago, DARPA exerted profound influence on networking and operating systems and processor design to create an amazingly scalable foundation for network centric warfare and modern command and control generally. It worked directly with the vendors, the innovators, and the researchers throughout the DOD supply chain.

And, four, the main input to the IT food chain is university research and education. Without the people and expertise and the innovative attitude, we have nothing.

There is another reason. IT innovation leadership is pivotal to the future of our country. I'm here from Pittsburgh. We can argue about the strategic necessity of leadership in steel or in consumer electronics, but IT innovation leadership is different. We cannot give it up. It's a driver of productivity, as Alan Greenspan has noted. It is a principal force multiplier in defense. And, perhaps most importantly, we still see no bounds on the potential for creating new value, new kinds of capability and cognitive powers. The frontier of innovation will continue to exist well beyond the frontier of commoditization. It will be our future for a long time.

My conclusion is that we need proactive Federal R&D leadership. We need both basic science and mission motivated Federal R&D in order to retain our leadership position and to address the new challenges that we face. In the public private partnerships—the collaborations of industry, academia, and government—the government must be a full partner. I appreciate the opportunity to appear today.

Mr. PUTNAM. Thank you very much. I appreciate it, Dr. Scherlis.

[The prepared statement of Dr. Scherlis follows:]

Statement of Dr. William L. Scherlis
Professor, School of Computer Science
Carnegie Mellon University

Before the U.S. House of Representatives
Committee on Government Reform
Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census

Federal Information Technology Research and Development
July 7, 2004

Mr. Chairman and members of the Committee. My name is William Scherlis, and I am a Professor in the School of Computer Science at Carnegie Mellon University, where I direct a newly inaugurated PhD program in Software Engineering and lead a research project involving CMU and five other universities related to software dependability. Earlier in my career, I spent more than six years at DARPA managing research programs in areas including trustworthy systems, high performance algorithms, and software technology. I departed from that position to return to research in 1993. Our present project work is in collaboration with NASA, and has the goal of helping improve the safety and dependability for future generations of software-intensive mission systems. Software dependability is particularly important for NASA, and as you know it has broad significance for the security of our nation and its critical infrastructure.

I appreciate the opportunity to appear before you today to discuss the need for research and development for information technology. In this testimony, I address two areas of information technology (IT) that present particular challenges to federal agency CIOs and mission managers—cybersecurity and software dependability. These areas are among a number of IT challenges facing federal managers that are considered in an NSF-sponsored National Research Council study I led on IT for e-government (http://www.nap.edu/catalog/10355.html). I highlight these two areas because of their fundamental strategic and economic significance, and because of the importance of far-sighted strategic R&D to future agency systems.

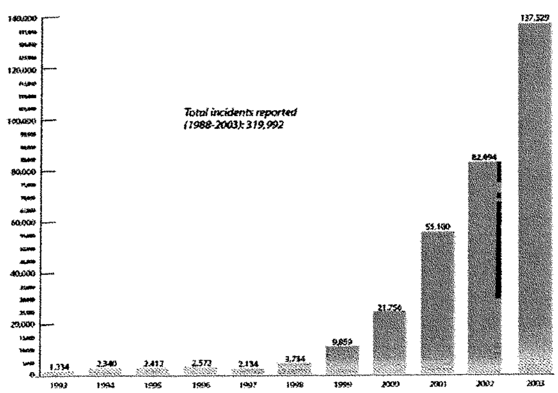
Most IT leaders and computer scientists believe that IT is still evolving rapidly, and nowhere close to a plateau, either with respect to capability or quality. Mission managers will face a very different environment in the future—even in five years. We have a huge national stake in the definition of that environment.

This examination leads to three conclusions: (1) Strategic long-term federal IT R&D is more important now than before. (2) We must retain our national advantage in innovation leadership. (3) We need pro-active federal R&D leadership for critical IT challenges. This statement addresses primarily the "who," "what," and "why" questions posed by the Subcommittee.

1. Mission IT Challenges: Cybersecurity

Stop-gaps. Let us consider a mission manager who must provide an immediate cybersecurity solution for an organization. Following today's best practice, the manager will apply a range of available security interventions such as managed networks, firewalls, virus detection, intrusion detection systems, patch management, configuration management, and spam filters. Unfortunately, most of these interventions are stop-gaps that only partially address the weaknesses intrinsic in today's engineering practices and network and system architectures. With these interventions, the manager will be slightly less exposed in the current war of attrition (for example, between virus writers and virus detection tool creators). But statistics from the CERT and other sources suggest quite vividly that we will not win this war with the current set of interventions (http://www.cert.org and http://uscert.gov). There is a broad consensus that the stop-gaps are failing and more fundamental kind of progress is needed, despite the significant improvements in quality we have experienced over the years. The CERT security "exploit" and vulnerability curves continue to trend upwards geometrically (see chart below, from the CERT/CC).

Incidents Reported to CERT/CC



Product evaluation. Cybersecurity evaluation is a kind of product acceptance testing for security attributes of IT components and systems. The difficulty of evaluation is evident in established processes such as ISO 15408—NIST's Common Criteria (http://csrc.nist.gov/cc/). Commercial vendors may spend a year or more undertaking a system evaluation, which leads to useful and important assurances regarding specification and design. But the evaluation does not—and indeed cannot at this stage of development—assure an absence of malicious code or other vulnerabilities. Nor can it easily extend from a particular system instance to a family of configurations. These difficulties are consequences of the fact that general-purpose technical means are not yet available to make such evaluations and, from an engineering standpoint, to make positive promises about software and IT components. Indeed, many of the fears regarding outsourcing and open source derive from the difficulty of evaluating the safety, dependability, and security of software, even when the code is fully available for inspection. The technical advances that are most promising in addressing this problem rely on deep mathematically-based techniques to analyze software code directly.

Engineering practices. We may conclude from the foregoing that we are unable to build secure systems—or evaluate those that we ourselves create—and that, more significantly, there are intrinsic characteristics of software and IT that place us in this quandary. This is not the case. Rather, it is simply the immature state of current technical understanding and engineering practice. Technical progress in the NITRD research portfolio suggests that strategic R&D effort can lead in the long run to fundamental changes in our ability to deliver higher levels of security (http://www.nitrd.gov). There are several recent reports from the Computer Science and Telecommunications Board of the National Research Council that summarize recent results and offer recommendations (http://www.cstb.org).

In the meantime, for the most highly critical systems, the present practice is to accept severe constraints on system capability and architecture in order to achieve the possibility of acceptable levels of assurance. In other words, our lack of ability to do evaluation forces us to limit the capability of the critical systems we build. There are emerging research results that demonstrate how key architectural and design commitments, coupled with analysis tools, may offer steps away from this state of limited capability. These results include, for example, self-healing architectures, framework designs for composable components, component evaluation tools, techniques for safe concurrency, etc.

Future systems. Many government agencies face cybersecurity challenges that lead the market in significant respects. (Additional examples of IT areas where government is a demand leader are offered in the e-government study cited above.) Managers who are planning next-generation systems can benefit by collaborating with the multi-agency R&D community in order to address these needs in a more strategic manner. This pattern—of investing in R&D in the supply chain in order to ensure future needs can be met—is well established in other industries, for example in supply chains for automobile and airplane design and manufacture.

In government, there is a record of success in major mission agency IT consumers applying this model, particularly DoD. The idea is to follow the established market model of supply chain management, which involves working with all levels of suppliers, helping them anticipate critical needs, and investing in R&D that has broad benefits. This market-based approach, in which major technology consumers, but particularly government mission agencies, collaborate through the supply chain to accelerate response to leading edge requirements, has stimulated much of what we take for granted in modern computing.

Many important cybersecurity improvements are already in the early stages of the R&D pipeline, including, for example, better security-focused engineering processes, evaluation and analysis tools, component designs, more secure network protocols and services, more securable system architectures, improved identity and authorization management schemes, architecture for self-healing and resilient systems, and others.

2. Mission IT Challenges: Software Dependability

A second area of IT challenge facing CIOs and mission agency managers is software dependability. Software dependability is critical for systems safety (such as for medical devices, plant control systems, and weapon systems), for management of sensitive records (such as for law enforcement, government financial and tax records, and health care records), and for critical infrastructure (such as for SCADA—supervisory control and data acquisition systems).

Software dependability is also fundamental to cybersecurity. More than 90% of the thousands of exploits reported annually to the CERT build on software flaws. Some observers have stated that these flaws exist because vendors feel they can "get away with" shoddy quality. This is not true. Rather, these flaws are the result of the fact that both the industry and the R&D community are still struggling with how to achieve high levels of quality in software engineering practice.

Process and quality. Today, software program managers generally employ traditional engineering management approaches that are taken from the statistical quality community. These involve process and metrics, with the metrics used as feedback to improve both product and process attributes. This is the essence of the ISO 9000 family, Six-Sigma, SEI's CMMI, and other process-based approaches. These are excellent, workable, and widely adopted approaches that have provided enormous benefit to projects of all sizes.

But the statistical approaches have a stop-gap character—they do not address all the challenges of producing dependable and secure software. In particular, software bugs are flaws of design and implementation—software components are not like physical systems that wear out over time. In cybersecurity, for example, when the threat model is based on frequencies of spam-zombie viruses, port scans, and spyware intrusions, the resulting system design may not be appropriate for a multi-point attack by a determined adversary. In addition, all software faults are not created equal, either with respect to the kinds of system failures they may trigger or the difficulty of repairing them. Some faults may be intrinsic in the system architecture, while others are mere coding oversights. The Common Criteria, noted above, assists in making this latter distinction with respect to security.

Software quality. A Defense Science Board task force noted that, "improvements to process, training, incentives, and procurement are critical, and yet improvements to the process without improvements to the technology cannot address the staggering complexity necessary for achieving a national competitive advantage." The President's Information Technology Advisory Committee (PITAC), in its inaugural report, noted that

"Our ability to construct the enormously complex software systems that lie at the core of our economy (is) painfully inadequate. Therefore, the increases in research on software should be given a high priority" (http://www.nitrd.gov/pitac/).

Industry leaders also recognize the seriousness of the technical challenge. Two months ago, the Business Roundtable, representing 150 U.S. CEOs, issued a report that notes, "Most of the significant cyber incidents that have harmed American business and consumers over the past several years have had at their root cause defective and readily exploitable software code." It adds, "Most software development processes used today do not incorporate effective tests, checks, or other safeguards, to detect those defects that result in product vulnerabilities" (http://www.businessroundtable.org). The Washington Post titled its report on this study, "Old Economy Fed Up With Cyber-Security."

Evaluation and assurance. As noted above, software assurances in present practice are usually based on indirect measurements—evaluation of process or organizational attributes as substitutes for direct evaluation of a product. Because existing measures are weak and overly approximate, it is difficult to build an ROI model—the "R" cannot easily be measured and so the "I" is not readily forthcoming. Improving our ability to measure the "R"—at every level from code-level fault identification to organization-level failure impacts—is part of the process of maturing the discipline. More concretely, research attention must be focused in areas such as: (1) Improved technical means to evaluate system components directly for critical security and dependability attributes, (2) Better techniques to engineer software with higher levels of security and dependability "out of the box," and (3) Principles of architecture, design, and coding that can reduce the overall impact of internal engineering faults (such as buffer overflow) on the kinds of failures that can result (such as compromise of data or loss of service).

There is some basis for optimism—including significant emerging research results (for example, relating to modeling of critical attributes, software analysis, and model checking techniques), and good indicators in industry practice that a business case is starting to emerge (an example from Microsoft is cited below).

Progress on this challenge has high leverage because it exists at every producer/consumer interface in supply chains for IT systems. Producers benefit by being able to provide concrete evidence of security, dependability, or other quality attributes. Consumers benefit when they (or third-parties acting on their behalf) can undertake effective acceptance evaluations.

3. The Essential Role of Government R&D

These challenges—cybersecurity and software dependability—have three important common characteristics. The first is that there is a compelling case, based on both need and opportunity, to develop R&D approaches that are strategic. These are fundamentally different in character from the current stop-gap practices. Second, in both areas there are government mission agencies whose requirements anticipate rather than follow market demand. Cybersecurity and software dependability are important for everyone, but these needs are frankly more urgent for our national and infrastructural systems. Third, critical and mainstream solutions are converging rather than diverging. Many critical infrastructural systems, national defense systems, and enterprise systems are constructed from diverse components from diverse sources, and such systems may include extensive use of many familiar pervasive IT applications and components. In other words, what is pervasive is also becoming critical. And, engineering practices for critical systems are not that far beyond engineering practices for the pervasive systems. It is dangerous, therefore, to contemplate solutions where government and other critical consumers separate from the mainstream market.

Will industry do it? It is tempting to think that, while these problems—cybersecurity and software dependability—are challenging, the IT industry will eventually address them as a matter of course—that "industry will do it." In many other industries this is a legitimate conclusion, and best policy for meeting government requirements may be to follow the market. But this is generally not true for IT. And in fact it defies the historical truth of the past 50 years of IT innovation.

The leadership in IT innovation that we currently enjoy in the US is the legacy of several decades of effective and steady Federal R&D leadership, much of which is in response to the leading-edge requirements of government mission agencies. A recent National Research Council Report called "Innovation in Information Technology" notes that, regarding modern electronic commerce, "nearly every key technological component has been shaped by [federal] investment," including the Internet, web browsers, public-key cryptography, back-end database and transaction processing, and search engines. The report illustrates this by tracing the research origins of more than a dozen multi-billion dollar IT markets (http://books.nap.edu/catalog/10795.html).

The unique government role. Why is the government R&D role so essential for IT? The answer has three parts:

a. Non-appropriability. Many of the most significant research results in IT are non-appropriable. That is, there are foundational results that cannot successfully be confined to a single sponsoring organization—their impact diffuses broadly into the technical community and the market. It is difficult for firms to build an ROI model for investing in this kind of research, whose results may diffuse directly to competitors. Many of the most important concepts of information technology are in this category. The revolutionary concept of networked personal computing developed principally at Xerox PARC under a combination of federal and private sponsorship is an example. In the end, it didn't do much for Xerox, but it triggered the creation of an entire industry.

In the area of software dependability, there is recent evidence in the R&D community of progress in addressing some of the longer-term needs. Companies such as Microsoft and IBM are developing a new generation of engineering tools to improve software quality through direct analysis of software code and other artifacts. The Microsoft tools are partly responsible for the significant reduction in the frequency of "blue screens" in the past couple of years. Of the tools I am aware of, most rely on fundamental technical concepts that were developed earlier in university labs, generally sponsored by NSF, DARPA, and other NITRD agencies. These concepts include, for example, finite-state model checking, binary decision diagrams, rule-based inference, and many program analysis techniques.

b. Commonalities. The early definition of standards is a critical element of the pattern of innovation in the IT industry. Government has had a long-standing role in facilitating the so-called pre-normative work that leads to the commonalities critical to the creation of markets for new IT capabilities. The early IETF had a pivotal role and provides an important model for consensus management in a community of innovators. For example, the first versions of the fundamental standards of the modern web-based Internet (IP, TCP, HTTP, HTML) were developed by a handful of researchers, all working under government sponsorship, collaborating through the IETF.

c. Education and universities. More obviously, the research programs in most universities and labs are closely coupled with the education enterprise. The direct engagement in the most aggressive research, including traditional exploratory basic research and far-sighted mission research, creates the next generation of inventors and innovators, who become tomorrow's industry leaders.

Industry senior managers recognize the need for R&D. Two months ago, Craig Barrett, the CEO of Intel, said to USA Today, "We have to invest more in R&D. If you have a worse education, a worse infrastructure, and you spend less of your gross domestic product on R&D, what makes you think you should be in a pre-eminent position?" Perhaps most importantly, he notes the importance to US employment of "research and development investment that is government funded," noting that the fraction of output that has gone to R&D has declined over the past two decades. "R&D creates the ideas for future products and services."

4. Moving Forward

The difficulties we are facing nationally with cybersecurity and software dependability are consequences of the limitations of our present engineering capability. Software is an unusual building material, almost unlimited in its potential for capability and scale—but we are still learning how to work with it successfully, and particularly how to create systems that are genuinely dependable and secure. This is ironic, because IT has become pervasive and, as noted recently by Alan Greenspan, is an important contributor to national productivity. But this immaturity need not persist—many in industry and universities believe that a combination of public-private partnerships and aggressive federal R&D can lead to fundamental change.

I conclude my statement with three observations:

1. Strategic long-term federal IT R&D is more important now than before.

The NITRD agencies identified in the President's Budget, along with the Department of Homeland Security, share leading-edge requirements for advanced IT capability. They recognize the necessity of stimulating innovation in order to ensure that their future mission requirements can be effectively met. By collaborating with each other they can share new technologies, spread risks, and build more effectively on the basic science portfolio principally sponsored primarily by NSF.

The NITRD process, which began with the High Performance Computing Act of 1991 and is now led by Dr. David Nelson and Dr. Peter Freeman, is an effective mechanism to support this coordination among mission agencies. NITRD has several coordinating teams focusing on specific issues and supporting strategy development. Cybersecurity is addressed by several of the teams, most notably the High Confidence Software and Systems (HCSS) coordinating group. Software dependability is also addressed by several teams, principally the Software Design and Productivity (SDP) coordinating group and the HCSS coordinating group (http://www.nitrd.gov/pubs/blue04/). Challenges related to achieving significant new levels of systems capability are addressed at several agencies, particularly at the NSF in the new Science of Design research program and at DARPA/IPTO (http://www.darpa.mil/ipto).

In the strategic planning process, it is essential to understand that we are not at a plateau in any aspect of IT capability. The capability, performance, and interconnection of IT systems are advancing at a rapid rate. Many in the industry recognize that Moore's Law will continue to hold for another decade or more, and that we are likely to experience several more decades of the kind of rapid innovation we experienced in the past ten years, which brought us the public Internet, World Wide Web, e-commerce, e-government, grid computing, and many other fundamental changes.

The critical challenges of IT are increasingly focused on quality and assurance, and this is why in this statement I have highlighted the areas of cybersecurity and software dependability. There are other areas of critical need. The NITRD agencies should be given the charge—and the resources—to address these challenges in a strategic long-term fashion.

2. Addressing these quality issues is fundamental to retaining our national advantage in IT innovation.

The NITRD innovation investment, including both mission-focused investment and the basic science component primarily at NSF, is essential to our national success in an international market that is becoming increasingly competitive with respect to IT innovation leadership. The patterns of IT innovation and the value of IT innovation leadership are now increasingly understood throughout the world—and many countries are making national-level commitments on this basis. Many believe that loss of IT innovation leadership will, for national security, have more severe consequences than the losses the U.S. has experienced, say, in steel or much of consumer electronics. (Note, however, that this does not imply that offshore outsourcing and open source are necessarily bad for the U.S.—the economic story in these cases is nuanced, with both positives and negatives, and few general answers.) The point is that we need to maintain our strength in IT innovation. We can do this only by leading in education and in well-managed R&D.

3. Establish pro-active R&D leadership for the critical IT challenges.

Needs and opportunities have been well articulated in many studies and workshops in the past few years. It is now time to build on this progress by taking the next step, and defining some elements of a national strategy that is far-sighted in terms of impact, but actionable and concrete in terms of R&D activity. There are important new concepts and technical opportunities emerging in many labs across the country. The purpose of a national strategy is to link these efforts together to accomplish the next critical set of changes in the constantly-changing landscape of IT.

As noted in the previous section, development and execution of the strategy must be a collaborative process involving research leaders and far-sighted users in industry, academia, and government. An example of a collaboration focused on strategy development is the Accelerating Trustworthy Internetworking (ATI) initiative (http://www.ati2004.org). The most recent ATI workshop included active participation from industry, government, and academia. The purpose of the strategy is to provide a focus for government R&D in selected critical areas.

Long-term mission-motivated federal R&D is how the U.S. established its present IT leadership position, and it is what we must do both to retain this position and to address the new challenges that we now face. This will require collaboration of government, industry, and academia.

Thank you for giving me the opportunity to testify today. I would be pleased to answer any questions.

Mr. PUTNAM. Dr. Squires, you are going to have a few moments to collect your thoughts to defend HP's honor with regard to your R&D budgeting. We are going to recess for a moment while we go have one vote. It should be a fairly brief recess, and we will return shortly. So everybody sit tight, enjoy your orange juice. And the subcommittee will stand in recess.

[Recess.]

Mr. PUTNAM. The subcommittee will reconvene. I apologize for the delay.

Our final witness for this panel is Dr. Stephen Squires. Dr. Squires is the chief science officer and vice president at Hewlett-Packard. He is also a Special Government Employee Expert Consultant for the Department of Defense through the Defense Advanced Research Projects Agency [DARPA]. In that role he is a member of the Intelligence Science Board and also served on the Defense Science Task Force on Defense Roles and Missions for Homeland Security and other special working groups. Previously, he worked for NSA for 15 years on IT systems.

We look forward to your testimony. You are recognized, Dr. Squires.

Dr. SQUIRES. Thank you for inviting me to testify. I consider it an honor and a privilege to be here to discuss these critical issues.

I want to focus on one main issue which was in the letter that invited me, and that issue is how the investments serve to protect this Nation and position the United States as a leader in the information technology arena.

My answer to this critical question is based upon my understanding of the history of IT, my own direct experience and expertise in the most advanced research and development application programs focused on the most challenging problems facing the Nation, and my own vision of the future.

The best way I can think of starting is to reference a paper titled "As We May Think" by Vannevar Bush in July 1945. It was written in his role as Director of the Office of Scientific Research and Development, coordinating activities of some 6,000 leading American scientists in the application of science to warfare. You should actually take a look at this article. It presents an extraordinary vision filled with all kinds of interesting examples, including one example called the "memex," which is essentially the Internet with a web of linked objects.

The history of information technology is dominated by fundamental devices from the invention of the transistor, the integrated circuit, and the microprocessor, along with many other devices for the past 50 years and an extraordinary collection of systems developed through multiple layers of modules, structures, and massive amounts of software to support a wide range of applications.

Information technology has become increasingly pervasive. It is hard to imagine life without it. Our national defense, homeland security, depend on it, in addition to our critical infrastructure, the economy, and the future of science and technology.

IT industry and its applications have become a multitrillion dollar sector of the global economy that is recognized as enabling a new global dynamic. Information technology as generally viewed today appears to be a commodity, but it is not. The larger IT companies claim to have multibillion dollar R&D programs, which they do. But it is also very important to understand the operating point and the time horizon of those programs.

It is natural for many people familiar with normal technologies to believe that there has been more than enough U.S. investment in the future of information technology and enough is enough. Let me say now in the strongest possible terms that I believe that such a belief is fundamentally misguided and in my opinion dangerous.

The entire field has been through multiple revolutions and extraordinary advances that have been made across a wide range of science and technology areas. But with all of these advances and all of this investment in the past 50 years, we are really only at the beginning of a much longer process.

As the limits of what have become conventional integrated circuits are reached, new technologies with its revolutionary implications are emerging at the atomic scale in the form of nano-technologies. New nano-devices can be integrated into new kinds of things such as new kinds of nano-integrated circuits with extraordinary properties, and properties that go beyond just computing to include new kinds of storage, sensors, effectors, and new ways to act with the physical world, including biological.

The advances in these new devices will enable new kinds of modules, new kinds of units of replication, and present new challenges, challenges which simply will not be overcome by conventional industrial R&D. These, the new kinds of systems which we can imagine happening and emerging over the next 50 years, or even the next 10 or 20 years, will be far more dramatic than anything we have seen in the last 50.

Let me just give you some examples of the role of information technology that go beyond normal market trends: The role of information technology in things like critical infrastructure of the country, in science and technology itself, in national defense, homeland security, trusted information sharing, protecting individual privacy, and the most important of all, protecting the future of civilization.

Let me briefly sketch four alternative futures. I'm just going to call them red, orange, yellow, green in the context of an idealistic vision, blue.

Red is essentially pre-Internet technology.

Orange is essentially an attempt to extend the red to cope with the emerging Internet revolution.

Yellow is essentially an attempt to apply commercial Internet technology to the challenges of the Internet.

And green is essentially the development of fundamentally more advanced technology than commercial Internet technology for the purpose of achieving strategic advantage. Such systems have more advanced cybersecurity than the commercial Internet.

And then all of this is set in the context of blue, which is an idealistic vision of the future which I call "intrinsic trust" and that is the essential distinguishing characteristic of the fundamental advance needed for the future of information systems themselves.

The most challenging problems provide insight needed to establish the most effective advanced research agendas. The ideal of blue is essential to guide the advanced research agenda for green.

Given its own market forces, the information technology system will simply be stuck on the yellow brick road. The insights needed to create effective advanced research agendas emerge from interdisciplinary interaction among science, business, homeland security and national defense. The interactions are more critical because the need for public-private systems to interoperate over a wide range of modes are all dependent upon critical and pervasive interoperable information systems capable of trusted information sharing while protecting privacy.

I believe it is essential that the U.S. Government continue to invest in advanced research and information technology focused on protecting this Nation and ensuring that the United States continues to be the world leader in information technology. The future leadership depends upon continuing advances in science and technology at a time when information technology itself is not only becoming critical and pervasive but itself going through its own reinvention process.

Mr. PUTNAM. Does that conclude your remarks?

Dr. SQUIRES. Yes.

Mr. PUTNAM. Thank you very much, and I apologize for making you wait.

[The prepared statement of Dr. Squires follows:]

Testimony
to
Congress of the United States
House of Representatives
Committee on Government Reform
Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census

Defining Federal Information Technology Research and Development: Who? Where? What? Way? and How Much?

Focusing on
how investments in Information Technology
serve to protect this Nation and
position the US as a leader in the Information Technology arena.

Stephen L Squires, PhD

Hewlett-Packard Company
Chief Science Officer
Vice President

July 7, 2004

This testimony and associated statements are based on my personal expertise and experience and is not necessarily the official position of the Hewlett-Packard Company

Executive Summary

Introduction

Thank you for inviting me to testify.
I consider it an honor and privilege to be here to discuss these critical issues.

My name is Stephen L Squires. In the private sector, I am the Chief Science Officer of the Hewlett-Packard Company. I am also a Special Government Employee (without compensation) Expert Consultant for the Department of Defense though the Defense Advanced Research Projects Agency. In this role I am a member of the Intelligence Science Board and also served on the Defense Science Board Task Force on Defense Roles and Missions for Homeland Security and other special working groups.

My testimony today is based on my own experience and expertise and does not necessarily represent the official position of HP or any other organization.

I will focus on what I believe is the most important issue identified in the letter requesting my testimony on the role of Federal investment in IT R&D.

> **Quote** *We also are interested in discussing how these investments [in Information Technology] serve to protect this Nation, as well as, position the US as a leader in the information technology arena.* **End**

My answer to this critical question is based on my understanding of the history of IT, my own direct experience and expertise in the most advanced research and development and applications focused on the most challenging problems facing the Nation, and my vision for the future.
My testimony is organized into four sections.

- A brief reference to history
- My own experience and expertise
- My Perspective
- Alternative Futures

A brief reference to history

The best way I can think of to start is a brief reference to history is the article titled "As We May Think" by Vannevar Bush in July 1945. The article was written in his role as Director of the Office of Scientific Research and Development, coordinating the activities of some six thousand leading American scientists in the application of science to warfare. He presents an extraordinary vision filled with a multitude of interesting examples including some in information technology. For example, he describes a system called "memex" that is essentially the Internet with a web of linked objects.

> The URL for the article is
> <http://www.theatlantic.com/unbound/flashbks/computer/bushf.htm>
> and can be accessed on the Internet using a standard browser.

The history of modern Information Technology is dominated by fundamental devices from the invention of the transistor, the integrated circuit, and the microprocessor along with other devices for the past 50 years. An extraordinary collection of systems have been developed though multiple layers of modules and structures to support a wide range of applications. The general term that describes the existing system is the Internet.

Information Technology has become increasingly pervasive. It is hard to imagine life without IT. And, our National Defense and Homeland Security depends on IT in addition to our Critical Infrastructure.

My own experience and expertise

I was recruited by NSA as a freshmen undergraduate electrical engineering student where I worked in its most advanced communications and information technology advanced research laboratories. Those laboratories focused on the most challenging problems, pursued advanced research to develop potential solutions, and worked with mission organizations to develop actual solutions. The extraordinary people that I had the privilege to work with and learn from for over 15 years made major contributions to much of the Information Technology revolution until the early 1980s. The extraordinary Information Technology systems of NSA made major contributions to winning the Cold War.

I joined ARPA in 1983 where I contributed to the vision, strategy, leadership, and management of advanced computing systems architecture that produced the technology base and foundation for the Federal High Performance Computing and Communications Program in 1992 and its extension to the National Information Infrastructure. It may be of interest to note that I testified to advocate the proposed legislation that initiated that program.

During my career with DARPA, I continued to maintain a close working relationship with the Intelligence Community. And, I was often called upon to participate in special working groups focused on critical issues of maintaining or achieving strategic advantage through advanced Information Technology. In fact, it was during a particularly frustrating period with one these working groups that I developed a briefing titled "Breaking out of the 'post-Cold War' Syndrome" in March 2000. This briefing focused on the limitations of existing information systems and the need for a new kind that would enable trusted information sharing along with other advances to achieve strategic advantage.

I joined HP in mid November 2000 as the Chief Science Officer, a new position created to focus on fundamental issues of Information Technology futures.

Less then a year later ...

On the morning of 9.11,

it is still painful for me to think of that moment

— a globally shared moment in time —

I was at NSA that day on the second day of a two day meeting.

I was a member of a special working group focused on certain advanced technology issues to achieve strategic advantage in the new world of the Internet.

In general terms, these issues are an important aspect of this hearing

when we focus on the role of Information Technology

in National Defense and Homeland Security to

"*protect this Nation, as well as,*

position the US as a leader in the information technology arena"

as raised in the letter inviting me to testify.

My Perspective

New discoveries and new application challenges affect the dynamic and rate of change of the system of science, technology, and applications. The US Government has had a critical enabling leadership role in accelerating the advanced research, development, and application of IT since its beginning.

While the academic and commercial activities are generally well known, the relationship with the National Security Establishment is not because attention is normally deferred to the civilian departments, administrations, agencies, and organizations. The major exception to this is the Defense Advanced Research Projects Agency (DARPA) created as ARPA by President Eisenhower shortly after the launch of Sputnik. The DARPA focus has been and continues to be on advancing the frontier of science and technology in areas critical to the Defense mission. DARPA has had and continues to have an extraordinary impact on IT and related technologies.

The DARPA model is so successful that it serves as a model for others. We can only hope that the new HS ARPA in DHS is able to achieve its expectations. There is a similar kind of organization operating in the Intelligence Community. These are working together, complementing each other, building on each other's results, reducing risks, and accelerating technology transition. These investments also work to complement those of the National Science Foundation. The mission agencies also have their own research and development programs that work with the others in an effective complementary way including the National Laboratories. The collections of activities form an extraordinary system that has accomplished great things in cooperation with the academic and industry sectors.

Most of the work is done in the open. Most of the results first emerge in the academic and industry sectors. Many of the results transition into commercial products that are used by all sectors including the national security sector. But the goals, strategies, tactics, and management are often motivated and guided by classified issues, challenges, and applications—applications by the earliest of the early adopters.

The challenges of World War II, the Cold War, and the post 9.11 era each have their own distinctive characteristics. In the post 9.11 era the power and potential of Information Technology is recognized throughout the global community communicating and collaborating though the Internet

— a globally recognized phenomena.

IT industry and its applications have become a multi-trillion dollar sector of the global economy that is recognized as enabling new global dynamics.

Information Technology has become a commodity. The larger IT companies claim to have multi-billion dollar research and development budgets. The White House estimates that 85 percent of the critical infrastructure is in the private sector with much of it dependent on commercial information technology.

Therefore, it is only natural for some people familiar with other technologies to believe that there has been enough US Government investment in the future of Information Technology.

Let me say now in the strongest possible terms that such a belief is fundamentally misguided and absolutely wrong to the extent of being dangerous.

Now let me explain in terms of the one sentence I referenced in the letter inviting me to testify today.

> How investments in research and development on information technology
> 1. Serve to protect this Nation and
> 2. Position the US as a leader in the information technology arena.

The investments were essential when they were not well known and the results were not directly visible. In the past 10 years the results have become more visible as IT has become pervasive. This represents a fundamental paradigm shift that is unprecedented in its impact. But, IT is not a single paradigm shift itself. IT is really a complex collection of paradigm shifts. While most of existing IT that is in pervasive use has become a commodity, this is the result of decades of investment by a complex public private sector partnership. The result of this investment has served to protect the Nation and has positioned the US as the leader in Information Technology. The fact is that IT enabled the US to win the Cold War as a critical part of the National System though research, design, development, deployment, and management of those systems. At the same time, the commercial applications served to strengthen the economy and demonstrate US leadership in Information Technology.

The effect has been profound. IT represents the most dynamic of all technologies. The past 50 years, since the invention of the transistor and the integrated circuit, has produced extraordinary advances through public private partnerships. These advances emerged from a complex science technology policy economy dynamic that we are only beginning to understand. While much of it started in the US, it has become a global phenomenon.

The entire field has been through multiple revolutions and extraordinary advances have been made across a wide range of science and technology.

But, we are only really at the beginnings of a much longer process.

As the limits of what has become conventional commercial integrated circuit technology are reached, new technologies with revolutionary implications are emerging at the atomic scale in the form of nano-technologies. The new nano-devices can be integrated into new kinds of things including new kinds of nano-scale integrated circuits with extraordinary properties. The properties go beyond computing to include new kinds of storage, sensors, effectors, and new ways to interact with the physical world including biological.

The advances in devices will enable new kinds of modules that will be the units of replication in new kinds of systems. The challenges in creating the new kinds of systems and their implications will be extraordinary as will be their capabilities. The advances are expected to be as revolutionary relative to the existing Internet as the Internet was to the first computer 50 years ago. And, at the nano-scale we are able to operate at the intersection of fundamentally new kinds of interdisciplinary interactions.

While the IT systems of today have become progressively more pervasive, the systems are awkward and visible, difficult to use, not well integrated into the environment and society, not suitable for critical applications, and not capable of trusted information sharing -- not to mention the continuing geometric increase in vulnerabilities and incidents that occur every day on the Internet.

Therefore, it should be obvious that there is even more advanced research to be done and it is more critical then ever – particularly in the post 9.11 era. While there is a growing global market and industry, it tends to focus on the near term even with their own research and development programs.

The US Government has a Constitutional responsibility and obligation to protect the national interest by providing for the common defense and enable the life, liberty, and happiness of the People. Among all the technologies, information technology is among the most critical and pervasive.

Some examples of the role of IT

- The role of IT in Critical Infrastructure
- The role of IT in the National and Global economy
- The role of IT in Science and Technology
- The role of IT in National Defense
- The role of IT in Homeland Security
- The role of IT in Trusted Information Sharing
- The role of IT in Protecting Individual Privacy
- The role of IT in the Future of Civilization

Some insight in the advanced research challenges can be found by exploring the fundamental trends, limits, and alterative futures in the context of a 5 layer model that covers everything from the devices to the applications:

Devices
The fundamental devices and their integration into components that provide the foundation for modules

Modules
The scalable components and systems of components that provide the underlying hardware, embedded software, and system software that serve as the foundation for scalable systems.

Virtualizations
The virtual system modules that are configurable into extensible scaling systems that serve as the foundation for customizable system structure.

Structures
The system structures that serve as the foundation for composing dynamic extensible scalable applications.

Applications
The applications of a system to the environment outside the system including users, the real world, and other systems.

Alternative Futures

There are four major alterative futures that I call Red, Orange, Yellow, and Green in the context of an idealistic vision of the future, Blue.

Red is essentially pre-Internet technology.

This is legacy IT that was developed and deployed before the Internet revolution. This is the IT of the Cold War era.
The old world of IT called legacy systems that should be donated to the Computer History Museum.

Orange is essentially an attempt to extend the Red to cope with the emerging Internet revolution.

An attempt to extend the life of legacy systems trying to connect IT to the Internet.

Yellow is essentially an attempt to apply commercial Internet technology to the challenge of the Internet.

The Internet and its evolution.

Green is essentially the development of fundamentally more advanced technology then commercial Internet technology for the purpose of achieving Strategic Advantage. Such systems also have fundamentally more advanced cyber security then the existing commercial Internet.

The revolution beyond the Internet representing a collection of fundamental advances across the 5 system layers providing federated adaptive enterprises capable of trusted information sharing for critical and pervasive applications.

Blue is an idealistic vision of the future that is called Intrinsic Trust and that is the essential distinguishing characteristic of the fundamental advance needed in future of Information Technology systems.

In this framework, the existing Internet is Yellow as generally applied throughout most of the modern global community. The US Government systems span the Red, Orange, Yellow, range with selected special features to protect them through a combination of physical separation and advanced cyber security. The existing US Government systems are obviously not Green because it does not exist—yet.

The most challenging problems provide the insight needed to establish the most effective advanced research agendas. The ideal of Blue is essential to guide the advanced research agenda for Green.

The insights needed to create effective advanced research agendas emerge from interdisciplinary interaction among science, business, homeland security, and national defense. The interactions are more critical because of the need for the public and private sector systems to interoperate over a wide range of modes that are all dependent on critical and pervasive interoperable information systems capable of trusted information sharing while protecting privacy.

Therefore,

I believe it is essential that the US Government continue to

invest in advanced research in Information Technologies

focused on protecting this Nation, and

position the US as the leader in Information Technology.

The future leadership of the United States depends on advanced science and technology at a time when Information Technology has become critical and pervasive and is itself going through its own re-invention.

Mr. PUTNAM. We will begin with the questions; and I will begin with you, Dr. Squires.

Given that there will always be a finite amount of money available for Federal research and development, are we prioritizing the use of that funding in the most efficient manner?

Dr. SQUIRES. I don't think efficiency is the way to think of it. If you try to optimize the systems so that there is minimum duplication and maximum efficiency, you are very likely to lose the most interesting and innovative system that the world will see. It is all right for the innovation process of the national R&D agenda to be slightly loose and informal. You always need the flexibility for a bright young mind to come up with a new idea without having to go through a long-drawn-out proposal process. Start soon.

The other thing is I think that there's a general structure that I've found that is useful in trying to set research agendas and that is to focus on the fundamental technology trends, understand their fundamental limits, and when you begin to identify a limit, look as hard as you can for effective alternatives. If you take a look at every major advance in information technology, you discover that it is a result of that process.

Mr. PUTNAM. As someone who transcends the public and private sector, is there adequate collaboration between the two?

Dr. SQUIRES. There is a lot of collaboration, but I don't think it's adequate, and I will give you the main barriers. I think that the mechanisms in place for setting agendas and for holding full and open competitions and for negotiating the actual agreements takes too long. It is way too burdensome and actually tends to be a disincentive to people and individuals and universities and companies, my own personal opinion, working in that way.

The phrase that I sometimes use in discussions like this, and I say our adversaries do not have the advantage of our procurement system.

Mr. PUTNAM. Dr. Fossum, do small startups and smaller universities with less well-established research relationships with the Federal Government, startup companies that have a great idea born in a garage, do they receive adequate attention, adequate opportunity to compete with the big, well-established companies that are out there?

Dr. FOSSUM. In theory, yes. Is it a level playing field on paper? Yes. But there's an awful lot of networking, connections, and experience that go into knowing how you actually successfully get a grant proposal through and how you actually go through a procurement and become a participating competitor, so to speak. I think it is a very large threshold for some to get across.

Actually, when you mention universities, there are over 1,800 4-year accredited colleges and universities and professional schools in this country, and only 80 of them receive 71 percent of the Federal funds for R&D. It shows you the concentration of these funds. It is an enormously concentrated world.

Mr. PUTNAM. Dr. Lazowska, is that a concern, the concentration?

Dr. LAZOWSKA. I think equity and distribution and participation is always a concern. But I think the numbers that were just cited need to be interpreted in light of the fact that many of those 1,800 4-year schools do not purport to have a research program. They are purely educational institutions. So we need to make sure that research funds are equitably distributed to those best positioned to carry out the work. And I think Federal agencies do a reasonable job of that. There are also programs that ensure adequate research funding to States that don't have perhaps a full complement of research institutions.

In terms of prioritization, I would just remark that the PITAC committee in 1999 did a fairly thorough analysis and concluded that the Federal investment in IT R&D, compared to other fields, was dangerously inadequate; and they proposed a ramp-up which has not been nearly met. In fact, as Mr. Clay pointed out, the NITRD funding will actually decrease in the proposed budget. So I think many Members of Congress are coming to the conclusion that the Federal R&D portfolio has become unbalanced. Perhaps that doesn't mean we're investing too much in some areas, but it means we're investing too little in others, and you have identified a number of them today.

Mr. PUTNAM. The imbalance being toward the biological science and CDC, health?

Dr. LAZOWSKA. I would say the imbalance is against information technology. If you look at the role IT plays in national security, in advancing the sciences, in driving our economy, we are investing a relatively tiny amount of Federal money in creating the next generation of advances.

Mr. PUTNAM. Dr. Scherlis, do you have anything would you like to add going to this?

Dr. SCHERLIS. I guess I would.

Your first question to Dr. Squires was concerning prioritization within the R&D portfolio, and I think it's worth clarifying a little bit from the outside my understanding of the NITRD process. It is not a top-down process. It involves a combination of vision and mission. The mission agencies who are collaborators within the NITRD process identify their needs and priorities on an agency mission basis. This is combined with input from the research community, who drive the process on the basis of their invention and imagination and desire to explore. It's the juxtaposition of those two things that really creates the innovative magic that several of my colleagues have spoken of earlier in this hearing.

Mr. PUTNAM. Is the allocation of R&D skewed too heavily to defense and defense-related research? Dr. Scherlis?

Dr. SCHERLIS. Actually, it's interesting, the history of IT in this country has a history that's really largely been driven by a combination of Defense and the National Science Foundation. It is a combination of those two organizations. And it has been interesting growing up in IT to see that IT researchers and scholars have adopted defense metaphors. They speak in terms of survivability and command and control. DOD has had a profound influence; and, as a consequence of that, the mission needs of defense have been very well met through the research community.

This has worked well because of the very farsighted, broad attitude of the DOD basic science investors, those who invest 6–1 and 6–2 funds in the R&D world. It's the supply chain management story. They work throughout the supply chain, not just with the prime contractors and the systems integrators but with the vendors and the innovators and the inventors who feed that supply chain. They do it in a way that provides value well beyond the defense mission. There is a leverage in that story. The leverage is that DOD is able to buy off-the-shelf components and systems that they can apply directly in their mission. We have pervasive applications, spreadsheets, word processors, operating systems; and these are increasingly incorporated as components into systems. They are pervasive not just in our offices and homes but also in our national infrastructure and critical national security systems. So what has happened is that the pervasive systems have become critical. This is an inevitable and positive outcome. It's the nature of IT that we have come to this point. It makes these problems, in some ways, much more significant and challenging.

Mr. PUTNAM. Dr. Fossum.

Dr. FOSSUM. I think one of the questions that you raise is about what is defense R&D. We don't really know how to divide R&D. R&D doesn't know a home agency or a discipline. It can go across all kinds of areas. Let me give you an example.

I happened to be at the Army 1 day talking to a gentleman there whom I literally asked "What is your major technology challenge?" And he said they needed a "miniature, long-life, anticorrosive fuel cell" to put in every piece of equipment they deployed in the field. And we put in the term RaDiUS—"fuel cell" into RaDiUS and got hits in six or seven different agencies including NIH. We shortly were looking at an actual description of "miniature, long-life, anticorrosive fuel cell" research at NIH for the artificial heart. That is why it is very hard to talk in terms of "health" research versus "defense" research. R&D doesn't know boundaries like that. Discovery doesn't recognize those boundaries.

Mr. PUTNAM. Dr. Squires.

Dr. SQUIRES. One thing I'd like to add to what Dr. Scherlis mentioned is the fact that throughout the history of advanced research in science and technology leading to advanced products there's a pattern that having people able to understand and focused on the hardest problems of the time with the resources and flexibility to solve those problems is what leads to great invention. You don't make great advances by looking at the easy problem. You don't make great advances by doing what everybody else is doing. You make great advances by going beyond what you normally can think of doing and trying to invest the future.

It turns out that because of the nature of the American system, the American economy, the role of defense in the United States and around the world, the defense and national security system, the homeland security system of the country has among the most challenging problems for information technology and science. It's just a fact, and that is a tremendous source of insight and motivation, and the people who make the investments and set up the research agendas normally do it in such a way that the technologies are as much as possible dual use. Because it doesn't do you much good to have an advanced technology if you can't afford it. So it's a very subtle, complicated and important relationship between the public sector, the private sector, the civil agencies in the government, the National Security Agencies, and the government how that works in the community.

Mr. PUTNAM. Clearly, it is an important role for defense to play in research; and it's allowed us to be on the cutting edge. Frankly, it is something to be very proud of. But it's just interesting to think about the breadth of research that occurs in the name of defense, whether it is an MRE in food preservation or it is training a dolphin to go seek out a mine and everything in between that leads us to things like the Internet, things like GPS that are now in every brand-new suburban sold and all of these other things.

Dr. Scherlis.

Dr. SCHERLIS. One of the reasons why it is important to focus on mission R&D is that the needs of Federal agencies often anticipate the market in terms of their demands for capability and quality. In areas where they follow the marketplace they should generally follow the marketplace with respect to acquisition as well. But in IT, the history has always been that many mission agencies, not just the DOD but the Department of Energy, NASA, other agencies, have needs that, frankly, go beyond the needs that are evident in the marketplace at any given moment. When they invest in a dual-use fashion, they get this tremendous impact from the investment because it creates an economic stimulus as well as a response to the agency needs. That actually pays off for the mission agencies. It's an important and sometimes essential payoff for those agencies.

Dr. LAZOWSKA. I'd just add one other fact to this, and that is the track record over many decades is that it takes about 15 years from the invention of an idea to when it's exploited in a billion dollar industry. OK? So what that means in some sense there is no such thing as just-in-time research if you are a commercial enterprise. Companies cannot afford to be investing in innovation that is not going to pay off for 10 or 15 years. I'm a shareholder, and you are a shareholder, and that is not the way we make investment decisions.

That speaks to the role of the Federal Government and the Federal agencies because the mission of the Federal agencies require these advanced technologies. They support the innovation which in many times makes its way into the private sector, but it is many years later, and that is why the Federal Government has such an important role.

Dr. SCHERLIS. Forgive me for prolonging the discussion, but I have to add one more point. Mission agencies enjoy another advantage, which is that they can afford to be farsighted. They don't have to make a quarter-by-quarter ROI case for every research investment they make. They can anticipate their needs through a planning process, and they can respond to these needs through their R&D mechanisms. And that, combined with the fact that they don't need to explicitly appropriate the value that they create through that R&D investment, creates a tremendous synergy that allows them to be much more aggressive and to get more leverage for their funding.

If you look at the level of DARPA funding over these many years as compared with R&D funding in any one of the major IT companies, it is relatively low. But DOD gets enormous impact for that investment because they are investing in a leveraged way. They are applying this supply chain management trick of investing where they see they can get the maximum impact for that investment in the long run.

Mr. PUTNAM. Are we still the cutting-edge Nation for basic research?

Dr. LAZOWSKA. There have been many claims in recent years that we are losing that edge, and the concern of PITAC has been that we are losing that edge in information technology because the level of investment has not kept pace with the opportunities of the field and the increasing demands on the field. So I think there is reason for concern, but it's very difficult to measure.

For example, there was something in the papers a few months ago talking about the number of physics publications in Europe and Japan versus North America. I think we have to expect that the rest of the world is going to start contributing at a level comparable to what we're contributing. I urge to you think about the areas in which this Nation cannot afford not to be the world leader, and I would assert that information technology is one of those areas. We cannot afford not to be the world leader in information technology, because it drives everything else. It drives every other field of science, every other field of engineering. It drives the economy. It drives defense and security. We can't afford to fail to be the world leader in this one field.

Mr. PUTNAM. Give me another field that we can't afford not to be the world leader in.

Dr. LAZOWSKA. You will have to convene another panel, sorry.

Mr. PUTNAM. If I had CDC, would they say we couldn't afford not to be the world leader in gnomics and biotechnology and——

Dr. LAZOWSKA. I firmly believe that 30 years ago I stumbled into the field that underpins all other fields, OK? So I firmly believe that this field is No. 1 in terms of the leverage that it offers.

Dr. Scherlis is talking about leverage, and this is a field that offers enormous leverage in all other fields. You can't do advances in the biomedical sciences these days or in health care delivery without advances in information technology. You know, astronomy is digital imaging and data mining of the images.

Mr. PUTNAM. You are not supposed to say data mining anymore. Ask these DARPA guys.

Dr. Squires.

Dr. SQUIRES. Don't ask me that question.

I think next on my list is, obviously, nano-technology, because of its fundamental implications. But simply investing in nano-technology without the context of its transforming effect on all of information technology and all other science would be a mistake. As I said in my testimony, as extraordinary as the advances have been in the last 50 years, they were enabled by a relatively small number of fundamental device inventions and a massive number of systems structures and a massive number of software technologies; and what we have today, as wonderful as it is from my sort of perspective of the future, is a really very small scale prototype of what it could really be 50 years from now.

Mr. PUTNAM. In the green world or the blue world?

Dr. SQUIRES. Yes, the blue curve. My blue sky vision says we need to be in this world of the green, and we need to get off the yellow brick road. The rest of the world has seen what the U.S.

process of invention and innovation has done. We need to get on the new curve. Otherwise, what is the risk of having some other part of the global community decide to get on the green curve?

Mr. PUTNAM. It is a tremendous risk. But I mean, in 1985, we were all being told to go on to speak Japanese and that the Japanese were buying up the whole Nation and they owned the motion picture studios. And because they owned the motion picture studios, it was the end of America as we knew it.

We go through these periods, and I am not in any way arguing with a distinguished group like yourself that it is not important for us to continue to be the world leader in IT. I am just trying to play devil's advocate here.

Dr. SCHERLIS. I made a point in my testimony about the necessity of IT innovation and leadership as compared with other engineering disciplines. The issue is where, globally, is the focus of innovation and how important is it to have that focus of innovation. The reason that IT is interesting, as compared with other building materials—we can think of software as a kind of building material—is that other building materials can only scale up so much. You can only build a building that is so tall before various laws of physics start to impede our ability to build it taller. With software, we don't see any such natural limits.

The Windows operating system I believe is now 50 million lines of code. Who contemplated 50 million lines of code even 20 years ago? Impossible. And there is no reason why we can't go from 50 million to 50 billion and to create systems of tremendous cognitive power, for example, that can translate languages or be autonomous robots or cars that can drive themselves. There are many such visions.

My point is that these are no physical limits in the world of IT that impede us from addressing those aggressive visions directly. And in fact, as Steve Squires just said, let's focus on the hardest problems. What's interesting, in fact, is that partly is what DARPA is doing right now. They are focusing on the hard problems of cognition and how to build smart systems that can learn. That is a very good topic.

But we also need to be focusing on the bread and butter issues of how can we make promises about the systems that we build, how can we make dependable systems and secure systems? These are hard problems, and these are the impediments to scaling up.

Mr. PUTNAM. You said earlier there are absolutely no bounds for innovation to IT.

Dr. SCHERLIS. No physical bounds. There are only intellectual bounds.

Mr. PUTNAM. Does anyone disagree with that? Anyone wish to add to that?

So how do you jump off the yellow brick road, Dr. Squires? Is it, as Dr. Freeman said, education, turning out more engineering and computer scientists and graduate degrees that are home grown? What is the trick to maintaining our leadership role in IT?

Dr. SQUIRES. I think it is important to have an effective framework for thinking about these future worlds that go beyond just the nano-devices and beyond just the applications so that you are actually able to effectively organize the different disciplines to work with each other.

My favorite one, which I wrote a little bit about in the testimony, has five major layers from the bottom up: devices, modules, structures, virtualizations, and applications. Each of these is a major discipline in itself which works with all the other disciplines; and the most important thing is to look in, pick your favorite framework—that's my favorite one—and try to understand what the fundamental trends and limits are.

So, for example, in devices, the fundamental trends and limits at the device level, these are actually running out of the ability to build integrated circuit technology with increasing performance and cost-effectiveness as we do it today. It costs billions of dollars to build the next VLSI product. You can save hundreds—many orders of magnitude when we transition to nano-scale self-organizing technologies. That may be 5 years before we get the first devices, but we certainly need the first new devices in that area.

Assuming that you can do that, you have to think what are the new modules, units of replication, which, if we could have that new manufacturing capability, would we choose to have? If you had that, then what would be the new virtualizations, what would be the new system structures, and what would be the new applications?

The interesting thing is what has happened is the transistor was invented and all the kinds of wonderful things happened after that. What we learned is that having multiple layers of the system work in parallel is way better than having them work in series. So if you have the basic and applied sciences working across the full range, from devices to applications through those intermediate levels, working on always the most important problems so the feedback would be not just produce the papers, produce real stuff, real system prototypes, real prototype products, real products which early adopters can use sooner rather than later and get the feedback to the system, you have the potential to bring the future into reality sooner rather than later.

So I view this whole investment strategy as a kind of time machine. What you are actually doing with Federal R&D investment is getting an earlier view of the future than anybody else can, Getting it in the minds of the best scientists and engineers and businesspeople in the country and making it available to the United States and all the people of earth sooner rather than later. And doing one more thing: Through the American system, providing the incentives so it is used for good, as opposed to used for something else. So I can't imagine life without being on the frontier.

Mr. PUTNAM. Dr. Lazowska.

Dr. LAZOWSKA. I think the simple answer to your question is "support IT R&D by Federal agencies at the level that the President's Information Technology Advisory Committee recommended in 1999." What you see from this graph that I showed you earlier is that we're increasing Federal R&D overall. What you see from this graph is that Federal R&D in information technology has flat-lined. It has fallen far below the PITAC recommendation, and it has flat-lined, and the good news is these are very small numbers.

We are talking about only hundreds of millions of dollars a year. That is not an inconsequential amount of money, but on the scale in which the Federal Government operates or the Federal R&D operates, it is inconsequential.

Our government has failed to prioritize this field. Simple as that. What you understand very well is the role that this field plays in our economy and in all other fields.

Mr. PUTNAM. Dr. Fossum, anything to add?

Dr. FOSSUM. Just sort of a random thought that came by. I look back at the history of some of the things that the U.S. Government has done in R&D over the last 50 or 60 years, and what it took to do it. We have a history of when something is a true priority nationally of essentially having a major program or an incubator on it. Go back and start with the Manhattan project and look at the form they took. If IT R&D is very important to this Nation, which I think we all agree it is, maybe we need to look at some models that we used before, rather than rely on the current funding streams of the current agencies. Maybe we need to rethink how better to pull the parts together.

Mr. PUTNAM. You raised a good point, and I have forgotten most of what I learned in junior high and high school science. All of you operate, as Dr. Squires put it, on the frontier. There is a great deal of apprehension and concern about our inability to attract young people into the math, science, and engineering fields; and yet as far back as the Manhattan project we were pretty well co-opting the world's talent anyway. We were offering them freedom, a safe place to live, work, raise their family, and have a future and apply their brilliance to productive, hopefully peaceful things, although we could certainly have a whole other hearing on that.

But how great a crisis is that? How big a threat is that? And how much attention should we be paying to it? Is it a natural demographic occurrence that China will produce an annual increase of more engineering degrees than the sum of all of our schools? Or is it truly a crisis in American higher education? We'll start with Professor Lazowska.

Dr. LAZOWSKA. One thing I would say we should make sure that our immigration policies are in line with the sorts of goals you have articulated. That is, do we allow the best students from around the world to come to the United States and get training? And do we allow them to remain in the United States once trained? If they return to their home countries, do we use them as agents of international cooperation or perhaps are we closing our borders and preventing these smartest minds from around the world from coming to us and learning?

Mr. PUTNAM. Anyone else before we lose power?

Dr. SCHERLIS. I just want to say that it is a serious issue and that many universities are struggling to develop strategies to attract the very best students into these fields. In our programs, we continue to get the very best students, but, in many other programs, there are challenges. We find, for example, that applications from overseas have gone down considerably because of this friction at the border.

So, yes, this is definitely an issue. The most fundamental element of our supply chain is the people who populate it, and I think we need to take it up explicitly.

Mr. PUTNAM. Dr. Squires, you and Dr. Scherlis, y'all were both recruited very early in your careers into government service and research?

Dr. SQUIRES. I was, essentially as a freshman undergraduate.

Dr. SCHERLIS. I was on the faculty at Carnegie Mellon when I was recruited.

Dr. SQUIRES. But I recruited him.

Dr. SCHERLIS. I thought it would be an easy desk job for a couple of years, and I could write papers in my spare time. But seriously, it was the most exciting and demanding thing I ever did. I stayed much longer than the usual tenure, and I continue to strongly recommend service. You talked about this with the earlier panel. We all feel the sense of possibility and opportunity to really do something significant for the Nation. There are many good reasons to take this up.

Mr. PUTNAM. So high turnover is a fact of life in these fields? I mean, you said you stayed longer than normal.

Dr. SCHERLIS. The IPA law, Interagency Personnel Act, allows a maximum stay of 4 years for somebody rotating in from a university or a State or local government. In fact, what I did was to stay on the IPA for 4 years; and then I rejoined as a senior executive government employee.

Typically, rotators from universities to NSF or DARPA or other agencies will stay between 2 and 4 years and then return so that they don't lose continuity in their home institutions.

Dr. LAZOWSKA. I think it helps to be part of the research community, to work with the research community. So both NSF and DARPA have had great success with recruiting top members of the research community into being office directors and program managers for a period of time and then sending them back.

Mr. PUTNAM. Dr. Fossum, and then we're going to wrap it up.

Dr. FOSSUM. DARPA and NSF are stellar examples of this. That's not the case as I can see with a place like NASA where IT is very critical and where they have a large budget for R&D, but they are not real good at R&D partnering because they tend to deal more with contract-driven R&D, then grant-driven R&D. And the world you are talking about is where universities can coordinate with the Federal Government to cooperate and leverage the talent at universities is a "grant driven" world for the most part. In that world, you are talking about the "science program" at Department of Energy. You are talking about NSF. You are talking about NIH.

So just like we have a problem with the substantive border—perhaps we also need to take a look at how the R&D dollars move, and also, where the laboratories in the Federal Government will open their doors to various and sundry people. DARPA is world famous for this. World class. Maybe we need to use them as an example to teach a few other parts of the Federal Government how they might do that, too.

Mr. PUTNAM. You pushed a button.

Dr. Scherlis.

Dr. SCHERLIS. Yes. I just want to present an alternative perspective about collaboration with NASA.

Dr. FOSSUM. Oh, they do some. No doubt.

Dr. SCHERLIS. I lead a project with NASA that involves Carnegie Mellon and five other universities, MIT, University of Southern California, University of Washington, University of Wisconsin, and University of Maryland. And that project is structured as a cooperative agreement which allows us to collaborate directly with NASA mission managers, mission engineers, and intramural researchers. We find that to be a very successful structure for collaboration. And I also want to note that at DARPA, at least to my knowledge, most of the relationships that they build with researchers at universities are framed as contracts or cooperative agreements. The nature of the vehicle through which the collaboration is undertaken, is I think, less important than the culture and horizon of the sponsoring organization.

Mr. PUTNAM. Dr. Fossum's total agreement is noted for the record.

Dr. FOSSUM. Yes. I just wanted to make one point. And the only point I was trying to make is that if you look at the proportion of, for instance, cooperative agreements, which are the vehicle that should be used, in some agencies, they haven't learned how to use them quite to the extent they might want to. NASA is an example of such an agency.

Mr. PUTNAM. One of the things that I talk about in my Rotary Club speeches is when you look at the success of the American military and exponentially ahead of our competitors in a variety of fields, it's really because of the investments that the American people have made with their hard-earned tax dollars for decades that yields tremendous military prowess that then translates into the commercial sector. And, you know, people don't normally realize it until they hear it that they are shareholders in the success that ultimately not only raises our living standards but saves lives.

Our society is not particularly good at recognizing and rewarding smart people, and yet it's the brilliant people in laboratories, in universities and in the Federal Government that just do tremendous things to make our lives easier, better, healthier, more productive and worthwhile. And one of the side effects, the positive side effects among many in the dot-com boom was that it kind of made it OK to be smart again. Working hard and being smart and attentive and paying attention to the sciences and math and computers, would get you a billion dollars or more in the case of some of them. And, hopefully we can find some way to tap into that generation of young people who have grown up seeing that and encourage them to continue to pursue their studies and academics and make it OK to be smart again.

It's been a pleasure having such a smart panel showing their wisdom with us.

Before we adjourn, I want to just convey to you the subcommittee's deepest appreciation for your accommodating us and dealing with the voting schedule. Your testimony is very important to our better understanding of Federal R&D, and we appreciate you.

In the event that there may be additional questions that we do not have time for today, the record shall remain open for 2 weeks for submitted questions and answers.

Thank you all very much. The subcommittee is adjourned.

[Whereupon, at 4:38 p.m., the subcommittee was adjourned.]

[Additional information submitted for the hearing record follows:]

TESTIMONY OF KATHLEEN KINGSCOTT
Director, Governmental Programs
Science, Technology and Innovation Policy
IBM Corporation
Before the
U.S. House of Representatives
Government Reform Committee
Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census
June 9, 2004

Good morning, Mr. Chairman and members of the Subcommittee and thank you for inviting me to be with you today. My name is Kathleen Kingscott. I am Director, Governmental Programs for Science, Technology and Innovation Policy for the IBM Corporation. Thank you very much for the opportunity to offer IBM's views on the federal investment in information technology research and development. Given the fundamental role of information technology in underpinning American economic growth and national security, I believe that these issues are more important now than ever before.

I would like to thank Chairman Putnam for his support on the important issue of information technology research. Our nation needs both balanced progress on all aspects of computing and an adequate interagency planning process to support continued US leadership. Today I will comment on the current federal portfolio, several significant changes in our economy and the information technology industry and how these changes affect an IT research investment strategy.

As a basis for understanding IBM's perspective on the federal research program, I would like to provide the Subcommittee insight on IBM's own research activities. IBM has a long history of substantial investment in research and development. In 2003, we invested $5,077 billion in research, development and engineering. In the past five years, we have invested $26 billion in R&D. IBM has eleven years of patent leadership in the United States, with more than 25,000 patents – nearly triple the total of any U.S. IT competitor. Our 3000 researchers are located in eight research labs around the world. Five of our researchers have been recognized as Nobel Laureates. We have been honored to receive both the National Medal of Science and the National Medal of Technology.

IBM participates in a number of the federal IT research programs included in the Networking and Information Technology Research and Development Program (NITRD). For example, our Research Division partners with DARPA in its High Productivity Computing Systems Program, PERCS, (Productive, Easy-to-use, Reliable Computing Systems.) PERCS is a long-term study of high-end system performance efficiency, scalability, robustness, and ease-of-use. The overall program emphasizes groundbreaking, high-risk, high-reward research with a close eye on commercialization prospects. We were recently named as a partner with DOE in its leadership-class computing award through our relationship with Argonne National Laboratory. Since 1996, we have partnered with the DOE National Nuclear Security Administration in the development of high-end computing for the management of our nation's nuclear stockpile. At the other end of the technology spectrum, in semiconductors, we provide funding to the Semiconductor Research Corporation for its joint university-based efforts with the Department of Defense and the National Science Foundation.

These are examples of the very important and classical information technology research and development programs in the federal portfolio. Programs like these create the fundamental understandings of information technology from semiconductors to supercomputers. This portfolio has served the U.S. well and has helped our nation earn global leadership in information technology.

However, the world is changing dramatically and our federal research investments will need to change as well. Some of the changes we are observing center the potential of technology for integration of people, processes and information, not just automation. Success in IT increasingly will depend on adoption of open computing, specifically open standards and open source methodologies. We also see that invention is not the only source of innovation. Innovation occurs when inventions are actually put to use.

Technological, economic and social forces are making PCs, the Internet, wireless and other technologies ubiquitous. Even supercomputers have become so much less expensive and so much more powerful that they can now be applied in areas where they were never before affordable.

For example, EPA will use a powerful new supercomputer to assess the risks to human health and the environment posed by exposure to chemical and air pollution and other agents. And life sciences clearly represent an entirely new set of challenges for supercomputing with the potential to revolutionize health care in this country and the rest of the world. Computing is moving beyond its classic challenges and applications.

At IBM we have described an emerging state of business called On Demand. This is fundamentally what happens when we become an information-based society with everything and everyone connected using open standards, and with computing power, storage and networking essentially unlimited.

Today's applications and huge amounts of data are making high-end computing a standard requirement. High-end computing enables problem analysis which was impossible to perform previously. We see this already in areas as diverse as fraud detection and customer relationship management. New business models are allowing high-end computing to be delivered to customers over the Internet, freeing them from the fixed costs and management responsibility of owning a supercomputer.

Omnipresent communications keep the world online and in touch 24-hours a day. Open standards are integrating the billions of devices attached to the Web and enabling it to amass and transmit huge volumes of information. The availability of information on such a scale and time frame leads to decisions, changes and the need for response. The pace of change will only accelerate with the constant proliferation and integration of technology.

Another aspect of our changing information technology world is the growth of IT services and software. Users -- companies, governments, and universities -- realize that hardware alone is not enough for success. They now want to pull together all of the systems they already have and integrate them securely with their core business activities – horizontally across not just their whole company but their entire value chain, from customers or constituents to suppliers. They want to become on demand enterprises.

This is causing a significant shift in the information technology industry. Let me use my own company as an example. For 2003, IBM's revenue stream was composed of 64 percent services and software and 32 percent hardware. This is a remarkable reversal for IBM, given our nearly 100-year history. And the rest of the IT industry is in hot pursuit. The shift in the nature of the IT industry mirrors the shift in the US national economy, which now generates 17 percent of GDP from manufacturing and over 70 percent in services.

The modern computing structure includes services, software, networks and grids. It is essentially ubiquitous in our society and this structure enables traditional computing uses plus real-time information analysis.

The United States must ensure that it will have the information technology assets needed to prosper in this constantly changing, on demand environment. Clearly, that requires aggressive research, performed at a level commensurate with the environment of change that we face. As these changes occur, our research portfolios should change to reflect the opportunities these trends create. A forward-leaning portfolio must focus on research for an on demand world.

An IT Research Portfolio for National Leadership

The United States should recognize and leverage its areas of strength to extend its leadership in a rapidly changing world. Several critical focus areas include:

High-end computing – High-end computing has become the third node of science and engineering. Leadership is based on many factors. They include: sustainability, meeting application needs, developing algorithms, enhancing skills and creating test beds and partnerships between government, industry and universities. By these measures, there is no question that the U.S. continues to lead the world in high-performance computing. Major programs, as previously mentioned, such as DARPA's PERCS program and DOE's ASC and ASCR programs play critical roles in creating the skills, technologies (both hardware and software), application development, training methodologies, research, development, engineering, and manufacturing capabilities that will advance high-performance computing. Agencies must focus on all of these components to ensure success.

Price/performance plays a major role in making supercomputing a prime tool for competitive advantage. Scalable systems based on common components make it possible to reach a large user base, help reduce the cost and risk of development, and support a wide range of applications. To be clear, widespread use throughout society, a characteristic of national leadership, is closely related to price. Government investment in unique systems to meet specialized needs is not sustainable. We believe that government agencies must work with the research communities and the private sector to define supercomputing applications and technology solutions to achieve sustained performance improvements. The U.S. should increase its application capability in a cost-effective manner.

The road map developed to meet these needs must be based on commercially viable technologies that can be optimized for application-specific needs. Government, as a partner with industry, should specify its critical needs and work with industry to meet them. These cooperative partnerships are critical.

Semiconductors – Semiconductors are at the heart of electronics and systems performance. They are the enabling technology for all computers and communications systems. For forty years, the semiconductor has been rapidly advancing, with each product generation providing smaller dimensions and faster performance, reducing cost per function by more than a million-fold. Today, for the first time in history, this once reliable progression faces a number of technical challenges to continuing on this path for which there are no known solutions. DOD has been partnering with the semiconductor industry in basic research to address these problems through a joint program called the Focus Center Research Program - (GICUR-Program Element Number 0601111D8Z). Industry has provided more than $61 million over the past five years; DOD's Basic Research Program has funded over $28 million in the same period.

Thirty universities nationwide are engaged in research to advance our current chip making technology and find a replacement for the current technology before it reaches its physical limits in the next 10-15 years. All funding through the program goes directly to universities. This program will double the number of Ph.D. graduates in electrical engineering and computer science funded by the semiconductor industry over the next decade. Federal funds are leveraged through the matching contributions of semiconductor firms.

The Focus Center Research Program has already produced a variety of technologies that DARPA has selected for additional funding, such as polymorphous computing, silicon-based millimeter wave integration, and mixed analog/digital applications. DARPA has not provided any funding for the FCRP in FY05. This greatly concerns the semiconductor industry.

Nanotechnology - The history of information technology can be viewed as a process of miniaturization -- of continuous invention of ever smaller versions of the devices that process, store, and communicate information. For example, the mechanical systems used to tabulate the U.S. census a century ago were replaced by electromechanical calculators. Vacuum tubes used to build the first stored program computers a half century ago were quickly replaced by the transistor. In an historical eye-blink, the discrete transistor was displaced by the monolithic silicon integrated circuit. Smaller has consistently translated into faster and cheaper, supporting the ongoing explosion of new applications of information technology and the growth of the entire industry.

The rapid pace of technology development is accelerating worldwide. Engineering teams, striving for a competitive edge, are taking greater risks and exploring a bolder range of options. With this furious rate of progress, two established drivers of information technology-- silicon microelectronics and magnetic information storage (hard disk drives) -- are expected to reach fundamental limits of miniaturization within the next fifteen years or less. Yet laboratory demonstrations suggest that new devices for processing, storing, and communicating information can be made even smaller, faster, and cheaper, eventually approaching the scale of individual atoms.

Thus, nanotechnology is the future of information technology. Nanotechnology pools appropriate knowledge from diverse scientific fields in the service of an engineering goal -- making things that are very small and integrating them into complex systems. Without further advances in nanotechnology, improvements in IT speed and cost must slow, and the economic growth of the IT industry must slow, along with its associated productivity gains. If key scientific advances are made and first exploited outside the US, growth will move offshore.

U.S. investment in nanotechnology research is critically important, as it can be used in a variety of disciplines and technical areas. Federal funding for nanotechnology initiatives has reportedly risen 83% since 2001. The increase in funding can be attributed to a sense of competitive urgency on the international scene: in the same period, Japan increased nanotechology funding by 40 percent, and Western Europe by 78 percent. IBM believes that although research fields are converging, divergence and specialization are also occurring in the world market. The United States leads in nanotech synthesis, chemicals, bio/medical applications, and perhaps materials. Japan is aggressively developing nano-scale devices and nanostructures and several European countries are strong in dispersion, coatings and new instrumentation. The U.S. must invest in this important technology area. IBM has long supported the National Nanotechnology Initiative.

Software – Software continues to be one of the areas of greatest need for the U.S. IT research portfolio. The President's Information Technology Advisory Committee (PITAC) detailed this quite clearly in its report, Information Technology Research: Investing in Our Future, February 1999. Five years later, the situation remains very similar. The demand for the next generation of complex and innovative software far exceeds the ability of our nation to produce it. A number of factors contribute to this situation: the accelerated demand for software, the increased complexity of systems, and the labor-intensive nature of development. Further, as organizations extend their online relationships in new directions, middleware software becomes even more important. Middleware enables clients to integrate systems, processes and applications across an enterprise through the use of open standards. There is strong demand for greater understanding of middleware in particular and software in general.

The Nation needs to make fundamental software research an absolute priority. We continue to depend on very fragile software, as evidenced by the frequent presence of "worms" and "viruses" which disable millions of users all too regularly. The technologies to build reliable and secure software are inadequate. There continues to be insufficient automation in the construction of software. Yet the activities of ordinary citizens are based on software, from the first weather forecast of the day to their daily cell phone calls to their bank statements to the on-line routing advice they receive regarding the commute home. We believe the United States is not investing sufficiently in fundamental software research.

Research Considerations for an On-Demand World

With the ubiquity of information technology, the changing nature of innovation and the importance of research as a backdrop, several important issues stand out.

The Role of Collaboration and Partnerships in Contemporary Innovation – We live in an era of unprecedented innovation. One of the most striking features of contemporary innovation is that hardly any organization can innovate alone. Most innovations involve a multitude of organizations. This is especially the case for the most knowledge-intensive, complex technologies such as IT. Further, with new communication technologies and a deeper understanding of how innovation can be managed across boundaries (interpersonal, interdepartmental, inter-organizational, and international), it is now desirable to innovate collaboratively. The state-of-the-art in managing innovation is the creation of collaborative networks capable of spreading the risks of failure and enriching the sources of knowledge for innovation.

These collaborative arrangements can range from simple partnerships to virtual organizational networks, defined as clusters of organizations which are bound by common objectives, broadly compatible technology platforms, and organizing principles such as language, dispute resolution processes, and information sharing protocols. Collaboration and partnerships are essential to innovation today.

Federal policy regarding IT partnerships and collaboration has been erratic. Public/private research partnerships, such as described earlier, are flourishing. However, IT development partnerships, such as those in the Department of Commerce, are being reduced. This approach ignores several important roles for the federal government as it strives to maintain national IT leadership.

In today's highly competitive global economy, success depends on speed. It is not sufficient for a country or a company to have the best technology or the best research. Success depends on the bringing new solutions to the market quickly. Collaborations and partnerships which create speed to market are recognized as "best practice." Collaborations can connect customers, universities and the government.

Government has a critical role in these partnerships. Its linkage programs provide a strong conduit into the marketplace. They form a bridge for the technology developed in our private labs, national labs and universities to move from the lab to the marketplace. It is not sufficient today to have an exploratory research program in isolation. Many of the most valuable programs today are being connected across disciplines to create greater economic value.

Another important aspect of the government's role in partnerships revolves around its performance as a reliable, steady partner. Uncertainty is the worst partner. The threat of premature termination of agreements dampens willingness to participate in government programs. Companies make significant commitments and investments based on the government's participation. Early termination of these agreements, such as is now occurring in the Focus Center Research Program, creates great problems for industry partners and reluctance to participate in the future.

Research in IT Services - Services are the predominant feature of today's economy. The non-goods-producing sector accounted for 78 percent of economic growth between 1992 and 2000, an 86 percent share of GDP in 2002, and 88 percent of the workforce in 2002. Services are running a $47.3 billion trade surplus, as compared to manufacturing, which ran a $470.3 billion deficit in 2002.

Nearly all of the post-1995 productivity growth increase can be explained by the performance of just six economic sectors: retail, wholesale, securities, telecom, semiconductors, and computer manufacturing, four of which are classified as services (Solow, McKinsey Global Institute 2001).

The structural transition to the service economy has been going on for years, yet our understanding of innovation in this sector, how services support and interact with manufacturing, and of how IT supports services is lagging.

In this new frontier of computing and information services, neither technology nor business alone can yield breakthrough innovation for growth. A new scientific discipline is being established and federal research investment and collaboration could accelerate learning in this area significantly.

This new area of IT research in human systems is being opened to examine the social, organizational and behavioral sciences. Leading universities are beginning to work with IBM to better understand the social and technical issues involved in collaborating across global enterprises. In fact, UC Berkeley is considering implementing a Services Science course in conjunction with IBM Research -- much in the way the first Computer Science department was initiated at Columbia University.

A wide community is beginning to discuss the technical and social effects of new developments in global connectivity, automation, technology integration and Web services.

We would welcome federal investment in university research in this area.

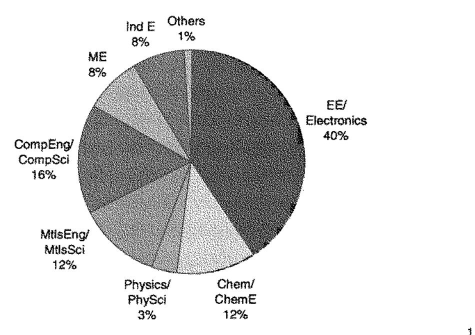
The Importance of A Balanced Research Portfolio –

The science community is loudly debating funding in the physical sciences. I would like to lay out several facts, then draw some conclusions about research funding and the future of IT.

Nanotechnology is at the heart of the future of information technology. IBM's Research Division is a leader in this science area among all research performers, industry, university and national labs. The skill composition of our personnel doing nanotechnology research illuminates IT scientific discipline requirements today and for the future. 95% of our researchers have degrees in physical sciences, including physics, chemistry, computer science, electrical engineering, materials science, math and other technical engineering areas.

It is also useful to examine the distribution of disciplines of the students funded by the Semiconductor Research Corporation (SRC). The SRC is a consortium of North American companies which funds graduate students in American universities who perform semiconductor research. These students both solve technical problems and are the seedbed of a workforce skilled in semiconductor knowledge. As in IBM, these people are creating the future of information technology. Their disciplines of study are in the physical sciences (see below).

SRC Students by Discipline: 2003 Graduates



Federal investment in the life sciences, through NIH, has increased approximately 40% in the last four years. With this in mind, we examined the skill composition of the people who bring together information technology, biology and chemistry in IBM's vibrant, $1 billion life sciences business. This business has grown from two people to over 1000 since 2001. Their skills are also heavily oriented toward the physical sciences.

Federal funding plays an important role in both increasing the knowledge base and training our future work force. Data linking student enrollments in disciplines and federal funding show that there is a very high correlation between funding and fields of study.

Today, our Research Division is actively recruiting for several hundred positions which require skills in the physical sciences. These positions are at the Masters and Ph.D. levels, both experienced professionals and recent graduates.

Federal IT research investment significantly affects our ability to fill these positions. IBM believes the core disciplines which drive the future of information technology, math, physics, chemistry, engineering, computer science and materials science need more investment. Funding should meet the opportunity. This investment will provide resources for the future of information technology and life sciences as well, since the life sciences are multidisciplinary and highly dependent on computational intensity and simulation.

Conclusion

Innovation has always been the strong suit of the United States. Today, innovation remains the key to maintaining our ability to compete in a changing global economy where technology, science and education are becoming widespread. Research is one of the critical inputs to innovation. It is critical that information technology research in the United States advance to meet the challenges of our complex world.

Answer submitted for the record by David Nelson, testimony on July 7, 2004, before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census.

In the hearing Congressman Clay asked me to compare the 2004 budget for Federal IT R&D to 2005. He indicated that it has been reduced by about $200 million, from $2.2 billion to $2.0 billion and wanted to know why the amount requested was reduced.

Although the IT R&D crosscut tables in the President's budget requests for FY 2004 and FY 2005 do total approximately $2.2 billion and $2.0 billion respectively, subsequent analysis is showing that the difference between the FY 2004 and FY 2005 requests is much smaller and almost inconsequential. This is possible because, despite a coordinated process for planning and budgeting federal IT R&D investments, the totals cannot be derived by aggregating budget line-items; rather they are derived by an allocation process that is necessarily imprecise and subject to refinement as agencies progress through their allocation processes.

The updated totals for the FY 2005 IT R&D request will be published shortly in the FY 2005 "Blue Book" that describes the Federal IT R&D program. These updates will show that the funding requested for FY 2005 is not significantly different from that requested for FY 2004.