NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT ACT OF 2009

HEARING

BEFORE THE

COMMITTEE ON SCIENCE AND TECHNOLOGY
HOUSE OF REPRESENTATIVES

ONE HUNDRED ELEVENTH CONGRESS

FIRST SESSION

APRIL 1, 2009

Serial No. 111–17

Printed for the use of the Committee on Science and Technology

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

U.S. GOVERNMENT PRINTING OFFICE

48–168PS WASHINGTON : 2009

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON SCIENCE AND TECHNOLOGY

HON. BART GORDON, Tennessee, *Chair*

JERRY F. COSTELLO, Illinois
EDDIE BERNICE JOHNSON, Texas
LYNN C. WOOLSEY, California
DAVID WU, Oregon
BRIAN BAIRD, Washington
BRAD MILLER, North Carolina
DANIEL LIPINSKI, Illinois
GABRIELLE GIFFORDS, Arizona
DONNA F. EDWARDS, Maryland
MARCIA L. FUDGE, Ohio
BEN R. LUJÁN, New Mexico
PAUL D. TONKO, New York
PARKER GRIFFITH, Alabama
STEVEN R. ROTHMAN, New Jersey
JIM MATHESON, Utah
LINCOLN DAVIS, Tennessee
BEN CHANDLER, Kentucky
RUSS CARNAHAN, Missouri
BARON P. HILL, Indiana
HARRY E. MITCHELL, Arizona
CHARLES A. WILSON, Ohio
KATHLEEN DAHLKEMPER, Pennsylvania
ALAN GRAYSON, Florida
SUZANNE M. KOSMAS, Florida
GARY C. PETERS, Michigan
VACANCY

RALPH M. HALL, Texas
F. JAMES SENSENBRENNER JR., Wisconsin
LAMAR S. SMITH, Texas
DANA ROHRABACHER, California
ROSCOE G. BARTLETT, Maryland
VERNON J. EHLERS, Michigan
FRANK D. LUCAS, Oklahoma
JUDY BIGGERT, Illinois
W. TODD AKIN, Missouri
RANDY NEUGEBAUER, Texas
BOB INGLIS, South Carolina
MICHAEL T. MCCAUL, Texas
MARIO DIAZ-BALART, Florida
BRIAN P. BILBRAY, California
ADRIAN SMITH, Nebraska
PAUL C. BROUN, Georgia
PETE OLSON, Texas

C O N T E N T S

April 1, 2009

NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT ACT OF 2009

THURSDAY, APRIL 1, 2009

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

The Committee met, pursuant to call, at 10:05 a.m., in Room 2318 of the Rayburn House Office Building, Hon. Bart Gordon [Chair of the Committee] presiding.

BART GORDON, TENNESSEE
CHAIRMAN

RALPH M. HALL, TEXAS
RANKING MEMBER

U.S. HOUSE OF REPRESENTATIVES

COMMITTEE ON SCIENCE AND TECHNOLOGY

SUITE 2320 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6301
(202) 225–6375
TTY: (202) 226–4410
http://science.house.gov

Hearing On:

Networking and Information Technology Research and Development Act of 2009

Wednesday, April 1, 2009
10:00 a.m. – 12:00 p.m.
2318 Rayburn House Office Building

WITNESS LIST

Dr. Chris L. Greer
Director, National Coordination Office for Networking and Information Technology Research and Development (NCO/NITRD)

Dr. Peter Lee
Professor and Head, Computer Science Department, Carnegie Mellon University

Mr. Amit Yoran
Chairman and Chief Executive Officer, NetWitness Corporation

Dr. Deborah Estrin
Director, Center for Embedded Networked Sensing, University of California, Los Angeles

HEARING CHARTER

COMMITTEE ON SCIENCE AND TECHNOLOGY U.S. HOUSE OF REPRESENTATIVES

Networking and Information Technology Research and Development Act of 2009

WEDNESDAY, APRIL 1, 2009
10:00 A.M.–12:00 P.M.
2318 RAYBURN HOUSE OFFICE BUILDING

1. Purpose

The purpose of this hearing is to receive testimony on the *Networking and Information Technology Research and Development Act of 2009.* The legislation is based on findings and recommendations included in a recent assessment of the program conducted by the President's Council of Advisors on Science and Technology (PCAST) and proposes changes to the research content and planning and implementation mechanisms of the program.

A section-by-section summary of the legislation is attached as an appendix to this memo.

2. Witnesses:

- **Dr. Chris L. Greer,** Director, National Coordination Office for Networking and Information Technology Research and Development (NCO/NITRD)
- **Dr. Peter Lee,** Professor and Head, Computer Science Department, Carnegie Mellon University
- **Mr. Amit Yoran,** Chairman and Chief Executive Officer, NetWitness Corporation
- **Dr. Deborah Estrin,** Director, Center for Embedded Networked Sensing, University of California, Los Angeles

3. Overarching Questions:

- Does the legislation ensure that the NITRD program is positioned to help maintain U.S. leadership in networking and information technology? What are industry's priorities for the NITRD program and are they adequately addressed in the legislation? What are the research community's needs for this program and are they adequately addressed?
- Does the legislation address the key recommendations of the recent PCAST assessment for making the NITRD program more effective and more relevant to the research needs and opportunities in information technology?
- Are there key research gaps or program management concerns not covered in this legislation? Are the mechanisms for industry and academic input into the planning process sufficient?
- Does the legislation effectively implement the PCAST recommendation for support of large-scale, multi-disciplinary research and development projects? What are the most appropriate mechanisms to undertake these projects? Are the requirements for these projects sufficient to encourage industry/university partnerships?

4. Background

NITRD Program

The Networking and Information Technology Research and Development (NITRD) program, originally authorized in the *High Performance Computing Act of 1991* (P.L. 102–194), is a multi-agency research effort to accelerate progress in the advancement of computing and networking technologies and to support leading edge computational research in a range of science and engineering fields. The 1991 statute established a set of mechanisms and procedures to provide for the interagency planning, coordination, and budgeting of the research and development activities carried out under the program.

The NITRD Subcommittee of the National Science and Technology Council (NSTC) is the working body for interagency planning and coordination and includes representatives from each of the participating NITRD agencies as well as the Office of Management and Budget (OMB). For FY 2009, 13 federal agencies contributed funding to the NITRD program; however additional agencies that do not contribute funding participate in planning activities. The FY 2009 budget request for the NITRD program was $3.548 billion, an increase of $0.207 billion or approximately six percent, over the FY 2008 level of $3.341 billion. A summary of the major research components of the program and funding levels by major component and by agency is available at: *http://www.nitrd.gov/pubs/2009supplement/index.aspx*

The National Coordination Office (NCO) provides staff support for the NITRD Subcommittee and the program's advisory committee and serves as the public interface for the program.

PCAST Assessment

In August 2007, PCAST completed an assessment of the NITRD program and issued a report entitled, *"Leadership Under Challenge: Information Technology R&D in a Competitive World"* [*http://www.nitrd.gov/pcast/reports/PCAST-NIT-FINAL.pdf*].

The PCAST report includes several findings and recommendations related to the research content of the program, as well as suggestions for improving the program's planning, prioritization and coordination. The recommendations from the PCAST report include:

- Federal agencies should rebalance their NITRD funding portfolios by increasing support for important problems that require larger-scale, longer-term, multi-disciplinary R&D and increasing emphasis on innovative and therefore higher-risk but potentially higher-payoff explorations.
- As new funding becomes available for the NITRD program, disproportionately larger increases should go for:
    - research on NIT systems connected with the physical world (which are also called embedded, engineered, or cyber-physical systems);
    - software R&D;
    - a national strategy and implementation plan to assure the long-term preservation, stewardship, and widespread availability of data important to science and technology; and
    - networking R&D, including upgrading the Internet and R&D in mobile networking technologies.
- The NITRD agencies should:
    - develop, maintain, and implement a strategic plan for the NITRD program;
    - conduct periodic assessments of the major components of the NITRD program and restructure the program when warranted;
    - develop, maintain, and implement public R&D plans or roadmaps for key technical areas that require long-term interagency coordination and engagement; and
    - develop a set of metrics and other indicators of progress for the NITRD program, including an estimate of investments in basic and applied research, and use them to assess NITRD program progress.
- The NITRD National Coordination Office should support the development, maintenance, and implementation of the NITRD strategic plan and R&D plans for key technical areas; and it should be more proactive in communicating with outside groups.

Cyber-Physical Systems

The top recommendation of the PCAST report for new research investments in the NITRD program is in the area of computer-driven systems connected with the physical world—also called embedded, engineered, or cyber-physical systems (CPS). CPS are connected to the physical world through sensors and actuators to perform crucial monitoring and control functions. Such systems would include the air-traffic-control system, the power-grid, water-supply systems, and industrial process control systems. On a more individual level, they are found in automobiles and home health care devices.

Examples of CPS are already in widespread use but growing demand for new capabilities and applications will require significant technical advances. Such systems can be difficult and costly to design, build, test, and maintain. They often involve the intricate integration of myriad networked software and hardware components, including multiple subsystems. In monitoring and controlling the functioning of complex, fast-acting physical systems (such as medical devices, weapons systems, manufacturing processes, and power-distribution facilities), they must operate reliably in real time under strict constraints on computing, memory, power, speed, weight, and cost. Moreover, most uses of cyber-physical systems are safety-critical: they must continue to function even when under attack or stress.

There is evidence that CPS will be an area of international economic competition. For example, the European Union's Advanced Research and Technology for Embedded Intelligence and Systems (ARTEMIS) program, funded by a public-private investment of 5.4 billion euros (over $7 billion in mid-2007 dollars) between 2007 and 2013, is pursuing R&D to achieve "world leadership in intelligent electronic systems" by 2016.

Recent Amendments to NITRD Program [included in COMPETES Act]

A 1999 assessment of the program found that the sponsored research was shifting too much toward support for near-term, mission focused objectives; that there was a growing gap between the power of high-performance computers available to support agency mission requirements and those supporting the general academic research community; and that total federal information technology investment was inadequate. In response to that report, the Committee developed legislation that became part of the COMPETES Act (section 7024(a)) and amends the 1991 Act in two significant ways: requires the advisory committee to conduct periodic evaluations of the funding, management, coordination, implementation, and activities of the program and requires OSTP to develop and maintain a roadmap for developing and deploying very high-performance computing (high-end) systems necessary to ensure that the U.S. research community has sustained access to the most capable computing systems.

5. Witness Questions

All witnesses were asked to give their views on the provisions of the bill, including any recommendations for ways to improve it. The list of overarching questions (item 3 above) was included in the invitation letters of all of the witnesses except Dr. Greer.

Dr. Greer

Dr. Greer was asked to please provide an update (since his last testimony before the Committee in July, 2008) of any significant changes to the NITRD Program and any actions the NITRD agencies have taken or plan to take in response to the recommendations of the 2007 PCAST report. In addition, he was asked to answer the following specific questions:

- The NITRD subcommittee of the National Science and Technology Council is in the midst of developing a strategic plan. Please describe those efforts and how, if at all, they address the requirements for strategic planning as described in the legislation. In particular, what are the current mechanisms for industry and academic input into the planning process, and how is the NITRD subcommittee addressing the need for the NITRD program to place more emphasis on higher-risk, long-term projects? What is the timeline for completing the strategic plan?
- Please describe the current responsibilities and activities of the National Coordination Office (NCO). How do those responsibilities and activities compare to the responsibilities and activities required for the NCO in the legislation? In particular, how has the NCO responded to the 2007 PCAST recommendation for improved communication with and outreach to outside groups?

SUMMARY

DRAFT NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT ACT OF 2009

SECTION 1. SHORT TITLE.

"Networking and Information Technology Research and Development Act of 2009".

SEC. 2. PROGRAM PLANNING AND COORDINATION.

PERIODIC REVIEWS.—Responds to the PCAST report recommendation to require the NITRD agencies to periodically assess the NITRD program contents and funding levels and make changes as appropriate. Also requires that the program content include activities authorized under section 3.

STRATEGIC PLAN.—

- Responds to the PCAST report recommendation to require the NITRD agencies to develop and periodically update (three-year intervals) a strategic plan for the program. The characteristics and content of the strategic plan are described.
- Adds to the responsibilities of the OSTP Director oversight responsibility to see that the strategic plan is developed and executed effectively.
- Specifies that the annual report now required for the NITRD program explicitly describe how the program activities planned and underway relate to the objectives specified in the strategic plan.

REPORT.—Specifies that the annual report now required for the NITRD program include a description of research areas supported in accordance with section 3, including the same budget information as is required for the Program Component Areas.

SEC. 3. LARGE-SCALE RESEARCH IN AREAS OF NATIONAL IMPORTANCE.

Generally addresses the PCAST recommendation to increase the NITRD investment in larger scale, high-risk/high-payoff, and multi-disciplinary research. These competitive awards must be made through collaborations between at least two agencies.

Characteristics of the projects supported include:

- collaborations among researchers in academic institutions and industry, and may involve nonprofit research institutions and federal laboratories;
- when possible, leveraging of federal investments through collaboration with related State initiatives; and
- plans for fostering the transfer of research discoveries and the results of technology demonstration activities to industry for commercial development.

Authorizes support of activities under this section through interdisciplinary research centers that are organized to investigate basic research questions and carry out technology demonstration activities

SEC. 4. CYBER-PHYSICAL SYSTEMS.

The first PCAST recommendation regarding NITRD program content was for developing and implementing a plan for research on cyber-physical systems.

Directs that cyber-physical systems be one of the areas supported in accordance with SEC. 3. Specifies R&D objectives and types of activities authorized based on the PCAST recommendations and the results of the community workshops (CPS Steering Group).

Requires the NCO Director to convene an industry/university task force to explore mechanisms for carrying out collaborative research and development activities for cyber-physical systems through a consortium with participants from academic institutions and industry. The goal of the task force is to develop recommendations for the structure and mode of operation of a joint industry/university research consortium and to report the recommendations to Congress. This provision is based on the recommendations of the Boeing witness (Winter) at July 31, 2008 hearing.

SEC. 5. NATIONAL COORDINATION OFFICE.

This section formally establishes the National Coordination Office; delineates the office's responsibilities; mandates annual operating budgets; specifies the source of funding for the office, which mirrors the current practice; and stresses the role of the office in developing the strategic plan and in public outreach and communication with outside communities of interest, following the PCAST recommendations.

Chair GORDON. This hearing will come to order, and good morning.

Welcome to today's hearing on the Networking and Information Technology Research and Development, or as it is commonly known, NITRD Act. Last year this committee held an oversight hearing on the NITRD program. At that hearing we heard from a panel of expert witnesses on the findings of a recent assessment of the program carried out by the President's Council of Advisors on Science and Technology. The PCAST recommendations and the testimony of the witnesses served as a basis for the legislation proposal we are reviewing today.

Last week there was a symposium at the Library of Congress celebrating the achievements of computing research. During the opening session of the symposium, one speaker cited a *New York Times* article to illustrate how far computing has come to demonstrate how profoundly information technology has changed our lives.

The article contained a laundry list of life-changing innovations over the last 30 years. Notably, two-thirds of the items on the list such as the Internet, open-source software and laptop computers, were the result of advances in information technology research. This result clearly demonstrates that information technology is a major driver of the economy and growth and that advances in the field have the potential to dramatically influence all aspects of our lives from manufacturing and health care to education and entertainment. In short, research and networking information technology translates to U.S. scientific, industrial and military competitiveness.

The legislative proposal we are reviewing today responds to two categories of concerns expressed by the PCAST assessment: the strength of NITRD program's planning and coordinating functions and the balance of the research portfolio.

First, the legislation addresses the PCAST recommendations to strengthen the planning, coordination and prioritization components of the program by requiring the development and periodic update of a strategic plan that will create a vision for information technology R&D allowing for continued technological breakthroughs in maintaining U.S. leadership.

Next, the legislation addresses the PCAST recommendation for increased support of large-scale, long-term, interdisciplinary research by creating large-scale R&D rewards that not only encourage collaboration among the NITRD agencies but also promote collaboration between the academic and industry researchers. Past achievements have shown that these large-scale, long-term partnerships are a recipe for success.

Many of the technical advances that led to today's computers and the Internet evolved from past research sponsored by industry and government, often in partnership and conducted by the industry, university and federal labs.

And finally, the legislation highlights the need for increased research in the area of cyber-physical systems. Cyber-physical systems such as the power grid and home health care devices are computer-driven systems connected with the physical world. The prevalence of these systems is likely to increase but technical advances are needed to realize their full potential. The legislation calls for an industry/university task force to explore the mechanisms for carrying out collaborative R&D in this important area, and while there has been breathtaking progress in the field of information technology, I believe the best is yet to come.

[The prepared statement of Chair Gordon follows:]

PREPARED STATEMENT OF CHAIR BART GORDON

Good morning. Welcome to today's hearing on the Networking and Information Technology Research and Development, or as it is commonly known, the NITRD Act. Last year, this committee held an oversight hearing on the NITRD program. At that hearing we heard from a panel of expert witnesses on the findings of a recent assessment of the program carried out by the President's Council of Advisors on Science and Technology (PCAST). The PCAST recommendations and the testimony of the witnesses served as the basis for the legislative proposal we are reviewing today.

Last week, there was a symposium at the Library of Congress celebrating the achievements of computing research. During the opening session of the symposium one speaker cited a *New York Times* article to illustrate how far computing has come and to demonstrate how profoundly information technology has changed our lives.

The article contained a laundry list of life changing innovations over the last 30 years. Notably, two-thirds of the items on the list, such as the Internet, open-source software and laptop computers, were the result of advances in information technology research. This result clearly demonstrates that information technology is a major driver of economic growth and that advances in the field have the potential to dramatically influence all aspects of our lives from manufacturing and health care to education and entertainment. In short, research in networking and information technology translates into U.S. scientific, industrial, and military competitiveness.

The legislative proposal we are reviewing today responds to two categories of concern expressed by the PCAST assessment: the strength of the NITRD program's planning and coordination functions and the balance of the research portfolio.

First, the legislation addresses the PCAST recommendation to strengthen the planning, coordination, and prioritization components of the program by requiring the development and periodic update of a strategic plan that will create a vision for information technology R&D, allowing for continued technological breakthrough and maintaining U.S. leadership.

Next, the legislation addresses the PCAST recommendation for increased support of large-scale, long-term, interdisciplinary research by creating large-scale R&D awards that not only encourage collaboration among the NITRD agencies, but also promote collaborations between academic and industry researchers.

Past achievements have shown us that large-scale, long-term partnerships are a recipe for success. Many of the technical advances that led to today's computers and the Internet evolved from past research sponsored by industry and government, often in partnership, and conducted by industry, university, and federal labs.

Finally, the legislation highlights the need for increased research in the area of cyber-physical systems. Cyber-physical systems such as the power grid and home health care devices are computer-driven systems connected with the physical world. The prevalence of these systems is likely to increase, but technical advances are needed to realize their full potential. The legislation calls for an industry/university task force to explore mechanisms for carrying out collaborative R&D in this important area.

While there has been breathtaking progress in the field of information technology I believe the best is yet to come. A brilliant young scientist who participated in last week's symposium is putting to good use a program he invented to distinguish between a human user and a computer and prevent SPAM e-mail. Now when you type the distorted text at the bottom of a Web registration form you are helping to digitize books that were written before the computer age. This type of ingenuity is the perfect example of why many believe information technology R&D is still in its infancy.

The witnesses before us today have extensive expertise in networking and information technology, and I look forward to their comments on our legislative proposal. I want to thank all of the witnesses for taking the time to appear before the Committee this morning and I look forward to your testimony.

Chair GORDON. Now the Chair recognizes Mr. Hall for an opening statement.

Mr. HALL. Mr. Chair, thank you, and before I make an opening statement, we are always proud when we have people in the audience that are related to us and are praying for us and working for us, and Melé, who wrote this opening statement for me, her mother is in the audience. Her name is Sandra Freeman and she is from Greenville, South Carolina, but she has been skiing in Boulder, Colorado, since the first of the year, and I am told that Colorado is made up of people from Iowa that don't want any more Texans. I don't know if that it right or not. Welcome, and thank you, Mr. Chair, for allowing us to recognize her.

Thank you, Chair Gordon, for scheduling this hearing to receive testimony on draft authorization legislation for the Federal Government's Networking and Information Technology Research and Development program. Currently the NITRD, as they are called, program provides a primary mechanism by which Federal Government coordinates the Nation's more than $3 billion of unclassified networking and information technology research and development investments. As I stated in our last hearing, given the ever increasing amounts of networking and information technology that affects our everyday lives, from power grid and water purification systems to automotive improvements and air traffic control equipment, to home health and care and health care devices and educational software programs, for all that it is important that we not only continue to support these R&D efforts but also make sure that this program is appropriately coordinating with our classified cyber security initiatives as well. In fact, I believe that this is of vital importance to our homeland security and to our economy.

It is my understanding that at this moment a computer worm called Conficker C may be affecting millions of computers in ways that we can't even completely identify yet, and whether this pans out to be a serious threat or simply a perceived threat, the ability for people to create this kind of computer havoc is a real problem. So I would suggest that non-classified cyber security efforts are just as important. Hopefully our witnesses will discuss and address that today as well.

I know that your staff has been working diligently with ours to put together good, solid legislation and I appreciate this bipartisan effort. The draft before us is a culmination of recommendations from the PCAST report, feedback we received from numerous organizations and witness testimony received in the hearing held on this topic last year. So I am sure we will learn today that there are yet more ways we can improve this bill and I hope that we can continue to work together to ensure that it moves forward in a bipartisan fashion and with bipartisan support, and our Chair, I think, is a champion of that type of support.

I look forward to hearing the views of our witnesses today and their recommendations about how we can make an already exemplary interagency program even better.

I yield back my time and I thank the Chair.

[The prepared statement of Mr. Hall follows:]

PREPARED STATEMENT OF REPRESENTATIVE RALPH M. HALL

Thank you, Chairman Gordon, for scheduling this hearing to receive testimony on draft authorization legislation for the Federal Government's Networking and Information Technology Research and Development (NITRD) program. Currently, the NITRD program provides the primary mechanism by which the Federal Government coordinates this nation's more than three billion dollars of unclassified networking and information technology (NIT) research and development (R&D) investments.

As I stated in our last NITRD hearing, given the ever increasing amounts of networking and information technology that affect our everyday lives from power grid and water purification systems to automotive improvements and air traffic control equipment to home health care devices and educational software programs, it is important that we not only continue to support these R&D efforts but also make sure that this program is appropriately coordinating with our classified cyber security initiatives as well. In fact, I believe that this is of vital importance to our homeland security and to our economy.

It is my understanding that at this moment, a computer worm called Conficker C may be affecting millions of computers in ways that we cannot even completely identify yet. Whether this pans out to be a serious threat or simply a perceived threat, the ability for people to create this kind of computer havoc is a real problem. So, I would suggest that non-classified cyber security efforts are just as important. Hopefully, our witnesses will address that today, as well.

I know that your staff has been working diligently with mine to put together good, solid legislation, and I appreciate this bipartisan effort. The draft before us is a culmination of recommendations from the PCAST Report, feedback we have received from numerous organizations, and witness testimony received in a hearing held on this topic last year. I am sure we will learn today that there are yet more ways we can improve this bill, and I hope that we can continue to work together to ensure that it moves forward in a bipartisan fashion and with bipartisan support.

I look forward to hearing the views of our witnesses today and their recommendations about how we can make an already exemplary interagency program even better.

Chair GORDON. Thank you, Mr. Hall.

If there are Members who wish to submit additional opening statements, your statements will be added to the record at this point.

[The prepared statement of Ms. Johnson follows:]

PREPARED STATEMENT OF REPRESENTATIVE EDDIE BERNICE JOHNSON

Good morning, Mr. Chairman and Ranking Member.

Advanced computer networks are the wave of the future.

As technology has improved, we are better able to predict the paths of hurricanes, the force of tsunamis, or even the trajectory of comets.

Advanced computing is a broad area of active research. The Texas Advanced Computing Center, in Austin, has scientists who are using supercomputers to simulate airflow and manage shock waves for next-generation, hypersonic aircraft.

Other researchers there have been working to understand the process by which enzymes convert plant matter into energy, with the goal of creating more efficient enzymes. Then we could more quickly convert waste to energy.

High speed computers have also enabled scientists to develop realistic models of the human lung.

Teams of Texas researchers are working to develop a new tool to image, understand, and diagnose how air flows through the thousands of branching passageways of the lung, and how abnormalities can lead to illness.

There are so many useful applications for high speed computers and advanced networks.

The Federal Government invests more than $3 billion on the Networking and Information Technology Research and Development (NITRD) program.

It is essential that such a large investment is spent wisely.

The President's Council of Advisors on Science and Technology recently provided recommendations on how to improve our federal efforts in computer network research.

A key recommendation was to support high-risk, multi-disciplinary research. I support this suggestion.

For far too long, federal investments have been made in "safe research," or research that has a certainty of getting a result.

The negative consequence is that science moves along at an incremental snail's pace.

Investments in high-risk research may never come to fruition or payoff. However we must support research of this nature.

Scientists must be unfettered to think more creatively. Then, they have the freedom to tackle big questions that sometimes take more time and more experimentation to answer.

As a previous Chair of the Research and Science Education Subcommittee, I have long been a strong supporter of this kind of research.

I want to welcome today's witnesses.

We value your feedback on draft legislation regarding the Networking and Information Technology Research and Development (NITRD) program.

Chair GORDON. Let me thank our witnesses for being here. We are one witness short right now. We have experienced sometimes that getting through the line downstairs can slow people down. There can be other problems. And so we will certainly treat that witness with respect if they come in later and do it in whatever is the appropriate way. Also, I want you to know that there is a busy schedule here in Congress today too. The lack of bodies in the seats is not a lack of interest. This is a very important issue and they will be following it with their staffs, and you are right, Mr. Hall, this has been a good bipartisan start. Melé has been an integral part of putting this together as usual and she is very important to this committee.

So at this time I want to introduce our witnesses. First, Dr. Chris Greer is the Director of the NITRD National Coordinating Office, Dr. Peter Lee is the Head of the Computer Science Department at Carnegie Mellon University, and Dr. Deborah Estrin is the Director of the Center for Embedded Networked Sensing at UCLA. Thank you for being here. As you know, we try to keep the oral statements to five minutes but this is an important area and we are not going to take you out with a hook because we want to hear what you have to say. Your written testimony will be included as a part of the record, and I probably at the end of the day have a couple of more questions that I am going to give to you that you then can respond back in writing. Again, we want to get this right.

So we will start with Dr. Greer.

STATEMENT OF DR. CHRISTOPHER L. GREER, DIRECTOR, NATIONAL COORDINATION OFFICE FOR NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT (NCO/NITRD)

Dr. GREER. Good morning. My name is Chris Greer. I am the Director of the National Coordination Office for the Networking and Information Technology Research and Development Program, and hereafter I will refer to those as NCO and NITRD by their acronyms, respectively, to keep this brief. With Dr. Jeanette Wing of the National Science Foundation, I also co-chair the NITRD subcommittee. I thank Chair Gordon and Ranking Member Hall and the Members of the Committee for the opportunity to come before you today to discuss the NITRD program and the Committee's draft *Networking and Information Technology Research and Development Act of 2009.*

My written testimony provides comprehensive response to the questions the Committee posed in preparation for this hearing, and in my oral comments I want to focus on two specific points.

First, we view the recommendations of the President's Council of Advisors on Science and Technology, the PCAST, and this committee's interest as helpful in further improving the NITRD framework. Our goal, as yours, is to enable the NITRD program to serve the Nation even more effectively in the future. Since I last appeared before you eight months ago, we have continued our vigorous response to the full spectrum of the PCAST recommendations. Our strategic planning process provides an example of that. The plan we are designing comprises elements operating at multiple levels, embraces the emphasis areas identified by PCAST, focuses significantly on opportunities for large-scale, long-term R&D, and benefits from a diversity of means for community input including a request for information published in the *Federal Register,* presentations at scientific and technical meetings, individual one-on-one interviews and small group discussions, a public strategic planning forum, webcasts globally and an opportunity for public comment on the draft text. The NCO is the focal point for supporting this planning process, the spectrum of outreach efforts that inform the plan, the response to the other PCAST recommendations and of course the full range of NITRD program activities. The NCO is currently developing its own strategic plan to further strengthen its capabilities in support of the NITRD program.

Now, the second point I wanted to make this morning is the critical importance of balance in the NITRD portfolio. The vision of previous amending legislation from this committee and of the NITRD agencies over the years has been for a balanced portfolio, one that recognizes that hardware innovations are constrained without corresponding advances in software. The use of advanced networks will be limited without improvements in security and in reliability. The massive data sets will not drive progress if the data cannot be preserved, accessed and used for increased understanding and so on. I urge the Committee to continue its history of crafting a framework that enables the NITRD portfolio of investments to respond to our nation's changing IT needs and opportunities. This includes recognizing the contemporary scope of the NITRD program, positioning emphasis areas in the context of the full NITRD landscape, providing for an advisory committee with the expertise to offer strategic guidance on emphasis and balance to the program and to the President, and encouraging strategic, large-scale, long-term research in all agency contexts.

So thank you for your work on the reauthorization legislation and for the opportunity to appear before you today. We at NITRD and the National Coordination Office, many of the outstanding staff of whom are behind me today including Ernest McDuffy, who is the Associate Director, Diane Theese and Virginia Moore, who are Office Leaders. Thank you for this opportunity.

[The prepared statement of Dr. Greer follows:]

PREPARED STATEMENT OF DR. CHRISTOPHER L. GREER

Good morning. I am Chris Greer, Director of the National Coordination Office (NCO) for Networking and Information Technology Research and Development (NITRD). With my colleague, Dr. Jeannette Wing of the National Science Foundation (NSF), I co-chair the NITRD Subcommittee of the National Science and Technology Council's (NSTC) Committee on Technology. I want to thank Chairman Gordon, Ranking Member Hall, and the Members of the Committee for the opportunity to come before you today to discuss the multi-agency NITRD Program and the Committee's draft *Networking and Information Technology Research and Development Act of 2009.*

The NITRD Program—now in its 18th year—provides a coordinated view of the Government's portfolio of unclassified investments in fundamental, long-term research and development (R&D) in advanced networking and information technology (IT). All of the research reported in this portfolio is managed, selected, and funded by one or more of the 13 member agencies under their own individual appropriations. The Program's current research areas are high-end computing, large-scale networking, cyber security and information assurance, human-computer interaction and information management, high-confidence software and systems, software design and productivity, and socioeconomic, education, and workforce implications of IT. IT R&D advances in these areas further our nation's goals for economic competitiveness, energy and the environment, health care, national defense and national security, and science and engineering leadership.

IT R&D research is performed in universities, federal research centers and laboratories, federally funded R&D centers, private companies, and nonprofit organizations across the country. The NITRD agencies—consisting of the member agencies and a number of other participating agencies and offices—work together to ensure that the impact of their efforts is greater than the sum of the individual agency investments. This synergy is accomplished through interaction across the government, academic, commercial, and international sectors using cooperation, coordination, information sharing, and joint planning, in selected areas where the agencies can identify significant leverage, to identify critical needs, avoid duplication of effort, maximize resource sharing, and partner in investments to pursue higher-level goals.

Program history in brief

The 18-year history of the NITRD Program includes three previous legislative acts. The first, the *High-Performance Computing* (HPC) *Act of 1991* (Public Law 102–194), launched the Program, establishing a framework that combined research goals with specific requirements for interagency cooperation, collaboration, and partnerships with industry and academia. This framework has withstood the test of time, enabling the Program to address its responsibilities under legislation to:

(A) establish the goals and priorities for federal high-performance computing research, development, networking and other activities; and

(B) provide for interagency coordination of federal high-performance computing research, development, networking, and other activities undertaken pursuant to the Program.

The next two acts—the *Next Generation Internet Research Act of 1998* (Public Law 105–305) and the *America COMPETES Act of 2007* (Public Law 110–69)—formally extended the scope of responsibilities for interagency coordination to include human-centered computing; flexible, extensible, inter-operable, and accessible network technologies and implementations; education, training, and human resources; and other areas.

In its first annual report to the Congress in 1992, the Program—then called High Performance Computing and Communications (HPCC)—reported an estimated 1991 multi-agency investment of nearly $490 million across eight federal agencies and four Program Component Areas (PCAs). Today, the NITRD Program coordinates among 13 member agencies that, together, invest more than $3 billion across eight PCAs, each coordinated by an Interagency Working Group (IWG) or Coordinating Group (CG) of member and participating agency program managers. (See Appendices 1 and 2 for a list of the current NITRD agencies and PCAs and a NITRD organizational chart.)

While these numbers reflect sustained and significant budgetary growth over the past 18 years, I believe that the Program is more than just the sum of the investments. The vision of previous amending legislation and of the NITRD agencies over the years has been for a balanced portfolio of investments—a portfolio that recognizes that hardware innovations are constrained without corresponding advances in software; the use of advanced networks will be limited without improvements in security and reliability; massive data sets will not drive progress if the data cannot be preserved, accessed, and used for increased understanding, etc.

The recent recommendations of the President's Council of Advisors on Science and Technology (PCAST) for adjustments in technical priorities and increases in large-scale, long-term investments underscore the need to continuously rebalance the NITRD portfolio in a fast-moving IT landscape. I urge the Committee to support a framework that enables the NITRD portfolio of investments to respond to our nation's changing IT needs and opportunities.

Response to the Committee Request

The invitation to testify here today included a request to address one topic and respond to two specific questions. Responses are provided in the numbered sections that follow.

Topic 1. "[P]rovide an update (since your last testimony before the Committee in July, 2008) of any significant changes to the NITRD Program and any actions the NITRD agencies have taken or plan to take in response to the recommendations of the 2007 PCAST report."

We view the recommendations of the 2007 PCAST report assessing the NITRD Program[1] as helpful in further improving the NITRD framework. Our goal, as yours, is to enable the NITRD Program to serve the Nation even more effectively in the future. Our activities over the past eight months in response to the PCAST recommendations are summarized by topic below.

a) Strategic Planning

The NITRD Program is engaged in a robust process, including extensive public input, for developing a comprehensive, five-year strategic plan. Details of this process are described below in the response to the Committee's questions on this topic. The contents of this strategic plan will guide our subsequent roadmapping process, including review of the structure of the NITRD Program. We expect the strategic plan to be completed later this year. However, it is important to remember that this strategic plan must complement and integrate the legislatively mandated strategic plans of the member agencies.

b) Education and workforce issues

With regard to the PCAST's education and workforce recommendations, SRI International is nearing completion of a NITRD-commissioned fast-track study of international education and workforce trends that we will use to inform the NITRD strategic plan.

We also moved ahead last summer, under the aegis of the Social, Economic, and Workforce implications of IT (SEW) Coordinating Group (CG), to convene a September 2008 workshop of federal program managers who have responsibilities related to networking and information technology education and workforce development. Since that meeting, a task force of the participants has been working with SEW to develop content for the strategic plan on the federal role in IT education and workforce development.

Moreover, in the strategic planning process we are discussing not just technologies and applications but the educational preparation of both technology workers and technology users. We devoted the first session of the public forum to education issues to emphasize their role in our considerations.

c) Rebalancing the NITRD portfolio

Our responses to the PCAST recommendations to increase emphasis on large-scale, long-term efforts and on cyber-physical systems, software, digital data, and networking are summarized individually below.

1. **Large-scale, long-term efforts:** The strategic planning process is explicitly designed to target PCAST recommendations on portfolio balance and emphasis areas such as large-scale, long-term, and high-risk investments. The planning thus is cast at a high level that can build on the existing strategic plans of our member agencies by focusing very directly on challenges that no single agency can meet on its own. In fact, we view the identification of these challenges as the principal goal of the NITRD strategic planning process and the necessary foundation to enable the member agencies to establish NITRD priorities and initiate roadmaps for specific research thrusts under the plan. We anticipate developing roadmaps by NITRD research area, as PCAST recommended, and will provide these separately rather than in the strategic plan, allowing different update cycles for the different types of plans.

[1] *Leadership Under Challenge: Information Technology R&D in a Competitive World.* President's Council of Advisors on Science and Technology, August 2007, Washington, D.C. Available at *http://www.nitrd.gov/Pcast/reports/PCAST-NIT-FINAL.pdf*

2. **Cyber-Physical Systems:** We appreciate the Committee's interest in cyber-physical systems and agree with the Committee on their importance. As we detail below, there are a number of ongoing activities under existing NITRD structures that are focusing on this area already. However, we are concerned with the precedent of including a specific application of NITRD research in this bill.

   A comprehensive plan for assessing national R&D needs in the complex life- and safety-critical technologies called cyber-physical systems was initiated prior to the PCAST assessment and is yielding positive results. In this plan, the High Confidence Software and Systems (HCSS) CG has a leadership role in convening researchers and companies across three selected sectors and industries comprising medical devices, transportation systems (air, rail, auto), and energy (which includes SCADA control systems). Our goals in identifying R&D challenges in each sector are to identify both opportunities for targeted investments and, more importantly, fundamental challenges common across the sectors that may merit large-scale, long-term, multi-agency investments. The first sector report—on high-confidence medical systems—has just been published (March 2009). For high-confidence transportation systems, the first in a series of workshop reports is expected in April 2009 with the NITRD analysis to follow that. An energy sector workshop is slated for June 2009; it follows a previous workshop on SCADA systems. These sector reports will be used to analyze common challenges that are potential targets for interagency investments.

   Through its workshop series, HCSS is establishing communities of interest for the first time—such as among researchers, medical clinicians, hospital administrators, industry representatives, and government regulators with a stake in improving the quality and increasing the capabilities of IT-enabled medical devices and systems, and among designers, safety experts, engineers, and academic researchers involved in the aviation, automotive, and rail sectors. This is an example of the broad outreach being undertaken by the NITRD Program.

3. **Software:** The NITRD Program's Software Design and Productivity (SDP) CG is revitalizing its collaborative agenda and interagency activities under new leadership from NSF and NIST. I participated last week in an NSF-sponsored "software sustainability" conference that signals that agency's continuing high interest in the challenges of improving the quality, performance, and cost-effectiveness of software. The reality that these challenges make slow advances across the spectrum of networking and information technology applications is a leitmotif of NITRD strategic planning discussions.

4. **Digital Data:** A number of NITRD agency representatives participated in, and served as co-chairs for, the Interagency Working Group on Digital Data (IWGDD) chartered by the NSTC in 2006 to "develop and promote the implementation of a strategic plan for the Federal Government to cultivate an open inter-operable framework to ensure reliable preservation and effective access to digital data for research, development, and education in science, technology, and engineering." Such a plan, with NITRD participation, was recommended by PCAST. The IWGDD, representing more than two dozen agencies, delivered its report—*Harnessing the Power of Digital Data for Science and Society*—to the NSTC in January 2009. The report addresses the substance of the PCAST recommendation. It provides essential conceptual foundations and proposes structural scaffolding for rationalizing federal roles and responsibilities in managing and maintaining critical scientific data on behalf of the Nation.

5. **Networking:** PCAST endorsed the development of a Federal Plan for Advanced Networking Research and Development. That plan, prepared by a task force of NITRD agency members and others pursuant to a January 2007 charge from the Director of OSTP, was posted in draft on the NCO web site in August 2007 for public comment and published in final form by the NCO in September 2008.[2] The document serves as an overarching guide for planning and coordination in the LSN Coordinating Group. For example, DOE/SC and NSF, with LSN and NCO support, hosted a "Networking Research

[2] *Federal Plan for Advanced Networking Research and Development,* Interagency Task Force on Advanced Networking Research and Development, September 2008. Available at *http://www.nitrd.gov/Pubs/ITFAN-FINAL.pdf*

Challenges" workshop shortly after the plan's issuance to elicit the views of the broader industry and academic networking research communities about the plan and key R&D priorities. The report of that workshop is currently being prepared for publication.

The LSN Coordinating Group also is addressing PCAST's recommendations on strengthening the infrastructure for large-scale data resources and increasing network security and reliability. The group is coordinating cross-domain performance measurement to enable improved management and security on networks. It is also fostering the development, use, and sharing of standardized tools and infrastructure for large-scale distributed access, data transfer, and collaborations.

Question 1. "The NITRD subcommittee of the National Science and Technology Council is in the midst of developing a strategic plan. Please describe those efforts and how, if at all, they address the requirements for strategic planning as described in the legislation. In particular, what are the particular mechanisms for industry and academic input into the planning process, and how is the NITRD subcommittee addressing the need for the NITRD Program to place more emphasis on higher-risk, long-term projects? What is the timeline for completing the strategic plan?"

We believe the strategic planning process currently underway addresses the requirements for strategic planning as described in the draft legislation. However, the planning process is mindful of the need to complement and integrate the legislatively mandated strategic plans of the member agencies.

The process currently in place provides for public input at each phase of the planning effort. Input at the outset was obtained through a Request for Information published in the *Federal Register* in August 2008, posted on our web site, and announced through a broad distribution to the community. This input and discussions by the NITRD strategic planning team were used to define an initial conceptual framework for the plan. Input on this conceptual framework was obtained at a public, webcast forum held in February 2009. The input we have received has been excellent and we are using this to significantly revise the framework and develop draft text for public comment in June/July 2009. Depending on the nature of the comments, we may either go forward with a final version—if minor revisions are required—or re-release for public comment—if major revisions are needed.

Question 2. "Please describe the current responsibilities and activities of the National Coordination Office (NCO). How do these responsibilities and activities compare to the responsibilities and activities required for the NCO in the legislation? In particular, how has the NCO responded to the 2007 PCAST recommendation for improved communication with and outreach to outside groups?"

The PCAST concluded that the NCO had been "effective" in its support of the NITRD Program. I believe that the main areas of the NCO's effectiveness are in its role as:

- The focal point for coordination and policy development for the Federal NITRD Program, facilitating the various Program elements (e.g., CGs and IWGs) and activities and fostering collaboration among federal agencies, university researchers, industry, and other members of the IT community.
- A source of timely, high-quality, technically accurate, in-depth information on IT R&D accomplishments, new directions, and critical challenges that IT leaders, policy makers and the public can use to maximize social and economic benefits.
- A team of technically expert, service-oriented professionals committed to advancing the mission of the NITRD Program.

The categories of activities the NCO supports are:

- Logistical/staff and expert technical support for regular meetings of the IWGs and CGs
- Expert technical and professional writing support for the annual NITRD supplement to the President's budget
- Logistical/staff and expert technical support for annual planning meetings of the PCAs to assess progress and identify priorities and activities for the coming year
- Logistical/staff, expert technical, and professional writing and graphics support for task groups and others developing federal reports and strategic plan

documents for IT R&D; includes support for the Senior Steering Group developing coordination and leap-ahead plans for the Federal Comprehensive National Cybersecurity Initiative (CNCI)

- Expert technical and management support for procurement, management, and oversight of contracted studies, reviews, and reports
- Logistical/staff, expert technical, and professional writing support for public and government workshops and other meetings
- Expert outreach through participation in appropriate government and non-government meetings and workshops and on-site visits to industrial, academic, and non-profit entities
- Expert outreach through response to requests for information from corporate, academic, international, and other inquirers
- Liaison between the NITRD Program and OSTP and OMB on NITRD issues.

A 2008 self-study of a 20-month period revealed that in an average month the NCO: supports more than seven IWG, CG and community of practice meetings; supports an average of one and a half workshops; participates in one workshop; supports two writing projects; and supports two studies or reviews.

In 2008, more than 350 government employees participated in NCO-supported NITRD events. Highlights for the past 12 months include producing the President's Budget Supplement, creating the coordination and leap-ahead plans for the CNCI effort, publishing the Federal Plan for Advanced Networking Research and Development and the High Confidence Medical Devices reports, producing a lessons-learned report for PCAST, launching an SRI study of the IT education/workforce landscape, publishing four requests for information (RFIs) in the *Federal Register* for public input to the NITRD strategic plan and the CNCI cyber leap year activities, and conducting a webcast public forum for input to the NITRD strategic plan.

This range of activities and responsibilities is similar to that envisioned in the Committee's draft 2009 NITRD legislation with the exception of two areas: coordination with State IT R&D activities and coordination of the proposed task force.

In its 2007 assessment, the PCAST recommended that the NCO *"develop and implement a plan for supporting the development, maintenance, and implementation of the NITRD strategic plan and R&D plans."* In response, NCO supported a two-day kickoff retreat for strategic planning by the NITRD community and supports bimonthly meetings of the NITRD strategic planning team. The team issued an RFI for public input in August 2008, developed a conceptual framework for the plan based on this input, conducted a webcast public forum for input on the framework, is now organizing a forum of government participants for similar input, and is entering the writing phase to produce text for public comment. Similar support for the roadmapping process is planned for the second half of this calendar year.

The PCAST recommendation also provided that NCO should develop plans for supporting the *"planning and coordination of larger, longer-term multi-disciplinary projects; greater interaction with academia, industry, and international entities; the planning of national workshops and preparation of workshop reports; and overall improved communication with NITRD NCO stakeholders."* We have launched an all-hands effort to develop the first-ever NCO strategic plan to address the responsibilities that are appropriate for the NCO. The plan will be shared with the NITRD community, with NSTC, OSTP, and OMB, and then with the public. I have set a deadline of October 1, 2009 for completing this NCO plan.

Comments on draft NITRD 2009 legislation

We greatly appreciate the Committee's interest in NITRD and its continuing efforts to strengthen the Program. We share your commitment to the success of the NITRD enterprise. In the spirit of shared goals, we would like to offer a few comments intended to be helpful as the Committee considers legislation. Since the Administration is still in the process of formulating its research and development priorities, it would be premature for me to comment in detail on the relative priorities implied in the draft legislation. Therefore, my comments below focus on the organizational elements of the draft legislation.

a) Scope of the Program

The Program's founding legislation, the *High-Performance Computing Act of 1991,* focused principally on high-performance computing and networking. This focus was reflected in the extensive use of the phrase "high-performance computing" throughout. Subsequent amending legislation significantly broadened the scope of the Program and facilitated rebalancing of the portfolio. While these previous amendments (and the current draft) redefined the meaning of the phrase "high-performance computing," the phrase itself remains embedded in the text. As a result, a reader not attentive to special definitions and, instead, relying on the common meaning of the phrase may be misled. For example, Section 101(b)(1) (Advisory Committee) describes "an advisory committee on high-performance computing." If the words are misinterpreted, the resulting committee may be too narrowly focused to serve the intended function.

We respectfully request that the Committee consider replacing the phrase "high-performance computing" with "networking and information technology" wherever appropriate throughout the text in order to clarify current legislative intent.

b) Cyber-physical systems

As evidenced in my description above of our extensive cyber-physical systems efforts, the NITRD agencies are seriously engaged in this area. Significantly, however, we feel that cyber-physical systems are best addressed in the context of a balanced portfolio.

Because the scientific basis of networking and information technology is inherently multi-disciplinary, the more complex the IT systems, the greater the number of cross-cutting technical issues. NITRD's strength is that its research areas are not so narrowly focused that topics become isolated. Each PCA includes many inter-related subject matters, and a number of these—multi-dimensional modeling, for example, or system inter-operability—are shared interests across the PCAs. Such interests often lead to collaborative planning activities and/or research projects drawing diverse technical contributions from different PCAs. For example, the National Security Agency (NSA) is an active participant in the HCSS workshop series, not due to a focus on cyber-physical systems per se, but rather on the design, certification, and operation of extremely secure and reliable software and systems; for NSA, cyber-physical systems represent one instantiation of technology with requirements it cares about.

c) Advisory Committee

We believe that to perform its function the proposed advisory committee should:

(1) be charged with providing strategic advice and not just Program assessment;

(2) possess deep technical expertise relevant to the full range of NITRD areas; and

(3) be in position to provide advice to the President.

The first of these criteria could be addressed in the draft legislation by adding to the current list of advisory committee responsibilities the strategic functions currently referenced elsewhere in the draft text. The second and third could be met by chartering the advisory committee as a subcommittee to PCAST.

d) Large-scale research in areas of national interest

The NITRD strategic planning process is explicitly designed to target PCAST recommendations on portfolio balance and emphasis areas such as large-scale, long-term, and high-risk investments. However, we believe this emphasis area is best considered in the context of the full scope of the NITRD Program. In particular, investments that meet the relevant criteria should be considered across all of the PCAs and should be complementary to and supportive of other investments being made by the NITRD agencies and by others throughout the IT R&D landscape.

The draft legislation also provides that "projects shall be carried out by a collaboration of no fewer than two agencies participating in the Program." This could be interpreted to exclude large-scale investments by any single NITRD agency or through partnerships between a NITRD agency and any non-NITRD entity. This may not be the intention of the Committee and clarification of the Committee's intent would be very helpful.

Thank you for your interest in NITRD, your work on the reauthorization legislation, and for the opportunity to appear before you today. We look forward to working with you to strengthen the NITRD Program.

Appendix 1: NITRD Agencies and Program Component Areas

Member agencies

AHRQ – Agency for Healthcare Research and Quality
DARPA – Defense Advanced Research Projects Agency
DOE/NNSA – Department of Energy/National Nuclear Security Administration
DOE/SC – Department of Energy/Office of Science
EPA – Environmental Protection Agency
NARA – National Archives and Records Administration
NASA – National Aeronautics and Space Administration
NIH – National Institutes of Health
NIST – National Institute of Standards and Technology
NOAA – National Oceanic and Atmospheric Administration
NSA – National Security Agency
NSF – National Science Foundation
OSD and Service research organizations (Office of the Secretary of Defense and DoD Air Force, Army, and Navy research organizations)

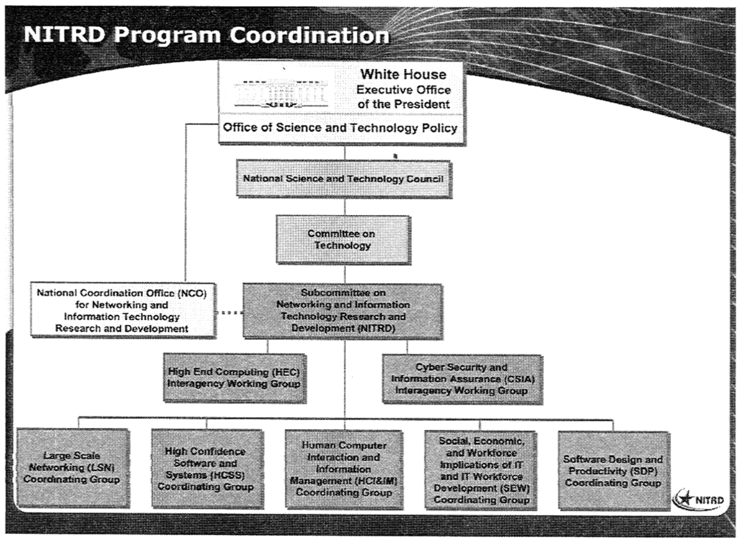
Participating agencies

CIA – Central Intelligence Agency
DHS – Department of Homeland Security
DNI – Office of the Director of National Intelligence
DOE (OE) – Department of Energy Office of Electricity Delivery and Energy Reliability
DOJ – Department of Justice
DOT – Department of Transportation
FAA – Federal Aviation Administration
FBI – Federal Bureau of Investigation
FDA – Food and Drug Administration
GSA – General Services Administration
IARPA – Intelligence Advanced Research Projects Activity
State – Department of State
Treasury – Department of the Treasury
TSWG – Technical Support Working Group
USGS – U.S. Geological Survey

Program Component Areas, Interagency Working Groups/Coordinating Groups/Teams

High End Computing Infrastructure and Applications (HEC I&A) – HEC IWG
High End Computing Research and Development (HEC R&D) – HEC IWG
Cyber Security and Information Assurance (CSIA) – CSIA IWG
Human-Computer Interaction and Information Management (HCI&IM) – HCI&IM CG
Large Scale Networking (LSN) – LSN CG
LSN Teams:
Joint Engineering Team (JET)
Middleware and Grid Infrastructure Coordination (MAGIC)
High Confidence Software and Systems (HCSS) – HCSS CG
Social, Economic, and Workforce Implications of IT and IT Workforce Development (SEW) – SEW CG
Software Design and Productivity (SDP) – SDP CG

Appendix 2: NITRD Program Structure



BIOGRAPHY FOR CHRISTOPHER L. GREER

Dr. Chris Greer is Director of the National Coordination Office (NCO) for the Networking and Information Technology Research and Development (NITRD) program. The NCO reports to the Office of Science and Technology Policy within the Executive Office of the President. Dr. Greer is on assignment to the NCO from his position as Senior Advisor for Digital Data in the NSF Office of Cyberinfrastructure. He recently served as Executive Secretary for the Long-lived Digital Data Collections Activities of the National Science Board and is currently Co-Chair of the Interagency Working Group on Digital Data of the National Science and Technology Council's Committee on Science. He is also a member of the Advisory Committee for the National Archives and Records Administration's Electronic Records Archive and a member of the Digital Library Council of the Federal Depository Library Program.

Dr. Greer received his Ph.D. degree in biochemistry from the University of California, Berkeley and did his postdoctoral work at CalTech. He was a member of the faculty at the University of California at Irvine in the Department of Biological Chemistry for approximately 18 years where his research on gene expression pathways was supported by grants from the National Science Foundation, the National Institutes of Health, and the American Heart Association. During that time, he was founding Executive Officer of the RNA Society, an international professional organization.

Chair GORDON. Thank you, Dr. Greer, and we are glad the guys that get the work done are here today too.

Dr. Lee.

STATEMENT OF DR. PETER LEE, INCOMING CHAIR, COMPUTING RESEARCH ASSOCIATION (CRA); PROFESSOR AND HEAD, COMPUTER SCIENCE DEPARTMENT, CARNEGIE MELLON UNIVERSITY

Dr. LEE. Good morning, Mr. Chairman, Ranking Member Hall and other Members of the Committee. Thank you for this opportunity to comment on the NITRD program. My name is Peter Lee. I am, as you mentioned, the Head of the Computer Science Department at Carnegie Mellon University. I am also the incoming Chair for the Board of Directors of the Computing Research Association, which is the key representative organization for over 30 industry labs and government organizations and 225 academic institutions in computing research.

You mentioned the symposium last week, Computing Research that Changed the World. I had the great privilege to attend that symposium, which was co-sponsored by several Members of your committee. It was a fantastic showcase for about 20 years of past advances in IT research, advances that have really touched every part of our lives, advanced our economy and enabled innovation in a multitude of scientific and engineering fields such as mapping human genome, creating the World Wide Web and Google and even now digitizing the world's books so everyone can access them. For all these past successes, what I found most exciting was that we are still in our infancy. We are on the cusp of major new advances in media and communication technologies, new tools for managing energy and the environment and new technologies for improving health care. The pace of innovation is really breathtaking.

Looking ahead, the question that enters my mind is, who will lead in future innovations. Today many countries are investing heavily in facilities, education and research in network and information technology. Consider, for example, the emerging field of cyber-physical systems that you had mentioned in your opening remarks. This is the science of computing systems tightly integrated with the physical world, and this promises to enable new advances in transportation, medicine and many other areas, even consumer products such as toys. It is no secret that the Europeans today are investing heavily, many billions of dollars, in fact, in cyber-physical systems today. We here look to industry but industry is not able to support the kind of speculative research in such emerging areas to the level that is necessary. Thus, your support, our government's support for this type of research, as the NITRD program is designed to provide, is crucial for remaining competitive. Given the strong track record of university and industry partnerships in information technology, I am confident that these investments will be paid back many times over.

The current legislation thankfully strengthens the NITRD program by addressing many of the key recommendations in the 2007 PCAST assessment. I applaud this. However, I still think that there are major challenges, particularly for university-based IT research. I would like to address just a couple of them with you today.

First, today, a staggering 86 percent of all academic computer science research funding comes from the National Science Foundation. As my written testimony explains, the lack of a broader base of agency support leads to several problems including making researchers less likely to propose the kinds of high-risk, high-return, multi-disciplinary research that we all recognize as necessary. I therefore recommend achieving a broader base of support for our university-based research by urging more agencies to take greater responsibility for advancing both fundamental and multi-disciplinary IT research.

Second, the PCAST assessment recommends that NITRD encourage innovation and risk taking, and in fact, the legislation encourages this by promoting both large-scale and multi-disciplinary research. I would also like to urge the agencies to develop patience, the patience for long-term, sustained and stable funding. This will be key to re-energizing high-risk innovative proposals.

And then finally, an area that deserves special mention is the pipeline of talent in information technology. Simply put, we are not attracting enough good people into the field. This problem is particularly acute with women and under-represented minorities. In my written testimony, I offer several recommendations from the computing research community that would bring a federal focus to issues in computer science education at the K–12 level and this would enable emerging concepts in computational thinking to make their way into the education of all Americans.

So in summary, network and information technology research and development is a field full of amazing opportunities and is a cornerstone for our future competitiveness. By encouraging broader agency support and stable, long-term university-based research support along with a healthy pipeline of talent, we can ensure U.S. leadership into the future.

Mr. Chair, Members of the Committee, thank you for this opportunity to address the NITRD program. My written testimony includes many more details about the points I have raised here as well as answers to the questions you have posed in writing. Thank you for your time and attention.

[The prepared statement of Dr. Lee follows:]

PREPARED STATEMENT OF PETER LEE

Good morning, Mr. Chairman and Members of the Committee. Thank you for this opportunity to comment on the proposed changes to the research content, planning, and implementation mechanisms of the Networking and Information Technology Research and Development (NITRD) program. I am Peter Lee, incoming Chair of the Board of Directors for the Computing Research Association (CRA). The CRA is widely recognized by the U.S. computing research community as its representative organization, with a membership of over 225 academic institutions, 30 government and industrial laboratories, and the leading professional societies in the computing field.

I have been actively involved in computing research for the past 22 years as a Professor at Carnegie Mellon University. Today I am the Department Head for Carnegie Mellon's Computer Science Department. I am also the Vice-Chair of the DARPA Information Science and Technology (ISAT) advisory board; a member of the National Research Council's Computer Science and Telecommunications Board (CSTB); and a member of the CRA's Computing Community Consortium (CCC).

On March 25, 2009, I had the great privilege to participate in a special symposium held at the Library of Congress entitled, *Computing Research that Changed the World: Reflections and Perspectives,*[1] which was organized by the CCC and cosponsored by several Members of your committee. The symposium, which was attended by members of academia, industry, and the government, reviewed the past two decades of "game-changing" advances in networking and information technology

[1] The symposium web site can be found at *http://www.cra.org/ccc/locsymposium.php*

(henceforth referred to as "IT") and provided a forum for discussing how to foster these kinds of advances into the future. The presentations and discussions at the symposium made clear the astonishing importance of IT research:

- **Advances in IT are transforming all aspects of our lives.** Virtually every human endeavor today has been touched by information technology, including commerce, education, employment, health care, energy, manufacturing, governance, national security, communications, the environment, entertainment, science, and engineering.
- **Advances in information technology are driving our economy.** IT research has shown an extraordinary ability to create transferable technologies, resulting in remarkable growth in the industrial IT sector over the past two decades. The impact of IT research on the Nation's industrial base is not restricted to just the IT sector; information technology has been a driver for economic growth in nearly every sector, since every industry is now "powered" by advances in IT. Recent analysis suggests that the remarkable economic growth the U.S. experienced between 1995 and 2002 was spurred by an increase in productivity enabled almost completely by factors related to IT.[2] The processes by which advances in information technology enable productivity growth, enable the economy to run at full capacity, enable goods and services to be allocated more efficiently, and enable the production of higher quality goods and services are now well understood.[3]
- **Advances in information technology are enabling innovation in all other fields.** In business, advances in IT are giving researchers powerful new tools, enabling small firms to significantly expand R&D, boosting innovation by giving users more of a role, and letting organizations better manage the existing knowledge of its employees.[4] In science and engineering, advances in IT are enabling discovery across every 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, and to collect, manage, and explore massive amounts of data.

The most exciting aspect of the *Computing Research that Changed the World* symposium was that it showed that networking and information technology is still in its infancy. In all likelihood, **the most important advances in IT are still ahead of us.** We are on the cusp of new media and communication technologies, new tools for managing our energy and environment, new technologies for improving health care, and even entirely new paradigms for scientific discovery. Worldwide there appears to be no slowdown in the pace of innovation, the production of new ideas, and the discovery of additional opportunities to advance the economy and improve the quality of life for all people through IT.

Several months ago, the National Academy of Engineering unveiled 14 *Grand Challenges for Engineering* for the 21st century.[5] The majority of these—the majority of the "Grand Challenges" for *all* of engineering—have either substantial or predominant information technology content:

- Secure cyberspace
- Enhance virtual reality
- Advance health information systems
- Advance personalized learning
- Engineer better medicines
- Engineer the tools of scientific discovery
- Reverse-engineer the brain
- Prevent nuclear terror (to a great extent a sensor network and data mining problem).

And there are many more information technology challenges of equally high impact:

[2] Jorgenson, Dale W., Mus S. Ho, and Kevin J. Stiroh. *Productivity, Volume 3: Information Technology and the American Growth Resurgence.* MIT Press. 2005.

[3] Atkinson, Robert D., Andrew S. McKay. *Digital Prosperity: Understanding the Economic Benefits of the Information Technology Revolution.* Information Technology and Innovation Foundation. 2007. *http://www.itif.org/files/digital_prosperity.pdf*

[4] Jorgenson, Dale W., Mus S. Ho, and Kevin J. Stiroh. *Productivity, Volume 3: Information Technology and the American Growth Resurgence.* , pp. 46–48. MIT Press. 2005.

[5] *http://www.engineeringchallenges.org/*

- Empower the developing world through appropriate information and communication technology
- Revolutionize transportation safety and efficiency
- Build truly scalable computing systems, and devise algorithms for extracting knowledge from massive volumes of data
- Engineer advanced "robotic prosthetics" and, more broadly, enhance people's quality of life
- Instrument your body as thoroughly as your automobile
- Engineer biology (synthetic biology)
- Revolutionize our electrical energy infrastructure: generation, storage, transmission, and consumption
- Achieve quantum computing.

It is impossible to imagine afield with greater opportunities to change the world.

For me, the inescapable conclusion is that **leadership in information technology is essential to the Nation.** Today, many countries are investing heavily in facilities, education, and research in IT. Industry today is not providing support for long-term, speculative research; hence, government coordination and sponsorship research is the foundation for maintaining our leadership.

It is against this backdrop that I would now like to consider the four questions you have asked me to address here today.

Question 1: *Does the legislation ensure that the NITRD program is positioned to help maintain U.S. leadership in networking and information technology? What are the research community's needs for this program and are they adequately addressed?*

Advances in networking and information technology enable advances in science, economic growth, and quality of life. A key element of the NITRD program involves fostering communication and coordination across thirteen federal agencies where IT is relevant, thereby creating a diverse ecosystem for IT R&D spanning across many areas. The current legislation strengthens the program by addressing several key recommendations from the 2007 assessment of the NITRD program by the President's Council of Advisors on Science and Technology (PCAST).[6]

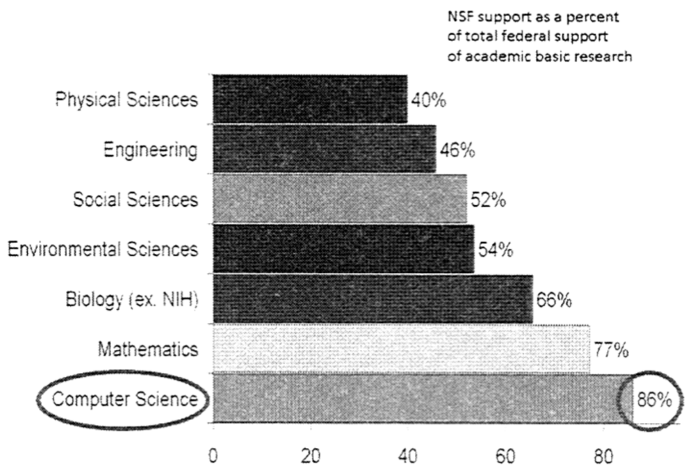
While the coordination provided by NITRD has proven effective, adequate funding diversity for IT research in universities has proven to be quite challenging. Over the past twenty years, two federal agencies have been dominant in university-based IT research: the National Science Foundation (NSF) and the Defense Advanced Research Projects Agency (DARPA). Most of the other NITRD agencies—for example, the National Oceanic and Atmospheric Administration (NOAA), the National Aeronautics and Space Administration (NASA), the Department of Energy (DOE), and the National Institutes of Health (NIH)—have invested far less in university-based IT research, choosing instead to leverage the NSF and DARPA efforts. **IT research would be strengthened by urging agencies such as NIH, DOE, and DHS to take greater responsibility for advancing IT in areas specifically relevant to their missions, particularly via university-based research.**

Furthermore, for academic IT research, policies at DARPA have left NSF standing largely alone. Frequent "go/no-go" program reviews and an overly aggressive approach to security classification have greatly reduced our leadership in the IT area and limited the DOD's access to the best minds in the country. The overall effect is the significant reduction in university participation in DARPA IT programs. Indeed, today NSF provides 86 percent of the federal support for academic research in computer science,[7] a far greater proportion than for any other field.

---

[6] President's Council of Advisors on Science and Technology. *Leadership Under Challenge: Information Technology R&D in a Competitive World.* 2007. *http://www.ostp.gov/pdf/nitrd review.pdf*

[7] National Science Foundation. *FY 2008 Budget Request to Congress.* 2007. *http://www.nsf.gov/about/budget/fy2008/pdf/EntirePDF.pdf*



In my own analysis of the situation,[8] the dramatic reduction of DARPA from the IT R&D ecosystem has had several a damaging effects. To a significant extent, increases in NSF funding for IT research at the start of this decade merely offset decreased DARPA academic engagement, thereby diminishing the possibilities for transformative impact of that funding. Coupled with increased competition for research funding, many researchers have become more risk averse. **Increasing participation by DARPA or another agency in university-based research in fundamental IT would strengthen IT research in all agencies.** This would provide greater leverage for increases in IT investments in NSF, NIH, DOE, and other agencies. Furthermore, the traditional DARPA model of higher-risk ventures within the context of focused program objectives provided a unique set of strategic advantages - an important feature of a strong R&D ecosystem.

Question 2: *Does the legislation address the key recommendations of the recent PCAST assessment for making the NITRD program more effective and more relevant to the research needs and opportunities in information technology?*

I am encouraged that the draft addresses many key recommendations of the 2007 PCAST assessment. I believe the provisions of that assessment will certainly make the NITRD program more effective in meeting the needs and opportunities in networking and information technology R&D. The PCAST assessment noted that the most critical need is to "rebalance the NITRD investment portfolio to include more long-term, large-scale, multi-disciplinary IT R&D." In this respect, the explicit focus on supporting such large-scale multi-disciplinary research is greatly welcomed. However, it is equally important to maintain strong investments in core IT research, in balance with multi-disciplinary research. As we learned at the symposium on Computing Research that Changed the World, strength in multi-disciplinary research is based on a foundation of strong core research. To the extent that core research activities are often conducted by single investigators or small groups, this also implies a balance between large-scale and small-scale efforts.

The legislation includes cyber-physical systems (CPS) research and development, as recommended in the PCAST assessment. One can observe that many of the grand research challenges listed earlier involve a deep embedding, coordination, and control of networking and information technologies with the physical world, making it clear that CPS is indeed an emerging area of opportunity. It is critical that **the legislation is phrased to reflect the full breadth CPS.** CPS pertains not just to man-made devices, but to any IT-enabled combination of physical sensing and actuation devices in the real world.

One of the most important recommendations of the PCAST assessment pertains to the oversight and review of NITRD investment and accountability against the

[8] Peter Lee and Randy Katz. Re-envisioning DARPA. CCC whitepaper. *http://www.cra.org/cec/initiatives.php*

program's strategic plan. Specifically, the legislation specifies the re-establishment of the President's Information Technology Advisory Committee (PITAC), functioning as a separate Presidential advisory committee of academic and industry leaders. As Daniel Reed testified before this committee in 2008, **"an independent PITAC is needed that can devote the time, energy, and diligence to ongoing assessment of successes, challenges, needs and opportunities in information technology."** In such a fast-moving field offering so many opportunities for university-industry partnerships, such focused oversight is crucial for maximizing the payoff of NITRD investments.

Question 3: *Are there key research gaps or program management concerns not covered in this legislation? Are the mechanisms for industry and academic input into the planning process sufficient?*

The legislation encourages large-scale, multi-disciplinary research. It is equally important to have **a renewed emphasis on long-term research, through sustained, stable funding, is critical for re-energizing high-risk, high-impact proposals.** As the National Research Council's "tire tracks" figure shows,[9] there can be long incubation periods for game-changing technologies. Providing the "patience" for such incubation is a key function of the NITRD program. As the 2007 PCAST assessment recommends, NITRD should "rebalance our research portfolio to encourage greater innovation and risk taking."

Another area of emerging need and opportunity is cyber security, as pointed out in a 2005 report from the President's Information Technology Advisory Committee[10] and, more recently, in a 2009 report from the Government Accountability Office.[11] Addressing the Nation's pressing needs in cyber security will require a broad, coordinated effort. Agencies such as DARPA that have invested significantly in cyber security can play a key role by broadening to the larger academic research community, thereby achieving what PITAC referred to as "fundamental research on civilian cyber security." To first approximation, aside from NSF the funding for cyber security research at universities has been too modest relative to the threats that the Nation faces. I suggest that **an explicit focus on cyber security that coordinates the efforts of multiple agencies and enables full participation by academia should be considered.**

An area that deserves special attention, as pointed out in the 2007 PCAST assessment, is to **increase the pipeline of talent in IT to meet both the demands of industry as well as future IT research, with a particular focus on women and under-represented groups.** Simply put, today we are not attracting enough people into computing education and careers, and this problem is particularly acute with under-represented groups. Recently, in a letter written by the ACM and joined by CRA and the National Center for Women & Information Technology, we urged that this crucial talent pipeline be strengthened by expanding and coordinating existing efforts within the NITRD program. We believe this can be done in ways that also gain better leverage for these efforts. Four specific recommendations were:

- Promote computing education, particularly at the K–12 level, and increased exposure to computing education and research opportunities, especially for women and minorities as core elements of the NITRD program;
- Require the NITRD program to address education and diversity programs in its strategic planning and roadmapping process;
- Expand efforts at the National Science Foundation (NSF) to focus on computer science education, particularly at the K–12 level through broadening the Math Science Partnership program; and,
- Enlist the Department of Education and its resources and reach in addressing computer science education issues.

Each of these recommendations would **bring a federal focus to issues in computer science education at the K–12 level, enabling emerging concepts in "computational thinking" to make their way into the education of all Americans.**

---

[9] National Research Council. *Innovation in Information Technology.* National Academies Press. 2003. *http://www.nap.edu/catalog.php?record_id=10795&page=5*

[10] President's Information Technology Advisory Committee. *Cyber Security R&D: A Crisis of Prioritization.* 2005. *http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf*

[11] General Accountability Office. *National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture.* GAO–09–432T, March 10, 2009, *http://www.gao.gov/products/GAO-09-432T*

Question 4: *Does the legislation effectively implement the PCAST recommendation for support of large-scale, multi-disciplinary research and development projects? What are the most appropriate mechanisms to undertake these projects? Are the requirements for these projects sufficient to encourage industry/university partnerships?*

It is encouraging to see that the legislation explicitly recognizes the importance of large-scale, multi-disciplinary research and development projects, and provides for direct support for such activities. Key to the role that IT plays in enabling innovation is the role of the IT R&D ecosystem that enables innovation. A 1995 study by the National Research Council[12] describes 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." That study, and a subsequent 1999 report by the President's Information Technology Advisory Committee[13] ,emphasized the "spectacular" return on the federal investment in long-term IT research and development. Indeed, a 2003 NRC study[14] identified 19 multi-billion-dollar IT industries—industries that are transforming our lives and driving our economy—that were enabled by federally sponsored research.[15] This year, National Research Council completed a study on *Assessing the Impacts of Changes in the IT R&D Ecosystem.*[16] The study makes four recommendations:

1. Strengthen the effectiveness and impact of federally funded IT research.
2. Remain the strongest generator of and magnet for technical talent.
3. Reduce friction that harms the effectiveness of the U.S. IT R&D ecosystem, while maintaining other important political and economic objectives.
4. Ensure that the US has an infrastructure for communications, computing, applications, and services that can enable U.S. IT users and innovators to lead the world.

Significant progress towards encouraging large-scale, multi-disciplinary research this can be obtained by launching a second Information Technology Research (ITR) program in the NSF CISE Directorate, as recommended in the 2007 PCAST assessment. Between FY 2000 and FY 2004, the original ITR program added $218 million to what is today (FY 2008) an NSF CISE budget of $535 million which constitutes 86 percent of the federal support for academic research in computer science. (ITR also added $77 million to other Directorate's budgets.) ITR was managed as a distinct program, and had a particularly important impact in encouraging *longer-term, larger-scale, multi-disciplinary* IT R&D focused on *areas of particular opportunity*.

In summary, networking and information technology research and development is the cornerstone of America's future infrastructure and economic competitiveness. By

a. encouraging broader agency support for advancing IT R&D,
b. restoring investment in long-term, stable university-based research in IT,
c. balancing core and multi-disciplinary research activities,
d. increasing the pipeline of IT talent, especially from under-represented groups,
e. bringing federal focus to K–12 computer science education, and
f. launching a second NSF ITR program,

we can ensure U.S. leadership in IT R&D and contribute real solutions to many of the challenges facing our nation today. Federal investments, as enabled by the NITRD program, are paid back many times as the field's ability to create effective university-industry partnerships and transferable technologies has shown time and again. The proposed legislation makes much-needed changes to the NITRD program and will help us meet many of the challenges facing us today. In order for the U.S. to remain the world's leader, further improvements will be needed; the proposed legislation makes a good first step.

[12] National Research Council. *Evolving the High-Performance Computing and Communications Initiative to Support the Nation's Information Infrastructure.* National Academies Press. 1995. *http:;%www.nap.edu/catalog.php?record_id=4948*

[13] President's Information Technology Advisory Committee. *Information Technology Research: Investing in Our Future.* 1999. *http://www.nitrd.gov/pitac/report/pitac_report.pdf*

[14] National Research Council. *Innovation in Information Technology.* National Academies Press. 2003. *http://www.nap.edu/catalog.php?record_id=10795*

[15] See *http://books.nap.edu/openbook.php?record_id=10795&page=5*

[16] See *http://books.nap.edu/openbook.php?record_id=12174&page=R1*

Mr. Chairman, thank you and this committee for your interest in the future of the NITRD program and its importance to innovation and U.S. competitiveness. Thank you for your time and attention. At the appropriate time, I would be pleased to answer any questions you might have.

About the Computing Research Association

The Computing Research Association (CRA) is an association of more than 200 North American academic departments of computer science, computer engineering, and related fields; laboratories and centers in industry, government, and academia engaging in basic computing research; and affiliated professional societies. CRA's mission is to strengthen research and advanced education in the computing fields, expand opportunities for women and minorities, and improve public and policymaker understanding of the importance of computing and computing research in our society.

The CRA Board of Directors and its Executive Officers are a distinguished group of leaders in computing research from academia and industry. The board is elected by CRA's member organizations. Representatives from each of our affiliated professional societies are also appointed to serve on the board. CRA relies on the volunteers that serve on its committees, as well as its professional staff, to carry out its programs.

CRA's Members:

Industry Lab/Center Members

Microsoft Corporation
IBM Research
Sun Microsystems
Argonne National Laboratory
AT&T Labs
Avaya, Inc.
CA Labs
Computer Science Research Inst.
FX Palo Alto Laboratory
Google
Hewlett-Packard Company
IDA
Intel Corporation
Lawrence Berkeley Nat'l Lab
Los Alamos National Laboratory
Mitsubishi Electric Research Labs
Nat'l Center for Atmospheric Res.
NEC Laboratories America, Inc.
Ricoh Innovations, Inc.
SCI Institute
SRI International
Telcordia Technologies

Academic Members

Arizona State University
Auburn University
Binghamton University, SUNY
Boston College
Boston University
Bowling Green State University
Bradley University
Brandeis University
Brigham Young University
Brown University
Bucknell University
California Institute of Technology
Carnegie Mellon University
Case Western Reserve University
City University of New York
Clemson University
Colgate University
College of Charleston
College of William & Mary
Colorado School of Mines
Colorado State University
Columbia University
Concordia University
Cornell University
Dalhousie University
Dartmouth College
DePaul University
Drexel University
Drexel University
Duke University
Emory University
Florida Institute of Technology
Florida International University
Florida State University
George Mason University
George Washington University
Georgetown University
Georgia Institute of Technology
Georgia Institute of Technology
Georgia Institute of Technology
Georgia State University
Grinnell College
Harvard University
Harvey Mudd College
Smith Colleges
Hofstra University
Illinois Institute of Technology
Indiana University
Indiana University
Iowa State University
Iowa State University
Johns Hopkins University
Juniata College
Kansas State University
Kent State University
KAIST
Lafayette College
Lehigh University
Louisiana State University
Loyola University, Chicago
Marquette University
Marymount University
MIT
McGill University
Memorial Univ. of Newfoundland
Miami University
Michigan State University
Michigan Technological Univ.
Mississippi State University
Montclair State University
National University of Singapore
Naval Postgraduate School
New Mexico State University
New Mexico Tech
New York University
North Carolina State University
North Dakota State University
Northeastern University
Northwestern University
Nova Southeastern University
Oakland University
Ohio State University
Oklahoma State University
Old Dominion University
Oregon State University
Pace University
Pennsylvania State University
Polytechnic University
Pomona College
Portland State University
Princeton University
Purdue University
Regis University
Rensselaer Polytechnic Institute
Rice University
Rochester Institute of Technology
Rutgers University
Saint Louis University
Santa Clara University
Simon Fraser University
Singapore Management University
Southern Illinois University
Southern Methodist University
Southern Polytechnic State Univ.
Stanford University
Stevens Institute of Technology
Stony Brook University, SUNY
Swarthmore College

Syracuse University
Temple University
Texas A&M University
Texas A&M Univ., Corpus Christi
Texas State University
Toyota Technological Inst
Tufts University
Union College
University at Buffalo, SUNY
Univ. of Alabama, Birmingham
Univ. of Alabama, Tuscaloosa
University of Alberta
University of Arizona
University of Arkansas
Univ. of Arkansas at Little Rock
University of Bridgeport
University of British Columbia
University of Calgary
University of California, Berkeley
University of California, Davis
University of California, Irvine
Univ. of California, Los Angeles
University of California, Riverside
Univ. of California, San Diego
Univ. of California, Santa Barbara
Univ. of California, Santa Cruz
University of Chicago
University of Cincinnati
University of Colorado, Boulder
University of Delaware
University of Georgia
University of Hawaii
University of Illinois, Chicago
U. of Illinois, Urbana Champaign
University of Iowa
University of Kansas
University of Kentucky
Univ. of Louisiana at Lafayette
University of Maine
University of Maryland
Univ. of Maryland, Baltimore Co.
Univ. of Massachusetts, Amherst
Univ. of Massachusetts, Boston
Univ. of Massachusetts, Lowell
University of Miami
University of Michigan
University of Michigan, Dearborn
University of Minnesota
University of Mississippi
University of Missouri, Columbia
Univ. of Missouri, Kansas City
University of Montana
University of Nebraska at Omaha
University of Nebraska, Lincoln
University of Nevada, Reno
University of New Brunswick
University of New Hampshire
University of New Mexico
Univ. of N. Carolina, Chapel Hill
Univ. of N. Carolina, Charlotte
University of North Dakota
University of North Texas
University of Notre Dame
University of Oklahoma
University of Oregon
University of Pennsylvania
University of Pittsburgh
University of Puget Sound
University of Rochester
University of South Alabama
University of South Carolina
University of South Florida
University of Southern California
University of Southern California
University of Texas, Austin
University of Texas, Brownsville
University of Texas, Dallas
University of Texas, El Paso
University of Toronto
University of Utah
University of Virginia
University of Washington
Univ. of Washington, Tacoma
University of Waterloo
University of Wisconsin, Madison
Univ. of Wisconsin, Milwaukee
University of Wyoming
Utah State University
Vanderbilt University
Villanova University
Virginia Tech
Wake Forest University
Washington State University
Washington Univ. in St. Louis
Wayne State University
Williams College
Worcester Polytechnic Institute
Wright State University
Yale University
York University

Affiliated Professional Society Members

American Association for Artificial Intelligence
Association for Computing Machinery
Canadian Association of Computer Science
IEEE Computer Society
Society for Industrial and Applied Mathematics
USENIX Association

BIOGRAPHY FOR PETER LEE

Peter Lee is the head of the Computer Science Department at Carnegie Mellon University. He joined the CMU faculty in 1987, immediately after completing his doctoral studies at the University of Michigan.

Peter Lee is an active researcher, educator, administrator, and servant to the academic community. His research contributions lie mainly in areas related to the foundations of software reliability, program analysis, security, and language design. He has published extensively in major academic journals and international symposia, with several of his papers receiving "test of time" awards for their seminal contributions to the field. Peter Lee is the recipient of several research awards, including the ACM SIGOPS Hall of Fame Award, for the seminal contribution of "proof-carrying code" in computer systems research. He is an elected fellow of the Association for Computing Machinery.

As the head of the Computer Science Department, Peter Lee oversees one of the top computing research organizations in the world. In addition to its substantial research program, the department offers highly rated doctoral and undergraduate programs in computer science, with the Ph.D. program consistently ranked among the top in the U.S. Prior to assuming his current position, Dr. Lee was briefly the Vice Provost for Research. In this role, he provided administrative oversight and strategic guidance for the university's research activities, an enterprise that exceeds $400M in annual expenditures. From 2000 to 2004, Peter Lee was the Associate Dean for undergraduate programs in the School of Computer Science. During this period, Dr. Lee shepherded the rise of Carnegie Mellon's undergraduate computer science programs to national prominence, including a #2 ranking in the Gourman Report and a six-fold increase in the number of women enrolled.

Peter Lee is dedicated servant to the computing community. He is the incoming Chair of the Board of Directors of the Computing Research Association and chairs it's Government Affairs Committee. He also sits on the CRA's Education Committee. He is a member of the Computing Community Consortium Council, the National Research Council's Computer Science and Telecommunications Board, and the Defense Research Projects Agency's Information Science and Technology Board (where he is the Vice-Chair). Dr. Lee is called upon as an expert in diverse venues, including distinguished lectures at major universities, memberships on senior government advisory panels, corporate and university advisory boards, and court testimony (such as the Sun v. Microsoft "Java lawsuit"). He maintains the CSDiary weblog.

Chair GORDON. Thank you, Dr. Lee.

And now we will hear from Dr. Estrin.

STATEMENT OF DR. DEBORAH ESTRIN, DIRECTOR, CENTER FOR EMBEDDED NETWORKED SENSING; PROFESSOR OF COMPUTER SCIENCE AND ELECTRICAL ENGINEERING, UNIVERSITY OF CALIFORNIA, LOS ANGELES

Dr. ESTRIN. Thank you, Chairman Gordon and Ranking Member Hall for inviting me as well to testify before your committee on this important legislation. I am a Professor of Computer Science and Electrical Engineering at UCLA and the Founding Director of an NSF-funded multi-disciplinary Science and Technology Center for Embedded Networked Sensing, CENS, which was established in 2002. CENS' research agenda falls under the umbrella of cyber-physical systems.

After reviewing the NITRD legislation as requested, I concluded strongly that the bill addresses the key recommendations of the PCAST assessment and in the process addresses important needs of networking and information technology research communities. Moreover, the focus on cyber-physical systems will have an impact that extends into the country's commercial leadership, into the sciences and into public policy. In these oral comments I will emphasize two aspects of the legislation: the nature and importance of cyber-physical systems and the role of multi-disciplinary centers in realizing the research agenda.

Technological advances of the past two decades enable us to combine sensing, computation and wireless communication in integrated devices that can then be placed in situ up close to physical phenomena whether embedded in engineered systems such as the power grids and factory floor systems where they monitor power consumption and indications of malfunctioning components or embedded in natural systems such as depleted forests and water resources, measuring physical and chemical parameters such as temperature and pollutants, or in human systems such as devices worn on the body monitoring activity and physiological indicators. Cyber-physical systems are created through a synthesis of technologies including embedded sensing, sensor actuator controls, mobile sensing as well as human-computer interfaces. All of these will be advanced by the proposed NITRD focus on cyber-physical systems research and together they will bring us closer to the promise of revolutionary advances in our management of the physical world.

First, embedded sensing brings much needed understanding of physical processes and informs critical decisions. For example, the National Ecological Observatory Network, NEON, an MREFC project, is comprised of in situ sensing systems which capture and transmit measurements into web-based data management and geospatial modeling systems in real time. This powerful and programmable observing system will employ a broad spectrum of sensor types from the simplest temperature sensor to the highest resolution digital imagers. And it will greatly promote our understanding of ecosystems and thus inform critical issues in resource management and land-use policy.

Second, when sensing is combined with automated actuation in a tight control loop, we enter a new regime in which physical processes can be managed and manipulated at the time scale of the physical phenomenon, not just at the time scale which human beings are able and available to react. For example, systems that implement precise and localized management of water and power resources can manage real-time inputs and demands on the system and make adjustments to resource treatment and distribution in real time.

Third, mobile sensing presents tremendous economies to cyber-physical systems because by moving a sensor through an environment, you can achieve high spatial resolution measurements that are not achievable or affordable with fixed sensors alone. Mobility can take multiple forms, a Pan-tilt-zoom camera for both ecological and built environments or human-carried devices for personalized measurements of human exposure and interaction.

And fourth, most cyber-physical systems are part of larger systems with humans in the loop. They are designed to be used by humans as real-time interactive systems to inform both short-term and long-term decisions and actions. Moreover, the proximity of these systems to people raises the need to attend to privacy in their design, deployment and usage and this is another area in which government-funded research can contribute significantly.

So in summary of this first of my two points of my testimony, the proposed support for cyber-physical systems in the NITRD legislation will greatly enhance our ability to address the design challenges of high-impact physically coupled systems by supporting research in robust and reusable, scalable and validative components, algorithms and integrated subsystems. It will thereby enable broad-scale, powerful and programmable environmental observing systems.

I want to say a few words before closing about my second point, which is the role of multi-disciplinary research centers in realizing this vision. Multi-disciplinary research centers offer scope as well as scale and they require extended timelines in addition to increased funding. In my research center, CENS, the most important results have been iterative where we began by applying existing technology in an innovative manner to the application scientist observational needs and then based on the resulting experience identified the most important areas for the next phase of innovation. This style of work has great potential for serendipitous results where you end up in places you did not expect and having learned tremendously more in the process.

We have also found consistently that the nature of these applications in this multi-disciplinary iterative work attracts a wider range of students. We believe this is because the social utility is very evident and is naturally integrated into the design discussions. We speculated that this social utility would end up appealing and attracting more women to computer science, for example, and we were not disappointed. Our center averages consistently double the percentage of women involved in our programs relative to the rest of the department, and that is 30 percent as opposed to 12 percent.

Finally, multi-disciplinary centers can contribute significantly to collaborative agency programs where a technology creation agency could partner with a mission agency to help bridge the gap between funding of the basic ideas and early prototypes and systems that can actually be used and run through trials and exploration before commercialization. A good example of this would be a large-scale, let us say million-person mobile sensing system that supports preventative and chronic health management and research. Today's mobile phones can easily report activity, location and prompted user input such as pain, diet, medication and other self-reports and such a project coordinated between, for example, the NSF and mission-oriented needs of the NIH and the CDC could prototype and pilot a privacy-preserving, population-scale system that would drive innovation in privacy and security of electronic health records, data analysis infusion and computer-human interaction while also providing unprecedented data sets and an experimental platform for public health and epidemiological studies.

So finally in conclusion, cyber-physical systems cover a broad and important range of networking and information technologies and will be essential in meeting some of the key environmental, economic and quality-of-life challenges facing our nation and the world. A broadly focused cyber-physical systems research program in NITRD balanced between fundamental and applied projects, leveraging university, agency and corporate R&D efforts will go a long way towards ensuring the United States continues to hold a leadership position in this critical field.

Thank you, Mr. Chairman, for the opportunity to provide my testimony on this important issue. I am pleased to answer any further questions you might have as you and your colleagues on the Committee move the legislation forward.

[The prepared statement of Dr. Estrin follows:]

PREPARED STATEMENT OF DEBORAH ESTRIN

Personal Introduction

Thank you Chairman Gordon and Ranking Member Hall for inviting me to testify before your committee on this important legislation. I am a Professor of Computer Science and Electrical Engineering at UCLA, and the founding Director of an NSF funded Science and Technology Center for Embedded Networked Sensing (CENS), established in 2002. I was educated at MIT and experienced my early career at USC supported by the Defense Advanced Research Projects Agency (DARPA) and the National Science Foundation (NSF). During the past decade I became involved in multi-disciplinary work in an area that falls under the umbrella of cyber-physical systems. I also served on DARPA's Information Science and Technology Study Group (ISAT) and NSF's Computer and Information Science and Engineering (CISE) Advisory committees and currently sit on the National Research Council's Computer Science and Telecommunications Board (CSTB) and have participated in numerous studies over the years.

In the invitation to testify at today's hearing, Mr. Chairman, you asked whether I believe the legislation you have proposed will help ensure the Networking and Information Technology Research and Development program (NITRD) is positioned to help maintain U.S. leadership in networking and information technology. Having reviewed the legislation, I believe the bill addresses the key recommendations of the PCAST assessment, and in the process, addresses important needs of networking and Information technology research communities. I also believe that the focus on cyber-physical systems in the legislation will have an impact that extends into the country's commercial leadership, into the sciences, and into public policy.

In this testimony I will emphasize a few issues I think are key in responding to the questions you posed: cyber-physical systems; the importance of experimental, purpose-driven research and opportunities for cross-agency projects; and the importance of multi-disciplinary centers in realizing a research agenda and creating effective opportunities to attract and engage a more diverse student body in IT research.

The importance of NITRD and Cyber-Physical Systems

The Computing Research Association's Computing Community Consortium hosted a symposium last week here on Capitol Hill, where an all-star cast of computer scientists reviewed the importance of information technology and how the advances that are now essential to science, government and citizens, are a direct result of federal support for research, particularly from NSF and DARPA. I was pleased to be invited to participate.

In my session on "Computing Everywhere," we focused in particular on how computing extends beyond the processing and sharing of knowledge encoded in text and numbers, to direct measurement, management, and manipulation of physical phenomena.

We often hear how miniaturization and Moore's law[1] has enabled the growth, proliferation and scaling of computational capabilities. Our computing power has become exponentially more powerful over time as our devices become smaller and more powerful. So the computer that once occupied the back room, then moved to the desktop, now fits in our pocket, or can be embedded in sensor rich devices.

These developments enable us to combine sensing, computation and wireless communication in integrated devices, that can be placed in situ, up close to physical phenomena. Whether embedded in:

- Engineered systems such as power grids and factory floor systems monitoring power consumption and indications of malfunctioning components.
- Natural systems such as depleted forest and water resources, measuring physical (e.g., climate) and chemical (e.g., pollutants) parameters.
- Human systems such as devices worn on the human body monitoring activity and physiological indicators.

[1] Moore's Law is the projection that the number of transistors that can be placed on an integrated circuit will increase exponentially, doubling approximately every two years, that was first noted by Intel Co-Founder Gordon Moore in 1965 and has held true to the present day.

Across this wide array of applications, the ability to observe physical processes with such high spatial and temporal fidelity will allow us to create models, make predictions, and thereby manage our increasingly stressed physical world.

Cyber Physical Systems are created through a synthesis of technologies, including: embedded sensing systems, sensor-actuator control, mobile sensing, and human computer interfaces. All will be advanced by the proposed NITRD focus on cyber-physical systems research and **together** will bring us closer to the promise of revolutionary advances in our management of the physical world.

- **Embedded sensing** brings much needed understanding of processes and informs critical decisions. For example, the National Ecological Observatory Network (NEON) and Ocean Observing Initiative (OOI) MREFC projects are primarily embedded sensing systems in that they are comprised of in situ sensing systems which capture and transmit measurements into web-based data-management and geospatial-modeling systems, in real time. These powerful and programmable observing systems will employ a broad spectrum of sensor types (from the simplest temperature sensor, to highest resolution digital imagers), and will greatly promote understanding of ecosystem and ocean dynamics, and thus inform critical issues in resource management and land use policy. Similarly, in the context of observing systems for the built environment, transportation related embedded sensing systems, for example, are being installed along major roadways to capture real time traffic information and inform real-time driving patterns and longer-term planning.
- When sensing is combined with **automated actuation** in tight control loops, we enter a new regime in which physical processes can be managed and manipulated at the timescale of the physical phenomena, not just at the timescale on which human beings are able and available to react. For example, biomedical systems can measure physiological parameters and based on the readings automatically adjust drug dosage (e.g., insulin pump) or system function (e.g., prosthetics). Similarly, systems that implement precise and localized management of water and power also can measure real-time inputs and demands on the system, and make adjustments to resource treatment or distribution in real time.
- **Mobile sensing** presents tremendous economies to cyber-physical systems because by moving a sensor through an environment you can achieve high spatial resolution measurements that are not achievable with fixed sensors. Mobility takes multiple forms. Pan-tilt-zoom cameras are useful in both ecological and built-environment settings. Unmanned Arial Vehicles are emerging for practical use in surveying natural and urban settings. Vehicle-mounted sensors on public transportation vehicles, can capture data specific to traffic, but more generally can take advantage of the natural coverage that these vehicles provide to measure other parameters such as air quality. And finally, human-carried devices offer tremendous opportunity for individual and aggregate measurements related to human exposure and interaction. Mobility presents tremendous coverage benefits but does call for more sophisticated internal operation of the system.
- Most cyber-physical systems are part of larger systems with **"humans in the loop,"** operating on human timescales. For example, all of the cyber-physical applications described above require visualization of the observed data and physical system. They are designed to be used by human users as real time interactive systems to inform both short- and long-term decisions and actions. Moreover, in some cases, human assistance and augmentation is desired to contribute additional data feeds to the system that cannot be fully automated (e.g., laboratory based analyses of manually-collected samples). Finally, the proximity of these systems to people raises the need to attend to privacy in their design, deployment and usage, which is another area in which research can contribute significantly.

In summary, cyber-physical systems cover a broad and important range of networking and information technologies and are essential to meeting the key challenges facing the Nation, and the planet as a whole, including: the need for cleaner and more efficient manufacturing, transportation, and energy production and distribution; water treatment and conservation; personalized health management, treatment, and care; and preservation and recovery of key ecosystems and services. The proposed support for CPS in the NITRD legislation will greatly enhance our ability to address the design challenges of physically-coupled systems by supporting research in robust and reusable, scalable and validated components, algorithms, and integrated sub-systems to enable broad scale, powerful and programmable environmental observing systems.

Importance of federally funded research to U.S. leadership

Federally funded research is directly responsible for today's technologies and the technologies we'll deploy tomorrow. Indeed, the development of every major sub-sector of the IT industry bears the stamp of federally-supported research, usually research supported at U.S. universities In fact, perhaps the most important aspect of federally supported university-led research is that it generates both the ideas of tomorrow and the people necessary for turning those ideas into reality. These are the students and researchers who generate the ideas that will power the innovations of tomorrow.

One of the great success stories of federally funded research in information technology in my own research area has been the growth of entirely new sectors and phenomenally successful commercial companies in support of the use of computing everywhere. These are companies like Apple that has revolutionized the design of personal technologies, and Nokia that has proliferated sophisticated mobile technology around the world at such a rate that now there are over three billion cell phones and Nokia sold devices at the rate of 16 million per quarter in 2008. At the same time, the existence of this strong commercial sector has not lessened the need for federally funded research dollars. While these companies are spending, in some cases, considerable dollars investing in research and development, that investment is almost always focused on reasonably short-range development efforts—generally the next product cycle or two. Federal support, particularly at U.S. universities, is essential for the long-range research necessary to advance the field and enabling the game-changing technologies of the next 10–20 years.

Even if, and that's a big if, commercial investment in R&D was high enough to maintain a healthy flow of new, long- and mid-term technology innovation, the role of federal dollars would still be essential. One of the reasons it is so essential to maintain a healthy investment in publicly funded technology research is so that issues of public good, which cannot always be the primary drivers in a commercial enterprise, can shape our technology; not to prevent commercialization and private investment, but rather to promote it in a form that addresses externalities such as open interfaces and privacy preserving architectures. Moreover, innovation can be focused in areas that don't yet have established revenue streams or business models, such as aspects of ecosystems science, for example.

This research ecosystem I've described—the interplay between federal support for university research and commercial research and development efforts—has been, as the National Research Council declared back in 1995, "extraordinarily productive." But in order to keep it as productive as possible, it's important to keep it as finely tuned as possible. Balanced ecosystems are essential in nature, in our diets, in our financial portfolios, and in our research. Currently our research ecosystem is lacking balance on both ends of the research time horizon. On the one hand there is a need for more basic research that explores foundational algorithmic capabilities. On the other hand, there is also a need for bold, experimental, purpose-driven research with discovery that comes from synthesis, problem solving and use. Space missions and the Internet are both excellent examples of the latter approach. And much of the work funded under NSF's highly successful Information Technology Research (ITR) program, which ran from 2000 to 2004, had this latter quality.

While there is a need for far out, theoretical work that disconnects from constraints—indeed, the PCAST assessment concluded that the portfolio is currently imbalanced in favor of low-risk projects and that too many are small-scale and short-term efforts—there is also a need for work that explores applying what is possible now but on a grand scale and to grand problems. Such projects lead researchers to uncover the "interconnection between the pieces"—and not just between technologies, but between technology and people, and in the case of cyber-physical systems between technology and nature as well! This research offers further value added relative to commercial R&D when it serves non-monetized applications such as environmental monitoring and public health, thereby creative innovative technologies for the under-served markets, while providing the technologists with the integrative experience they can only get when their technology or system is deployed and used.

The role of multi-disciplinary research centers

Multi-disciplinary research centers offer scope, as well as scale, i.e., extended timelines in addition to increased funding levels. Multi-disciplinary research, by definition, requires that you have more people at the table, and also produces its most important results when there is enough time for the collaboration to iterate and thereby expand on its own findings. In my research center, CENS, the most important results have been iterative: where we began by applying existing technology in an innovative manner to the application scientist's observational science problem, and based on the resulting experience identified the most important areas for the next phase of innovation. Two key innovations from the center came about in this way—the use of mobile sensing to achieve high spatial resolution, and the development of smart cameras as "biological" sensors for flora and fauna. It was only by engaging in this collaborative iterative process between the application scientists and technologists that these innovative solutions emerged. This style of work has great potential for serendipitous results where you end up in places you did not expect, having learned tremendously more. Through this we have discovered other new opportunities for addressing pressing problems—for example, using the mobile phone as an instrument for personal and participatory sensing, e.g., for congestion-based pricing on highways, personalized and precise management of medication, and individualized behavior shaping to combat avoidable health care burdens such as obesity.

Education opportunities also flourish in centers. At CENS we developed a hands-on research experience for undergraduates and high school students interested in the application of information technologies to environmental and urban sensing. We have had tremendous success with the program. It has been a source of innovation within the research agenda, and has produced excellent students, many of whom decided as a result to continue their studies in graduate school, and who are demographically more diverse than the equivalent populations in their local engineering schools. However, we also learned that these programs scale up better than they scale down. With a core of coordinated programming and staffing you can support a wide range of projects and students. However if you support only a few students, we found that they do not get the same structured social setting for their research, without generally unsustainable Inputs from the supervising faculty and graduate students.

We have also found consistently that the nature of these applications attracts a relatively diverse student population—perhaps because the social utility is very self-evident and is explicitly a part of the design discussions. We speculated that this social utility would end up appealing and attracting more women and we were not disappointed—our CENS averages for women students are consistently double that of the rest of the school.

Finally, multi-disciplinary research centers in pursuit of cyber-physical systems and applications could contribute greatly to collaborative agency programs where a technology creation agency could partner with a mission agency to help bridge the gap between funding of the basic ideas and early prototypes, and systems that can actually be used and run through trials and exploration before commercialization:

- A good example of this would be a large scale, ~million-person, mobile-sensing system that supports preventative and chronic health management and research. Today's mobile phones can easily report activity, location, and prompted user input (e.g., pain, emotional state, and other self-reports). Such a project, coordinated between the NSF and the mission oriented needs of NIH and CDC, could prototype and pilot a privacy-preserving, population-scale system that would drive innovation in privacy and security of electronic health records, data analysis and fusion, and human computer interaction, while also providing unprecedented data-sets for public health and epidemiological studies.

Another example opportunity would be for multiple user agencies with overlapping needs to launch development of an innovative sensor type that is not being brought to market because revenue streams are not large enough to justify the capital investment by commercial enterprise.

- Development of specific sensors for environmental monitoring is a good example. There is not a large enough commercial market to drive development and production of miniaturized, high precision, nitrate sensors for example which are critical to both ground water testing systems, coastal margin ecosystem health, and terrestrial ecosystem carbon cycle characterization. In this case, a coordinated effort between the NSF and the mission-oriented needs of EPA, USGS, NOAA, USDA to develop and produce such a sensor could have significant long-term ecological benefit to the country.

Conclusion

I was pleased to see the inclusion of cyber-physical systems as an area of emphasis in the PCAST assessment of 2007 and I'm pleased to see its inclusion in the NITRD legislation under discussion today. As I noted above, cyber-physical systems cover a broad and important range of networking and information technologies and will be essential in meeting some of the key environmental, economic, and quality of life challenges facing our nation and the world. A broadly focused cyber-physical systems research program in NITRD, balanced between fundamental and applied efforts and leveraging university, agency, and corporate research and development efforts will go a long way towards ensuring that the United States continues to hold a leadership position in this critical field.

Thank you, Mr. Chairman, for the opportunity to provide my testimony on this important issue. I am pleased to answer any further questions you might have as you and your colleagues on the Committee move this legislation forward.

BIOGRAPHY FOR DEBORAH ESTRIN

Deborah Estrin is a Professor of Computer Science and Electrical Engineering at UCLA. She holds the Jon Postel Chair in Computer Networks, and is Founding Director of the National Science Foundation funded Center for Embedded Networked Sensing (CENS). CENS' mission is to explore and develop innovative, end-to-end, distributed sensing systems, across an array of scientifically and socially relevant applications, from ecosystems to human systems. Estrin is currently exploring Mobile Personal Sensing systems that leverage the location, acoustic, image, and attached-sensor data streams increasingly available globally from mobile phones; with particular emphasis on human and environmental health applications and on privacy-aware architectures. Estrin's earlier research addressed Internet protocol design and scaling, in particular, inter-domain and multi-cast routing. She received her Ph.D. in 1985 from MIT and her BS in 1980 from UC–Berkeley, both in EECS. Estrin currently serves on the National Research Council's Computer Science and Telecommunications Board (CSTB) and was previously a member of the NSF National Ecological Observatory Network (NEON) Advisory board, the NSF CISE Advisory Committee, and DARPA–ISAT. Estrin was selected as the first ACM–W Athena Lecturer in 2006 and was awarded the Anita Borg Institute's Women of Vision Award for Innovation in 2007. She was elected to the American Academy of Arts and Sciences in 2007 and to the National Academy of Engineering in 2009. She is a fellow of the IEEE, ACM, and AAAS and was granted Doctor Honoris Causa from EPFL in 2008.

DISCUSSION

Chair GORDON. Thank you, Dr. Estrin. I agree, it is the discovery that you are not expecting that is oftentimes more important than the breakthrough that you originally sought.

Dr. Lee, I want to go back a little bit to your discussion about what is going on around the rest of the world and the competition that we might have, and you say Europe is really the center or where most of the research is going on outside the United States?

Dr. LEE. Yes, that is correct.

Chair GORDON. And are there any lessons learned—what they are doing that we need to be incorporating? And typically what they will do is, they will have more of a focus on, you know, breakthroughs in two or three different areas. Is that what they are doing there, and if so, where?

Dr. LEE. Yes. So indeed, one model that I think is very interesting, particularly in the European efforts in hybrid systems, which is roughly speaking their analog to cyber-physical systems, they have a very focused mission orientation in some of their research programs.

Chair GORDON. Is this E.U. or is this a particular country?

Dr. LEE. This is E.U., and in the—so, for example, in one major initiative, they would like cyber-physical systems or hybrid systems that would eliminate any possibility of collisions in the high-speed rail systems throughout Europe and so this provides a grand challenge framework but associated with those large programs are subprojects that provide sustained, long-term basic research funding.

Chair GORDON. And what is their vehicle for collaboration?

Dr. LEE. So they have multi-university research teams.

Chair GORDON. It is university based. Does industry play much of a role?

Dr. LEE. Industry does play a role, and in fact, in the large mission programs, industry is required to play a role but they are in our parlance sub-awards to the prime awards that are given to the university-based teams. This allows the university teams to really think beyond the leading edge but still provide a long-term partnership with industry to provide a smoother or a greased track, so to speak, for technology transfers.

Chair GORDON. I want to pose a question to all of you. The legislation calls for an industry/university task force to explore collaborative research models for cyber-physical systems. Are there other research areas where public-private partnerships would be particularly appropriate and what characteristics are necessary for a successful industry/university collaboration in networking and IT? Dr. Estrin, do you want to start us off?

Dr. ESTRIN. Certainly. I think successful efforts—everyone needs to be getting something out of the process to get true engagement. An interesting example of something like that is where industry has the capacity to construct things, let us say, a highly sensitive sensor type that is needed by a broad range, but they are not going to do it on their own because the commercial market doesn't yet exist but perhaps there are truly needs for such a sensor—pose it—in health, in ecology, in cleanup of contaminated water, and so by bringing together researchers, agencies that have a need, an industry that has the capacity but wouldn't otherwise produce such a device because the commercial market doesn't yet exist, you can bring those three together in very successful ventures and the number of the things, projects I would foresee would have that similar quality where you bring in the capacity of the commercial enterprise but focusing on problems that are needed for public good that don't yet have the market to have them do it on their own.

Chair GORDON. And what about the intellectual property? I mean, does that get worked out between the universities and industry relatively smoothly or what happens there?

Dr. ESTRIN. In my experience, that works out even more smoothly when the government is involved from the beginning because it keeps people from even thinking about trying to be greedy in the shorter-term. In the end we found first to market understanding the technology is the way to go. We benefited so much from open work. So we do all of our work open and without IP protection. Since this is for the public good, you would want——

Chair GORDON. Is that fairly well universal here in the United States, that attitude?

Dr. ESTRIN. It is not—I think it is broad enough and people have seen enough success from it that it is certainly a practical thing to pursue, an important role for government.

Chair GORDON. Dr. Lee, do you want to add anything there?

Dr. LEE. Yes. I think that many of the major challenges that computing research is really poised to contribute to, and let me just mention three: cyber security, energy and health care. These are sources of grand challenge, problems that university and IT-based research alone won't be able to solve and so partnerships, particularly partnerships with stakeholders and typically these stakeholders would often be industrial organizations, seem absolutely crucial. I would like to emphasize again though that universities, if we are looking at beyond the leading edge of technology, universities leading in this are absolutely crucial, and I would just bring your attention to the last year's DARPA urban challenge where the top three winners of the DARPA urban challenge robot race were in fact university teams that had significant industry support but the universities were leading.

Chair GORDON. Dr. Greer, do you want to conclude on that topic?

Dr. GREER. A couple of things I would add to the comments you already heard. The characteristics of successful efforts are really twofold. All involve bring their capabilities to the table and that all realize real value from the interaction. Those are the key issues that have to be addressed. In addition to the areas Dr. Lee described, the whole area of software development, design and engineering is a rich one for multi-sector collaboration, in fact, probably requires that networking capability, security, reliability. The vast majority of the networking capability around the globe belongs to the private sector, certainly in this country, than to the government. There are examples of effective cooperation of this type. The Semiconductor Research Corporation is an example of a consortium where it provides neutral ground for all the parties to reach agreement, for example, a common legal framework which everybody who wants to participate has got to buy into, so that I think is another important value.

Chair GORDON. Thank you, Dr. Greer.

Mr. Hall is recognized for five minutes.

Mr. HALL. I thank you, Mr. Chair.

Dr. Greer and Dr. Lee, are all of the federal agencies involved with NITRD pulling their, what we call their weight in this? What agencies could be doing more and in what area, and whether or not you believe it is a function of funding or is something else involved? Dr. Greer, do you want to take a shot at that first?

Dr. GREER. In my written testimony in the appendix is the list of member agencies and participating agencies. That is a list of 28 federal agencies all told. That is a remarkable set of federal agencies willing to participate in the program. I think that is a very strong signal that there is broad interest. The member agencies are the ones that contribute to our budget. Again, there are 13 of those. Our experience is that the networking and information technology issues touch on the missions of all of the federal agencies in one form or another and so we encourage their participation and actively seek it as well.

Mr. HALL. Well, is that—are they listed because they are participating, the 28?

Dr. GREER. That is right. They are listed because they have on the left-hand side the ones that contribute to the NCO budget, on the right-hand side those that participate in other ways in the NITRD program activities.

Mr. HALL. And are there other federal agencies that are involved that could also be on that list?

Dr. GREER. I certainly think—as I said, almost all federal agency missions touch on this and I think part of our responsibility is to find those areas where agencies not now participating could realize value from participating.

Mr. HALL. I guess I will ask all witnesses whether or not the draft version of the legislation that is before us today helps to achieve an appropriately balanced portfolio, and if not, what is missing or what has been given too much attention? Dr. Greer, do you want to take a shot at that again?

Dr. GREER. Sure. Let us take one specific example, cyber-physical systems. As Dr. Estrin has eloquently pointed out, that touches on a very broad range of issues and even the definition of a cyber-physical system ranges from a chip in your car to the National Ecological Observatory Network, quite a range of things. The software for achieving those capabilities, the reliability issues, networking, all of those things go into realizing success in the area of cyber-physical systems and so an important issue is not to view them as isolated from all of the challenges across the networking information technology landscape but as one of the key priority and goal areas in that landscape.

Dr. LEE. I have one comment.

Mr. HALL. Dr. Lee.

Dr. LEE. Yes. Thank you. I think on the subject of balance, one area that perhaps could use more emphasis, I think the legislation does very well in emphasizing large-scale multi-disciplinary research and that is in response to the PCAST assessment. We shouldn't forget though that for all of the wonderful technologies that we see, there is literally an iceberg, a gigantic amount of core research in fundamental algorithms and technologies, and that emphasis on the core I think should have equal weight in the legislation.

Mr. HALL. Dr. Estrin, you gave a very detailed and inclusive opening statement. Do you have anything to add to what either of these gentlemen have said, and if something is missing, what's missing, and if something is given too much attention, what is, and if something is not given enough attention, what is it?

Dr. ESTRIN. I will be brief. As was mentioned in the opening statements, I think language about security and privacy would belong and would be a great addition.

Mr. HALL. About a brief an answer as I have ever gotten out of anybody. I yield back. Thank you, Mr. Chair.

Chair GORDON. Thank you, Mr. Hall. Since you have got a little bit of time left, Dr. Greer, could you finish up on your question? You were saying there needs to be more outreach to other agencies. How would you suggest that—you know, who determines where they are and how should that outreach be made?

Dr. GREER. Of course, the legislation that this committee has provided says that the President and the Director of OSTP decide who in the end is a member of the NITRD program so there is——

Chair GORDON. Just in case they were busy that day, I mean, what would you—you know, how would we do this internally?

Dr. GREER. And what we do at the National Coordination Office is, we go to our agency counterparts, explain the role of the NITRD program, its value to the agencies, identify appropriate points of contact and start that dialogue, invite them to our meetings, share our reports with them.

Chair GORDON. Okay. I see. Thank you.

Ms. Woolsey is recognized.

Ms. WOOLSEY. Thank you, Mr. Chair, and thank you to these wonderful witnesses. You have each said something about the ability of the United States to lead in science, math, technology, information technology in particular, that we have to have an educated workforce. So my question and we will go right down the line, how are we doing? And there are three Members on this committee, Congressman Wu, Dr. Ehlers and myself who are senior Members on the Education and Labor Committee as well, so my question, what can we be doing better to encourage an increase for the recruitment and the education of women and minorities in particular but in general all individuals interested in this field that is so important to us? And finally, where does it start in the education system? Does it start at the Ph.D. level or does it start in the 8th grade or the 6th grade? So we will start with you, Dr. Estrin, because actually we want—I am the author of Go Girl, which encourages young girls from the 8th grade on to stay involved in science, math and technology and we are going to have a hearing in my committee and I want you to be one of the witnesses. Let us start from you and go up the stream from there.

Dr. ESTRIN. I am delighted this issue is being taken so seriously, and certainly a Ph.D. is far too late. We have far too few people available in the pipeline by then. We must start earlier. Eighth grade is just about right. Of course, we need excellent childcare, we need good prenatal nutrition, we need everything that feeds up to the 8th grade but 8th grade is about the time that these young people start forming their ideas about what they want to do. Something we have been trying to do is put an authentic face on information technology, explaining that it is not just this transparent set of mechanisms that happened behind your screen but rather it is a way to help save the planet, help save your community, and I have no formal evidence on that subject, but as I said, many people who are entering and selecting careers who might otherwise select to become doctors and now we have greater than 50 percent in pre-med in medical schools who are women and our intention is to draw some of those bright, engaged committed individuals from that community.

And finally, the same thing holds when you look at first-generation students becoming the first generation to get college degrees. There again tends to be a commitment to the world, to their community and they want something and they are on the front lines doing that. And certainly information technology innovations are really very much about that.

Ms. WOOLSEY. Thank you.

Dr. Lee.

Dr. LEE. Thank you very much for this question. It is really an issue that has caused a great deal of anxiety, I would say, in the academic research community. I believe and many of my colleagues believe that computational thinking is necessary for any educated person in the same way that mathematical thinking or global thinking is becoming necessary for any educated person in our society, and this really has to start, I believe in the K through 12 system and maybe the 8th-grade level is about right. The National Science Foundation actually has begun a number of important initiatives. One that I would call attention to is the Math Science Partnership Program, and there are ideas to expand this in order to improve K through 12 computing education, and this would undoubtedly increase access and participation by women and minorities further upstream.

Ms. WOOLSEY. Thank you. Do I have time for Dr. Greer?

Chair GORDON. Certainly.

Dr. GREER. Very quickly, I would say that that this is one of the largest challenges to the NITRD landscape and my agency colleagues agree. It should be a centerpiece of our strategic plan. It should address the entire pipeline including curricula that are inspiring, that put science in the computer science curriculum, that show the opportunity for IT innovation to benefit people, individuals and our society as a whole and teachers who are prepared to engage students on that ground.

Ms. WOOLSEY. Before turning the microphone over, I have to be clear. I don't think we start teaching math in the 8th grade. I just know that by the 8th grade we know there are kids that are very talented that we want to keep in the system. Thank you very much.

Chair GORDON. Ms. Woolsey, your leadership in helping pass the America COMPETES will help move this ball down the field very much.

Ms. WOOLSEY. That is true. Thank you.

Chair GORDON. Dr. Roscoe Bartlett was here a little bit earlier, and in talking with him, he mentioned that his son, who he claimed was smarter than him and even smarter than his mother, which was apparently even a greater accomplishment, is a graduate of Carnegie Mellon and was very complimentary of what you do there.

Mr. Akin is recognized.

Mr. AKIN. Thank you. Mr. Chair, a couple of questions. They are a little bit related. The first is, with the proposal before us, do we have the adequate mechanisms to ensure that patent rights and national security, particularly the patent right piece is the first part of my question, is that—because we are doing a lot of sort of network types of development. Do we still protect patent rights appropriately?

Dr. GREER. Clearly that is a challenge in the evolving IT landscape and I think it is one that this Congress will need to consider. For the most part, it is outside the portfolio of the NITRD program; it is cooperation on R&D, but it surely plays into our ability to interact with the academic and commercial sector, a very important part of what we need to be able to do. So I think there are major challenges here that constrain progress.

Mr. AKIN. I think my next question is a bigger one and a harder one because one of my other committee assignments is on the Armed Services Committee, and we have taken a look at sort of unique forms of warfare and one of the most threatening and one that we appear to be largely unprotected against is the whole hacking into networks. I am not a whiz on computers although I used to work for IBM but my son is with the Marine Corps and he is a communications guy and he said we are absolutely wide open in this area. My understanding is, there are hundreds or even thousands of attacks every day from China directed toward our information systems and hacking into them. One rather big situation I think was in the news. It was two days ago or so in a number of different countries where computers that had very sensitive information had been infiltrated with software which was downloading all of this sensitive information and it was tracked back to China, which is no big surprise. Are we doing enough in that security because the hearings that I held as a Subcommittee Chair indicated that there is good news and bad news. The good news is, we can hack into anybody's stuff. The bad news is, they can all hack into ours.

Dr. LEE. It is in fact I think imperative that we somehow find a way to bridge across classification levels in order to allow more university-based researchers to participate in solving this problem. As it stands now, many university researchers are really not able to effectively participate in those programs and that then ends up excluding a large amount of our technology base.

Mr. AKIN. So what you are saying is, is that there are some solutions that could help us in this area but because of the fact that they are coming from a university direction that it is hard for them to connect with things like the systems that we are actually using nationally?

Dr. LEE. That is right. To give a concrete example, can we access data for access patterns to apply the latest machine learning algorithms to help understand these attacks. Even access to data is now an issue.

Mr. AKIN. I don't totally understand what you are saying but you are saying that we have got more of this stovepipe stuff where one part of our Nation is not talking to another. We are not using all of the resources available to us. I gather that is what you are saying.

Dr. LEE. That is correct, sir.

Mr. AKIN. How would you then change that? Would you say that you would maybe put in some sort of a provision so that the Department of Defense would have more aggressive work with the— I know at the Naval Academy they do—you know, they have red team come in and hack and all that kind of stuff. My son just loved that. But are you saying more of those kinds of programs would be helpful?

Dr. LEE. I think that would in fact do quite a lot. There are some natural defenses that just come out of new networking core research, new research and operating systems and software but as it stands now, there is a virtual gulf that separates classified programs from open programs, and that gulf ends up creating a split personality, so to speak, in how we approach these cyber security problems.

Mr. AKIN. Thank you very much.

Thank you, Mr. Chair.

Chair GORDON. We should have had your son as a witness today.

Mr. AKIN. I bet he would have had some questions. I don't know about a witness.

Chair GORDON. Dr. Griffith is recognized for five minutes.

Mr. GRIFFITH. Thank you, Mr. Chair. I have a question that hopefully you can shed some light on. At what level of the cell can you introduce this technology? At what level of the organism, when we are talking about health care, can you begin to measure? Can you measure outside the cell membrane, nuclear membrane? Are you down into the DNA, RNA? I know that sequencing was critically important in your area or it was critically important to us, but where are we now in general? Anybody can answer that.

Dr. LEE. Well, this is a very large question. In fact, there is ongoing information technology research that is literally trying to treat DNA sequences as computer code, literally programming DNA sequences in order to understand from the ground up exactly what all of these things mean, and that is kind of a bottom-up approach from actually the top-down approach of looking at natural organisms, so we are very, very far down into the biochemistry today.

Mr. GRIFFITH. Thank you.

Yes, please.

Dr. ESTRIN. So in the laboratory and even laboratory-based analyses, again, very far down that path, in terms of worn systems, systems that you might wear all the time, current state of technology isn't there. You are measuring higher-level physiological, perhaps measuring blood glucose, perhaps capturing other physiological parameters. Those are actually quite easily accessible now whereas the more detailed DNA analysis is happening through collected samples and then in the laboratory. But these things advancing together help science in understanding of health tremendously because you can do that analysis in the lab but understand the exposures that people have had during the course of their everyday life.

Mr. GRIFFITH. I think it is a great selling tool, by the way, for young students to know that the advances in our computer technology have led to incredible advances in the care of patients, and I think that is attractive to them and it attracts them in, just as the greening of America or saving our ecosystem, so we appreciate you all being here. Thank you.

I yield back my time.

Chair GORDON. Thank you, Dr. Griffith.

Let us see. Mr. Hall says he doesn't have any questions at this time. So Mr. Davis, you are recognized for five minutes.

Mr. DAVIS. Mr. Chair, thank you very much. I will be very brief. As I heard the questions engaging in those back and forth and our concern about China being able to tap into our most sensitive systems that we have and find information, obviously we can do the same thing but do you see any way where we can ever prevent that? As we talked about the information superhighway, the highways in my district are interstates so you go both ways on them. I am just wondering, is there any way that we can perfect—that we would be able to block out with a certainty, that no one would be able to tap into our information?

Dr. LEE. So thank you for that question. In fact, today's Internet, just to take that as one key part of our information technology ecosystem, was designed to be completely open, to be that interstate that allows free traffic in all directions literally without even any kind of traffic control. This was fine in the early going. We have come to depend on it now and it is well past time to rethink what the next generation Internet should be, and in fact, there are concepts on the drawing boards that would provide large test beds to experiment with new architectures for the Internet that could in fact be much more secure.

Dr. ESTRIN. I would like to add a comment. Having been around in those early days as the Internet was being designed in that very open process, some people look back and say that was a mistake. I think of it a little bit more as, you take a child, you introduce them in childcare, they start to be exposed, you know, to viruses and such things and they build up some antibodies. You don't keep them in a bubble. And in that process of having the Internet open and accessible, we have started to develop a stronger set of ideas of how you begin to protect yourself from these attacks and you—I don't know that we will see the day that we will be completely immune but I think we can be much better in terms of our treatment of addressing these kinds of viruses and infections and building healthier immune systems, if you will, for our systems. I would just like to say that a critical component of that is that we build systems whose security measures are actually usable by everyday people. A lot of the technology that ends up in critical government parts of the systems comes from the commercial side because it is less expensive, it has so much functionality to it, and so it is very important for our national security that our commercial and consumer information technology systems are built with important and the latest security ideas and that those security ideas are actually usable, that the configurations and the defaults are ones that everyday people can do the right thing and the protective thing because that technology ends up coming back into our national security systems.

Mr. DAVIS. So in essence you are saying in the near future there is a possibility, a probability, likelihood that we will be able to protect our most sensitive information to keep someone else from tapping into it, either of you?

Dr. ESTRIN. I think we will be able to do better and I don't see that as being something that is an absolute guarantee. We always have to remain vigilant.

Mr. DAVIS. Thank you, Mr. Chairman. I yield back my time.

Chair GORDON. Mr. Davis, Dr. Bartlett has been out consulting with his son for questions so you are recognized for five minutes.

Mr. BARTLETT. Thank you. I am sorry that I couldn't have been here for your testimony and the discussion. I worked eight years for IBM Corporation. As I mentioned to Dr. Lee, my youngest son, youngest of 10, chose to go to his university for his doctorate, which was ostensibly in chemical engineering but he went there because his interest is in computers and they hired him at Sandia Labs because of his expertise in computers. I have a growing concern that we are becoming too dependent on computers. They now are involved in almost everything we do. When the hacker comes in, he wants you to know that he broke into your house so he pulls out the dresser drawers and strews the stuff all over the floor so that you know he was there. When the really bad guys come to your house and break in, they don't even want to disturb the dust on the dresser. They don't want you to know they were there. Several years ago—I am senior Member on the Armed Service Committee. Several years ago we commissioned several of our people to pretend that they were bad guys and see if they could break into our military computers. They did that 3,000 times. We caught them twice. Now, we are much wiser because of that but so are the bad guys, when they make mistakes and they figure out what they need to do next time so as not to make the mistake. I have a growing concern that they are just testing us with the viruses and the worms that they put in our computers now and I am concerned that in the operating systems, which I think we have trouble determining whether they are germ-free, that there could be a sleeper there that becomes active only with a big ramp-up in activity which is an emergency when you really need them. Shouldn't we have some redundancy in our society? Today we have essentially no redundancy. If the computers are down—and one thing that would bring all of our computers down is a single nuclear weapon detonated 300 miles high over Iowa or Nebraska and the Russian generals tell us that would produce 200 kilovolts per meter, which is 100 kilovolts per meter at the margins of our country. That of course would fry all of our microelectronics so you are essentially in a world in which the only person you can talk to is the person next to you, unless you happen to be a ham operator with a vacuum tube set, a million times less susceptible. And the only way you can go anywhere is to walk unless you happen to have an Edsel or a similar kind of car. Shouldn't our society have some sort of redundancy? When something is really, really important in our military, we always build in redundancies so if we lose the primary, we still can function. We can't function without computers, can we? Shouldn't we have a redundancy?

Dr. LEE. Congressman Bartlett, let me start by saying that your son, congratulations on his accomplishment, and I should say that I applied to Carnegie Mellon hoping to do my own Ph.D. studies there and was not admitted, so I am very impressed with your son.

So indeed, I think that we are facing some significant challenges as you say, and the redundancy is the most simple thing that we could imagine doing. Indeed, Wall Street uses redundant systems for precisely the reasons that you——

Mr. BARTLETT. Redundant computer systems?

Dr. LEE. Yes.

Mr. BARTLETT. They are all down under some scenarios.

Dr. LEE. That is true, and indeed, simple redundancy turns out to give you maybe one layer of protection, but in basic computer science algorithms research, and we saw this at the symposium at the Library of Congress last week, there are far more sophisticated concepts in the general area of redundancy and diversity that could lead to a great deal more reliability and robustness.

Mr. BARTLETT. I don't know where we go——

Chair GORDON. You have got them all scared.

Mr. BARTLETT. I am just more and more concerned that the more sophisticated we become in using computers, the more vulnerable we are.

Dr. ESTRIN. It is a clearly valid concern. In the scenario you gave, which is clearly disastrous from all perspectives, just addressing the bringing back of the information technology and such, it is—while it is about the United States, it is, we know from security, that when you do backups, you don't just keep backups locally. You also ship some backups off to a remote location. I am from Los Angeles. We have all sources of natural disasters there. We always do our backups off-site, and in that sense, I would expect that there are programs within our government as well that has backup of key data sets and key resources off-site so that one way that you deal with this problem is to allow yourself to do rapid restructuring, rapid build-up of a replacement infrastructure.

Mr. BARTLETT. An all computer replacement infrastructure?

Dr. ESTRIN. Yes.

Mr. BARTLETT. Yes. I am asking, shouldn't we have another fall-back redundancy?

Dr. ESTRIN. Certainly from a government infrastructure, community infrastructure, I think your fall-back are a well-trained citizenry and people and governments. I am not sure what form that takes in the information transfer. I think it is a very interesting question how we think about starting to bring up our capacity, relying again on the human beings.

Mr. BARTLETT. Thank you, Mr. Chair.

Mr. HALL. Mr. Chair, I can help the gentleman if he would like. For a fall-back redundancy, I still have my Big Chief tablet and cedar pencil.

Chair GORDON. Thank you, Mr. Hall. I think Dr. Bartlett has got the beginnings of a good screenplay.

Mr. Luján, you are recognized for five minutes.

Mr. LUJÁN. Mr. Chair, thank you very much. I want to go back to the importance in the questioning with collaboration with some of the entities that have capabilities, whether it is through our laboratories with the emphasis in DOD and DOE.

Dr. Estrin, you said that it was important that the commercial aspect of this drive the security of the experience and what can be done to protect the networks with the Federal Government. Can you elaborate on that a little bit?

Dr. ESTRIN. Sorry if I wasn't clear. I didn't mean that it should drive. Clearly you have to have classified activities and government-focused activities. What I meant is that if you look empirically and historically you see the adoption of commercial technology in our everyday government business, both classified and unclassified, and so since we know that there is technology that the government wants to bring in from the commercial sector, it is important from the government's interest that the technology that is being produced in the government sector has built into it good forms of security and usable forms of security. Does that clarify?

Mr. LUJÁN. Absolutely, and I appreciate that very much, and that is really the basis for the line of questioning.

Dr. Lee, you mentioned the importance of the collaboration between entities. I think Mr. Akin asked a question along those lines about how are we collaborating with all of the efforts and the investment that has been made in so many of these areas and with your experience, and I would ask Dr. Greer the same question, with your experience, how can we truly move forward where we are collaborating more, where we are supporting more tech transfer, where we take advantage of the investments that we made within laboratories with the Department of Defense, Department of Energy, Office of Science and others to utilize that brain trust and that expertise to move forward with some of the modeling that can take place, the supercomputing capabilities in all aspects, especially in the area of energy, disease, smart grid applications, developing the necessary software and security with their experience with the number of threats that they experience on a daily basis as well.

Dr. LEE. Thank you, Mr. Luján. Indeed, just recently, the former CIO G6 of the U.S. Army, Steven Boutelle, informed me that during his tenure the U.S. Army had moved to a position where over 80 percent of the software and networking technology employed by the U.S. Army today is commercial off the shelf, COTS, and this raises a specific question about how we can certify the security and trustworthiness of commercial systems. This goes all the way down even to the hardware and the circuitry. And in fact, as Dr. Greer had mentioned and emphasized before, much of this is really core research in areas related to software development, software analysis and networking, and I believe that if we are able to increase the base of agency support for academic research, right now we are at 86 percent coming from the National Science Foundation. If we are able to expand into other areas, DARPA and other defense agencies and DOE, we will be able to provide a wider range of attacks on this problem and really come to grips with our needs, particularly in this security-related and trustworthiness-related area.

Mr. LUJÁN. Dr. Greer.

Dr. GREER. I would second what Dr. Lee has had to say in the sense that inherent in your question are a number of basic research challenges that the NITRD agencies are currently investing in including issues of software assurance, validation and verification and how can you ensure that a software package being delivered does what it is purported to do, that the system doesn't have any Trojan horses and so on. That is an example of a very basic research question. In the end, what we are striving for is research and development informed by implementation and implementation informed by research and development. So there is a cycle and an interaction that has go on there. That is all about communication amongst the various groups, and that is what is important to us.

Mr. LUJÁN. Thank you, Dr. Greer.

Mr. Chair, I certainly appreciate the fact that this is coming forward and the importance of COMPETES that you stressed as well, and as we look to see how we can incorporate the federal laboratories into the educational component but specifically in the area when we are talking about large-scale research in areas of national importance and we characterize those, I truly believe that if we harness that energy and we are able to expose so many of our young people when they are in junior high, even elementary and high school, to some of the research taking place at our national laboratories, include them into that field where we can take advantage of those opportunities, really use them as a hub to expand our university system and those capabilities as it translates to solving some of our large-scale problems is something that we can truly do. So I appreciate the inclusion of those in the Act.

Chair GORDON. Thank you, Mr. Luján. You are absolutely correct. Our National labs are a tremendous resource, and by the synergy of them working with universities and private sector is going to make a big difference in our country. In the COMPETES bill, we did address some of this so that there will be collaboration where both teachers and students can go into the labs and hopefully those teachers come back and get the kids excited.

Before we close, is there anyone else that would like to ask another question? If not, I want to thank our witnesses. This has been a very good hearing. You have provided us very good information. This is not as high profile as climate change and energy independence and health care but it is important to all those areas, and we hope that this bill will help us to move forward.

Let me also say that we welcome any further comments you might have in terms of our bill, and we welcome also comments from the audience here and for those who are listening over the Internet or watching for this transcript, and the record will remain open for two weeks for additional statements from Members and for answers to any of the follow-up questions the Committee may ask of the witnesses.

So the witnesses are excused and the hearing is adjourned.

[Whereupon, at 11:16 a.m., the Committee was adjourned.]

Appendix 1:

Answers to Post-Hearing Questions

ANSWERS TO POST-HEARING QUESTIONS

Responses by Christopher L. Greer, Director, National Coordination Office for Networking and Information Technology Research and Development (NCO/NITRD)

Questions submitted by Chair Bart Gordon

Q1a. There is a growing concern that the educational programs in networking and information technology are insufficient to prepare our future IT workforce. Please describe the NITRD program's current efforts to improve networking and information technology education at both the secondary and post-secondary level.

A1a. In FY 2008, NITRD agency investments in the Social, Economic, and Workforce (SEW) Implications of IT and IT Workforce Development Program Component Area totaled $118.7 million, including the following education-related efforts:

- Cyber-enabled Discovery and Innovation (CDI). This major National Science Foundation (NSF)-wide, five-year initiative is intended to revolutionize the conduct of science and engineering by infusing computational thinking and methods across the disciplines both in laboratory research and at all stages of education and training. Funded activities include exploration of interactive virtual learning environments that maximize students' cognitive capacities and learning styles as well as IT for reliable identification of developmental and learning disorders.
- NIH's National Library of Medicine (NLM) bioinformatics and biomedical informatics training. This ongoing program, which supports a variety of doctoral and postdoctoral training fellowships at academic institutions across the country, was set up to develop a cadre of scientific professionals with expertise both in IT and informatics and in biomedical science; the effort has led to recognition of bioinformatics as a significant specialization in biomedicine and institutionalization of biomformatics training programs in academia.
- Computational science graduate fellowship program (DOE). This ongoing activity supports students pursuing doctoral degrees in scientific or engineering disciplines with an emphasis in high-performance computing. The fellows gain hands-on high-end computing experience working with computational and disciplinary scientists at national laboratories.
- The NSF Computer and Information Science and Engineering (CISE) Directorate's Pathways to Revitalized Undergraduate Computing Education (CPATH). Begun in 2007, CPATH is focused on developing a computationally skilled workforce that can maintain U.S. economic competitiveness in the 21st century. The program is supporting multi-sector activities to identify strategies for improving undergraduate computing education; grants for adopting, extending, and evaluating innovative undergraduate programs; "transformation" projects that model new academic structures and cultural approaches; and a Distinguished Education Fellows effort, which brings outstanding professionals into the curriculum planning process.
- Broadening Participation in Computing (NSF). The goal of this effort begun in 2005 is to develop effective undergraduate and graduate-level recruitment and retention strategies to increase the number of U.S. citizens and permanent residents receiving post-secondary degrees in the computing disciplines, with an emphasis on students from communities with longstanding under-representation in computing. The program also seeks to improve computing research and education opportunities for *all* students.
- The Education and Workforce Program (NSF). This program invests in education initiatives for women (the Advancement of Women in Academic Science and Engineering Careers, or ADVANCE program), graduate student fellowships (GRF), graduate STEM Fellows, Integrative Graduate Education and Research Traineeship (IGERT) program, Research Experiences for Undergraduates (REU) and REU Sites.
- Cyberlearning and impact of IT on education practice (NSF). NSF supports activities to provide new opportunities for using cyberinfrastructure as a platform fir student learning experiences. It also supports the study of the impact of IT on teaching and learning.
- Faculty Early Career Development (CAREER) Program (NSF). All core computing programs at NSF participate in the CAREER Program, which emphasizes the integration of research and education.

Q1b. To what extent has the Department of Education been involved in the Social, Economic, and Workforce program component area of NITRD?

A1b. The Department of Education has only occasionally participated in SEW activities in recent years. The NCO is currently working to develop contacts within the agency and exploring possible avenues to encourage its participation.

Q1c. Additionally, please describe how the NITRD strategic plan will address networking and information technology education to ensure an adequate workforce.

A1c. As I noted in my April 1 testimony, education and workforce challenges are envisioned as a central element of the NITRD strategic plan. Two NITRD activities are providing inputs to the plan directly on this theme: a fast-track study comparing international IT education and workforce data, and draft education goals for the plan being developed by SEW with an ad hoc interagency group. The latter effort began in September 2008 with a Collaborative Expedition Workshop on strategic leadership for networking and IT education; the participants were Federal managers with education-related responsibilities from non-NITRD as well as NITRD agencies. The workshop was designed to promote coordination among NITRD programs with educational missions and identify candidates for a working group to develop the draft strategic plan educational goals.

Questions submitted by Ralph M. Hall

Q1. One of our witnesses in a previous NITRD hearing called out the oversized role of the NSF in supporting academic NIT research, noting that this single agency provides 86 percent of the funding in this area. What do We gain or lose by having a single agency dominate funding? How can we assess whether specialization like this is leading to greater efficiency for the program overall or creates stovepipes that slow down overall progress?

A1. Each agency's NITRD investments support the particular mission of the agency. NSF has the unique mission of promoting the health of the science and engineering research and education enterprise in this country and has traditionally focused on the academic sector. Thus, NSF leads among NITRD agencies in investments in basic research in mathematics and computer science in the academic sector. However, the Department of Defense is the largest investor (56 percent) in *applied* research in math and computer science in the academic sector (source: NSF SRS, 2005–2007; NSF 09–309).

Advantages of having the federal agency whose mission is most closely tied to basic research at academic institutions take the lead role in academic IT R&D include familiarity with the relevant community and its processes and deep expertise in the fundamental research challenges. A potential disadvantage is that the interests and perspectives of the other agencies may be overshadowed. Among the goals of the NITRD program is to support the kind of close information sharing and cooperation among agencies that can ensure that all agencies' interests and perspectives are considered.

From the perspective of the NITRD portfolio as a whole, investments are fairly widely distributed across the member agencies. For example, NSF accounted for 28 percent of the 3.3 billion in estimated FY 2008 NITRD spending reported in the FY 2009 NITRD budget supplement. The Department of Defense (OSD, DARPA, and NSA combined) accounted for 37 percent; NIH accounted for 15 percent; and DOE (FE/NE/NNSA/SC) accounted for 13 percent; NASA, NIST, NOAA, EPA, and NARA together accounted for seven percent.

Q2. You suggested in your testimony that the recent PCAST recommendations reflect the need for a framework that enables the NITRD portfolio of investments to respond to our nation's changing IT needs. Does the draft legislation provide for the flexibility and responsiveness you feel is necessary? Are there any areas where the suggested language would throw up a roadblock?

A2. In the current *High-Performance Computing Act* as amended, the topic areas that make up the Program are listed together in Section 101. This allows a balanced view of the scope of the Program and emphasizes the critical inter-dependencies across all of the topic areas. However, the draft legislation placement of both cyber-physical systems and long-term, large-scale research in separate sections rather than in Section 101, could be a significant roadblock to research progress in these areas and encourage unnecessary duplication of effort.

Section 104(b)(2) of the draft legislation includes as a criterion that large-scale projects "shall be carried out by a collaboration of no fewer than two agencies participating in the Program." This phrasing could be misinterpreted to discourage critical large-scale investments by any one agency or by agencies outside the Program.

Q3. How much stimulus funding will be devoted to NITRD programs and activities, and is OSTP/OMB or the NCO undertaking any special efforts to ensure this funding is fully coordinated and spent wisely?

A3. OMB is collecting data on restoration and recovery act spending on NITRD goals, and OSTP and OMB have worked closely with the NITRD agencies in planning effective spending under the restoration and recovery act.

Q4. How successful have the Federal agencies been at figuring out ways to interact with one another through computer systems, particularly since September 11, 2001, when it became evident how important it could be to homeland security?

A4. The OMB Office of eGovernment and Information Technology and the Federal CIO Council are better positioned to comment on current IT deployment and implementation. I can comment, however, on how some of the results of NITRD agency investments are improving the IT landscape:

- **Identity management across domains.** Shibboleth is a standards-based open software suite that enables federations of networks—such as those linking together the academic networks of U.S. universities—to authenticate users on any participating campus through a secure "single sign-on" interface. Developed by Internet2 researchers funded by NSF's Middleware Initiative, Shibboleth has both raised the security level of campus networks and increased the ease of inter-campus resource sharing, allowing sites to make informed authorization decisions on access to protected online resources while preserving privacy.
- **Distributed computing.** Globus and Condor are software packages, developed with funding by NITRD agencies, that each has significantly enhanced U.S. distributed computing capabilities in this decade. The Globus concept originated in DOE/SC research in the late 1990's on how to enable networks not just to transmit data but also to make advanced scientific resources (such as telescopes, microscopes, high-end computers, large-scale physics equipment, and data repositories) accessible to researchers regardless of their location. The result was "grid computing," made possible by an open suite of software tools called the Globus Toolkit for managing a secure distributed computing environment. Condor, developed by University of Wisconsin researchers with NSF support, is cunning scalable software for maximizing the use of computing cycles on distributed machines—from small computing clusters to large-scale grids. By parallelizing tasks, scanning for free cycles on networked computers, and directing the scheduling of those cycles for jobs, Condor minimizes idle computer time and speeds certain types of massively parallel research tasks, such as the identification of effective cellular binding sites for promising new medicines.
- **Cyber threats and malware detection.** Two developments funded by NITRD agencies—the Protected Repository for the Defense of Infrastructure Against Cyber Threats (PREDICT) and the Cyber Defense Technology Experimental Research (DETER) network—have improved the ability of public- and private-sector enterprises to understand their cyber vulnerabilities and improve their defenses against cyber attacks. The secure PREDICT archive makes available to authorized cyber security researchers and developers real data sets from attacks on U.S. networks. Such data, normally closely held, are an invaluable resource for designing hardware and software to prevent attacks and/or mitigate damage to systems and networks. The DETER testbed—a 1,000-node virtual network isolated from the Internet—provides an equally critical component for improving U.S. cyber security. DETER enables researchers to test innovative security approaches and experiment with a broad range of hardware and software strategies in a realistic environment. DARPA plans to develop a more advanced facility to expand upon this important work.
- **Efficient and reliable development methods.** DOD's Systems and Software Producibility Collaboration and Experimentation Environment (SPRUCE) is a three-year collaborative effort among federal, industry, and academic researchers to establish a hardware/software testbed and evaluation infrastructure to improve the timeliness, reliability, and cost-effectiveness of DOD procurements of software-intensive systems such as aircraft.

- **Improved network performance.** NITRD's Joint Engineering Team (JET) plays a key year-round role in maintaining U.S. research networks and their global connections. JET, which includes members from federal agencies, industry, academia, and other groups with an interest in high-performance research networking, coordinates networking activities, operations, and plans among multiple federal agency operational and research networks. Among its multiple ongoing responsibilities are: planning for network access points (NAPS, 12 gigaPoPs, STARLight, etc.); security; coordinating Optical Networking Testbeds; high-performance research connectivity; international connections; traffic monitoring; performance measurement; new technology deployment (e.g., IM); and developing recommended best practices (e.g., 9000 Byte MTU frames).

Questions submitted by Representative Vernon J. Ehlers

Q1. Does the draft legislation help to achieve an appropriately balanced portfolio? If not, what is missing or has been given too much attention?

A1. In the current *High-Performance Computing Act* as amended, the topic areas that make up the Program are listed together in Section 101. This allows a balanced view of the scope of the Program and emphasizes the critical inter-dependencies across all of the topic areas. I believe the Program has benefited over many years from this broad balance in the networking and IT R&D portfolio, which recognizes that hardware innovations are constrained without corresponding advances in software; the use of advanced networks will be limited without improvements in security and reliability; massive data sets will not drive progress if the data cannot be preserved, accessed, and used for increased understanding; etc.

Rather than continuing this important means for achieving balance, the draft legislation places both cyber-physical systems and long-term, large-scale research in separate sections rather than in Section 101, suggesting that these topics may be separate from, rather than integral to, the other elements of the Program. Development and deployment of cyber-physical systems are, for example, heavily dependent on continuing advances in dynamic mobile networking technologies; high-confidence methods, techniques, and tools to achieve reliability, verification, validation, and assured security and privacy; and in the scientific foundations of hardware and software. R&D in these topics is germane to multiple NITRD PCAs. Because of these inter-dependencies and the need for balanced efforts, both cyber-physical systems and long-term, large-scale research might best be included as integral elements of Section 101.

Q2. The PCAST Report calls for a number of ways to improve interagency coordination? Do all of you agree with those.recommendations? Do you have additional ideas on how coordination could be improved?

A2. The PCAST assessment included six recommendations for improved coordination. All six are being addressed by NITRD and the NCO, as summarized briefly below:

- **Develop a strategic plan for the NITRD Program—**Currently midway in the planning process
- **Conduct periodic assessments of the NITRD Program Component Areas and restructure the NITRD Program when warranted—**Evaluation of the PCA structure is expected to begin once the new strategic plan is in place
- **Develop public R&D plans or roadmaps—**R&D plans are scheduled to be developed under the new strategic plan upon its completion
- **Develop a set of metrics and other indicators of progress for the NITRD Program—**These will be included in the strategic plan and R&D plans process
- **NITRD NCO should develop and implement a plan for supporting the development, maintenance, and implementation of the NITRD strategic plan—**An NCO strategic planning process is underway, with completion expected in Fall 2009
- **The NITRD NCO should be more proactive in communicating with outside groups—**
  - Implemented new policy: All NCO staff travel now includes outreach visit to academic or commercial counterparts

- ○ Increased opportunities for public input: Four RFIs issued in current year; globally webcast public forum for strategic plan
- ○ Increased one-on-one meetings with commercial partners (e.g., Telcordia, Microsoft, and IBM visits)
- ○ Explored increased coordination with the Federal CIO Council through the Federal Agency Administration of Science and Technology Education and Research (FASTER) Community of Practice

Q3. What are the main challenges facing the education pipeline supplying the workforce for the research community and the information technology industry? In what ways do you think the NITRD program can address these challenges?

A3. Based on the current reports on this topic and dialogue with experts, I see three categories of challenges:

- At the K–12 level, the issues are complex. Computer science has often not been part of the curriculum or, where it has been included, has been focused on programming and/or computer literacy. Many K–12 teachers have no formal training in computer science. Many schools do not have the resources to help their teachers and to provide 21st century computing environments (including high-bandwidth Internet access). At all levels, the central role of computation in many scientific fields is not well addressed in the computer science curriculum today.
- At the undergraduate level, additional efforts are needed to promote and support the participation of women and minorities. If they are not part of the pipeline in the early years, they will not become part of the skilled IT workforce our country needs to remain competitive.
- Finally, there exists a widespread misperception of computer scientists as solely programmers, who work in isolation on abstract code—and today are subject to employment out-sourcing. This misperception of IT career paths may be especially discouraging to women, but it has also depressed computer science enrollments over all and has inhibited a wide range of efforts to attract women and minorities to the field. We need to highlight the exciting opportunities in computer science to address important societal and scientific challenges.

Among the programs to address these challenges are the CPATH and ADVANCE programs described above, the Department of Energy's Computational Science Fellows Program, the Broadening Participation in Computing Program at NSF, and others. Efforts within the computing community include the development of additional components to the computer science Advanced Placement (AP) exam and the work of the Computer Science Teachers Association (CSTA) to develop model curricula. Efforts to expand on these activities through cooperation and coordination are described in my response to question 4, below.

Q4. What actions is the NITRD program taking to address computing education issues, particularly at the K–12 level? What additional agencies and/or resources need to be brought to bear to create the most effective strategies to address these issues?

A4. Education and workforce development have emerged as key elements in our NITRD strategic planning discussions. As I commented in my response to Chairman Gordon's question, a small interagency working group led by SEW is focusing on these elements of the strategic plan.

In addition, the NITRD NCO is currently exploring the potential for a three-way partnership to address the education and workforce challenges. In our current thinking, the elements of this partnership would include:

- NITRD agency program managers, division directors, and others with education/training/workforce investments and/or responsibilities. (Last September's Collaborative Expedition workshop was designed to create connections and strengthen ties in this community.)
- Department of Education counterparts with close ties to the education community. (NCO is currently interacting with agency leadership to examine this possibility.)
- Professional organizations with active programs in computer science education, including curriculum development—e.g., Computer Science Teachers Association (CSTA) of the Association for Computing Machinery (ACM), The Computing Research Association (CRA), the National Science Teachers Asso-

ciation (NSTA). (For example, we will meet with an ACM/CSTA delegation in a few weeks to discuss ideas.)

Q5. What efforts are being made within OSTP to encourage other agencies to become more involved in the NITRD program and to ensure that those currently participating are pulling their weight?

A5. I have not discussed this matter with the new leadership of OSTP and, thus, cannot comment on that aspect of your question. However, I and Associate NCO Director, Ernest McDuffie, have taken a number of steps over the last 12 months to strengthen and expand agency participation in the NITRD Program. We have:

- met with DHS representatives to brief them on the NITRD Program and the potential value of becoming a core member of the Program (DHS staff already participate extensively in NITRD activities as valued participating members);
- worked with DOD representatives to forge closer ties to Army, Air Force, and Navy service research organizations;
- established connections with the Nuclear Regulatory Commission (NRC) and facilitated their active engagement as participating NITRD constituents; and
- met with representatives of DOE's CIO Office to brief them on current NITRD activities.

ANSWERS TO POST-HEARING QUESTIONS

Responses by Peter Lee, Incoming Chair, Computing Research Association (CRA); Professor and Head, Computer Science Department, Carnegie Mellon University

Questions submitted by Representative Ralph M. Hall

Q1. One of our witnesses in a previous NITRD hearing called out the oversized role of the NSF in supporting academic NIT research, noting that this single agency provides 86 percent of the funding in this area. What do we gain or lose by having a single agency dominate funding? How can we assess whether specialization like this is leading to greater efficiency for the program overall or creates stovepipes that slow down overall progress?

A1. 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). In addition to the NSF and DARPA, research and development in supercomputing was supported in large part by the Department of Energy (DOE), though much of that funding went to industry or non-academic operations of universities. The fact that these agencies have had 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 mid-course 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 cyber security research, there is another significant cost to bear as well. The military (and the government overall) has a huge dependence on our nation's commercial infrastructure, but classifying the research in a range of areas, including information security, AI, computer vision, embedded networks, and more means that it is largely unavailable for use in protecting this commercial infrastructure.

A related problem has been the increasing inability of foreign nationals (for example, many graduate students) to participate in some of this type of research. The restriction of foreign nationals should not be applied blindly, but instead based on a careful analysis of risk/benefit issues per research topic or project.

Failure to act to broaden the base of support for academic computing research will jeopardize U.S. leadership in IT, and constrain the pace of U.S. innovation across the economy, imperiling many of the gains those innovations have enabled.

Questions submitted by Representative Vernon J. Ehlers

Q1. Does the draft legislation help to achieve an appropriately balanced portfolio? If not, what is missing or has been given too much attention?

A1. The draft legislation identifies cyber-physical systems (CPS) as an area of opportunity and importance to the Nation's leadership in information technology. CPS is clearly going to be extremely important. However, this IT subfield is still in its infancy, and thus it is critical that the legislation promote a broad definition, going well beyond the science of computer-controlled physical devices (such as cars, airplanes, and other machine controllers) and into all systems in which IT and the physical world are tightly coupled. To take just one example, consider a network of sensors embedded into a natural area, for the purpose of understanding the effects of climate change. Such systems directly address our nation's challenges in energy and the environment, and give a glimpse at the tremendous opportunities in CPS.

An area that has been difficult to address in a coordinated manner is cyber security. There is no doubt that the Nation is at risk, as we have become increasingly dependent on the reliability and trustworthiness of our networks and information technology systems. As suggested in the recent report issued by the National Research Council's CSTB, "Toward a Safer and More Secure Cyberspace," federal funding for harder, long-term research challenges in cyber security is lacking, with most funding today being targeted instead towards short-term problems, or on fixing already-existing systems. Almost no funding has been expended on radical new ideas of system architecture and design of systems that might be more securable yet capable of meeting necessary mission requirements. This has hampered attempts to build a solid science base for cyber security—something that is sorely needed if we are to develop the innovative solutions that will protect our IT assets in the future.

Q2. The PCAST Report calls for a number of ways to improve interagency coordination. Do all of you agree with those recommendations? Do you have additional ideas on how coordination could be improved?

A2. I agree with the recommendations called for in the PCAST Report. The strategic plan that is described in the legislation, as it is developed, should address interagency coordination directly, with each section of the plan specifying how such coordination should be achieved, as appropriate.

Q3. What actions is the NITRD program taking to address computing education issues, particularly at the K–12 level? What additional agencies and/or resources need to be brought to bear to create the most effective strategies to address these issues?

A3. On March 17, 2009, CRA joined with the Association for Computing Machinery and the National Center for Women and Information Technology in providing a series of recommendations to the Committee to bolster computing education in the NITRD program. The three organizations believe the current bill could expand and better leverage and coordinate existing education efforts within the NITRD program.

Specifically, they recommended that the bill:

- Promote computing education, particularly at the K–12 level, and increased exposure to computing education and research opportunities for women and minorities as core elements of the NITRD program;
- Require the NITRD program to address education and diversity programs in its strategic planning and roadmapping process;
- Expand efforts at the National Science Foundation to focus on computer science education, particularly at the K–12 level through broadening the Math Science Partnership program; and,

- Enlist the Department of Education and its resources and reach in addressing computer science education issues.

Computing and the innovations it yields are critical to the domestic economy. However, the current NIT workforce pipeline will not satisfy the demands of an industry that includes some of the country's most innovative and successful companies. It is crucial that K–12 students are exposed to computer science education. The PCAST report noted some of the concerns of the computing community in this regard, arguing that K–12 science and mathematics preparation is weak, and students and parents are exposed to a negatively skewed view of computer science and engineering. This was reinforced by a recent National Academies study of the information technology research and development ecosystem, which says, in part:

> Concerns about the generation of talent are exacerbated by the poor state of the kindergarten though grade 12 (K–12) IT/computing education system in the United States. In its report *The New Education Imperative: Improving High School Computer Science Education,* the Computer Science Teachers Association correctly assess the situation as one in which knowledge of computer science is as essential as any of the traditional sciences, but in which curriculums, leadership, funding, professional development for teachers, and fluency objectives for students are all deficient.

The diversity of the pipeline also remains a major concern. Participation rates among women and minorities in computer science are among the lowest of any scientific field. In 2008, only 17 percent of Advanced Placement (AP) computer science test-takers were women, even though women represented 55 percent of all AP test-takers. Participation in computer science AP tests among under-represented minorities has increased in the past decade, but it is only at 11 percent, compared to 19 percent of all AP test-takers.

NITRD has a Program Component Area (PCA) that includes education activities and specifically mentions the 21st Century workforce and K–12 education as strategic priorities. However there is little specific attention to these issues within the PCA or prioritization within the NITRD program in general. Most education funding is from NSF. The Department of Education does not participate in the NITRD program at all. And, the NSF activities appear to lack involvement with some of the key programs within NSF's Education and Human Resources Directorate, which are focused on strengthening K–12 science, technology, engineering and mathematics education, including the Math Science Partnership program.

The public investments in K–12 education are largely based on outdated visions of education, curriculum and the skills that high school graduates should master. Simply put, we must do more to strengthen computer science and related curricula to expose and attract a more diverse population of students to computing and to support teachers of computer science at the K–12 level. Given the national education and workforce needs, it is short-sighted to rely on a relatively small federal agency and effort to address K–12 issues in computer science education. It is imperative that specific investments in computing education are authorized and funded. Addressing this in the NITRD reauthorization would be a welcome and appropriate step toward strengthening the computer science education pipeline and supporting the critical innovations it brings to industry and the economy.

ANSWERS TO POST-HEARING QUESTIONS

Responses by Deborah Estrin, Director, Center for Embedded Networked Sensing; Professor of Computer Science and Electrical Engineering, University of California, Los Angeles

Questions submitted by Representative Ralph M. Hall

Q1. One of our witnesses in a previous NITRD hearing called out the oversized role of the NSF in supporting academic NIT research, noting that this single agency provides 86 percent of the funding in this area. What do we gain or lose by having a single agency dominate funding? How can we assess whether specialization like this is leading to greater efficiency for the program overall or creates stovepipes that slow down overall progress?

A1. NSF has enough diversity internally that I have not seen evidence of stovepipes or a slowing down of progress. They have been a tremendously affective steward of the IT R&D dollars and process. They have been particularly effective when they have had adequate funds to support multi-disciplinary and experimentally oriented research such as under the ITR program. However, it is a huge burden on NSF to be the only game in town for IT research and given the clearly evidenced importance of this technology to all aspects of economy and society, additional funding through partner agencies is warranted.

Questions submitted by Representative Vernon J. Ehlers

Q1. Does the draft legislation help to achieve an appropriately balanced portfolio? If not, what is missing or has been given too much attention?

A1. I believe that the draft legislation does in fact represent an appropriately balanced research portfolio.

Q2. The PCAST Report calls for a number of ways to improve interagency coordination? Do all of you agree with those recommendations? Do you have additional ideas on how coordination could be improved?

A2. As to interagency coordination, I would highly encourage a continued emphasis in this direction and suggest seeking input from representatives from the research community (such as those who provided testimony at this hearing, as well as from domain scientists representing the other mission oriented agencies) as to particular projects and opportunities that seem most promising from a technological opportunity and scientific need perspective.

ANSWERS TO POST-HEARING QUESTIONS

Responses by Amit Yoran, Chief Executive Officer, NetWitness Corporation

Questions submitted by Chair Bart Gordon

Q1. In your written testimony you indicate that the Department of Homeland Security is investing approximately $19.5 million in cyber security research. Do you think DHS could leverage their investment more effectively if they were to become a full member of the NITRD program? Are research areas that DHS is not actively pursuing that they should be?

A1. While only a small amount, the DHS investment is efficiently invested and NITRD membership would not impact their investment significantly. DHS participates in all of the NITRD activities and so is coordinating within the interagency process. The DHS S&T investment is very broad for the funding they have. They are limited more by their budget than in the ability to pursue other research areas.

Q2. In your written testimony you indicate that while certain areas of research should remain classified the vast majority of networking and information technology research should be unclassified. Can you describe what research should remain unclassified and how classification has affected the networking and information technology R&D ecosystem?

A2. The only research and development that should be classified is that which is specific to certain operational missions. Because most academic and small business researchers do not have clearances, they are unable to participate in classified research programs. Over the past decade research in this area has been classified, leaving out the innovative ideas of small business and academia. Additionally, classified research seldom results in commercial products, which has also impacted the transition of government-funded research into the marketplace. Most classified research efforts should be transitioned to unclassified programs and only specific use cases remain classified. This transition will lead to better research and result in greater benefit to the cyber defense mission.

Q3. In your testimony you state that the U.S. cannot match the large-scale investments China and India are making in networking and information technology R&D, but we can maintain our leadership through innovation. Can you compare the level and types of investments being made by our international competitors? What strategic investments should we be making to maintain our innovative edge?

A3. The OECD recently ranked the United States 22nd in the percentage of GDP devoted to non-defense research. According to Steven Ezell of the Information Technology & Innovation Foundation (ITIF), "compared with other industrialized democracies, the U.S. Government invests relatively little in innovation-promotion efforts. In fiscal year 2006, the Federal Government spent a total of $2.7 billion, or 0.02 percent of gross domestic product, on its principal innovation programs and agencies [.]. . . if the United States wanted to match Finland's outlays per dollar of GDP, it would have to invest $34 billion per year." In an article in *Physics Today* published in late 2006, Cong Cao, Richard Suttmeier, and Denis Fred Simon analyzed China's 15-year science and technology plan. They point out that, "according to the "Medium- to Long-Term Plan for the Development of Science and Technology," China will invest 2.5 percent of its increasing gross domestic product in R&D by 2020, up from 1.34 percent in 2005; raise the contributions to economic growth from technological advances to more than 60 percent, and limit its dependence on imported technology to no more than 30 percent." This plan also includes ambitious goals in the areas of developing Chinese scientific thought leadership and domestic Chinese innovation. While this is covering the broad spectrum of Science and Technology, it is clear that these countries are making the necessary strategic investments. To start with, we should increase our government funded research programs by an order of magnitude. Such an investment would revitalize the entire R&D ecosystems, including small business, venture capital, etc. While we cannot match dollar for dollar the investment of China and other nations, we can rely on innovative approaches and entrepreneurial functions in the United States to yield more efficient results with the funds we do chose to invest.

Questions submitted by Representative Ralph M. Hall

Q1. One of our witnesses in a previous NITRD hearing called out the oversized role of the NSF in supporting academic NIT research, noting that this single agency provides 86 percent of the funding in this area. What do we gain or lose by having a single agency dominate funding? How can we assess whether specialization like this is leading to greater efficiency for the program overall or creates stovepipes that slow down overall progress?

A1. The major drawback of having this single agency dominate the funding in this area is that NSF funds only basic research solely with academics and non-profits. Therefore, a majority of the funded research never makes it into the development, transition, and commercialization pipelines. Other government agencies, such as DHS S&T, have broad programs that includes the full research, development, test, evaluation, and transition (RDTE&T) spectrum and these programs are hampered when the majority of funding is given to NSF. Assessment of efficiency in the R&D environment is a difficult task. Current NSF assessment is usually based on the number of academic papers written and the number of granted degrees. These statistics do not provide a measure of progress. Other agencies can measure the impact by number of products developed, transitioned, and commercialized, which is an excellent measure for those program, but not applicable to NSF. There are many sources for development capital in the United States, of which the Federal Government is one. The government does have a larger role to play in fundamental research, where commercial entities typically investment with shorter-term expectations of commercialization.

Q2. You stated in your testimony that "care must be taken to no expend limited resources trying to enter the security product development business, especially via classified venues." Please elaborate. Are you concerned that DHS and/or other agencies may be attempting to develop their own cyber security hardware and software and sell it to (or force it upon) the private sector?

A2. DHS does not currently have a classified research program. The concern is that other agencies, e.g., DARPA, are creating "Government-Off-The-Shelf (GOTS)" products that are competing with the private sector. Additionally, there are intelligence agencies that are producing GOTS products and requiring their usage by other agencies as part of the current CNCI program. Many of these technologies are already available from the private sector and the government is not considering these solutions, instead they are spending their limited funds to create their own competing solutions. Furthermore, any such GOTS solutions are expected to be developed in classified environments where any possible benefits they make possible are not delivered to the private sector. The intelligence community should work with private industry to better refine the products and capabilities to address the government cyber requirements. Use cases and signature sets can remain classified so as to protect sources and methods. The resulting improvement in security products will better enable the private sector and critical infrastructures to better protect themselves.

Q3. The White House is publicly calling for a "national public-private partnership" on cyber security, which some believe may focus on regulating private sector cyber security standards and protocols. Separately, legislation has been introduced in the Senate that would "establish enforceable cyber security standards" that "would be applicable to both government and the private sector." Do you think this is a good idea? Why or why not?

A3. The government should be concerned about protecting its infrastructure and government data. As the largest consumer of IT and IT security products, any good standards and practices that the government requires will be embedded eagerly into security products and assist private industry in better protecting itself. In isolation the private sector has other interests, including profitability which sometime preclude it from aggressively adopting new security standards. Public-private partnerships are necessary going forward, but they can only be effective if they are clearly defined, with measurable objectives and clear value propositions for all participants.

Q4. How successful have the Federal agencies been at figuring out ways to interact with one another through computer systems, particularly since September 11, 2001, when it became evident how important it could be to homeland security?

A4. The information sharing environments of the government are still not working effectively. The recent resignation of Rod Beckstrom described some of the continuing problems in this area, some of which are technical and others cultural and political. In addition, the sharing of information with the private sector has not advanced very far. There have been many instances where the private sector has had information, but have not shared it with the government because there is no value proposition for sharing, and in many instances significant exposure.

Questions submitted by Representative Vernon J. Ehlers

Q1. Does the draft legislation help to achieve an appropriately balanced portfolio? If not, what is missing or has been given too much attention?

A1. Because the National Coordination Office (NCO) and the NITRD program is solely an oversight activity, the legislation doesn't guarantee a balanced portfolio. Each of the agencies that participate in the NITRD program has their own budgets, none of which are "controlled" by the NCO and NITRD. To truly force a balanced portfolio across all agencies, there needs to be some centralized entity that has the ability to control agency budgets, thus, ensuring that agencies do not focus only on their needs or "pet projects."

Q2. The PCAST Report calls for a number of ways to improve interagency coordination. Do all of you agree with those recommendations? Do you have additional ideas on how coordination could be improved?

A2. For the most part these recommendations are good. However, there doesn't appear to be significant coordination between OSTP and the NCO and this is then not reflected to the interagency working groups of the NITRD.

Appendix 2:

Additional Material for the Record

PREPARED STATEMENT OF AMIT YORAN

Mr. Chairman and Ranking Member, thank you for the opportunity to testify before the House Committee on Science and Technology on "Networking and Information Technology Research and Development."

My name is Amit Yoran and I am the CEO of the NetWitness Corporation, a company providing next generation cyber security monitoring technologies to the U.S. Government and the private sector, and in delivering critical infrastructure cyber protection to the Nation. I also serve as a member of the CSIS Cyber Commission advising the 44th Presidency and on numerous security industry advisory bodies.

I have served as the first Director of the National Cyber Security Division (NCSD) in standing up the United States Computer Emergency Readiness Team (US–CERT) and Einstein program at the Department of Homeland Security (DHS), as CEO and advisor to In-Q-Tel, as founder and CEO of Riptech, an innovative cyber security company, and as manager of the Vulnerability Analysis Program (VAP) of the U.S. Department of Defense's Computer Emergency Response Team (DOD CERT). I received a Bachelor of Science degree in Computer Science from the United States Military Academy at West Point and a Master of Science in Computer Science from The George Washington University.

Over the past fifteen years, automation and the use of computer systems has permeated every aspect of modern life. Our nation is entirely reliant upon computer systems and networked technologies in everything from national security and intelligence activities to commerce and business operations to power production and transmission to personal communications and correspondences.

Today's Internet has become one of the unifying fabrics driving globalization at an increasingly accelerated pace. Beyond its role as the pervasive communications medium, computer based automation and technology are the driving forces behind every major industrial and economic base in the world. Simply put, computer technologies and communications represent the greatest threat to and opportunity for our nation.

Networking and Information Technology Research and Development (NITRD)

The United States leads the world in networking and information technology (NIT). In recent years competitors in China and India have been investing strategically in large scale NIT research and development efforts. The U.S. leadership position is primarily driven by and can only be maintained by continuing with a broadly diffused and highly innovative industrial base in networking and information technologies. Simply put, we will lose if our efforts are reduced to long-term direct and linear competition. The competitive landscape overseas includes large scale, well coordinated and deliberate investment into NIT research, development and education programs, which we cannot match. It is, in fact, our innovation which is necessary for continued leadership in technology. The NITRD program, which invests approximately $3.5 billion, is a key component by which the U.S. Government contributes to defining the federal need and contributing to national efforts in these areas.

Research or Development Balance and Focus

In order for NITRD to provide the maximum benefit to the government and the Nation, it must work hand in glove with industry ingenuity and entrepreneurship. Every year through corporate programs and private industry, billions of dollars are invested in improving network and information technologies. According to the National Venture Capital Association, "Since 1970 venture capitalists have invested more than $466 Billion into more than 60,700 companies." Most of these investments are iterative improvements to technologies and methods which are known and are intended to develop and commercialize them, thereby making them broadly available. U.S. Government networking and information technology needs align very closely with those of private industry. These areas of alignment are broad, including large scale processing, networking and storage platforms, human computer interaction, data and knowledge management, software and systems design, cyber security and information assurance (which include resiliency, integrity and confidentiality), and workforce issues. Only in isolated instances are Government needs unique or do they differ from those of industry. In cases where they differ slightly or in cases where the government-specific requirements represent a significant enough commercial opportunity, private industry will evolve to meet those unique needs as well. Technologies developed by private industry not only fuel economic growth, they provide for technologies better supported in the field, more nimble to evolve as requirements change and ultimately lower the total cost of ownership. However, only in rare instances does the private sector invest in fundamental or long-term research activities, which must remain the focus of Federal Government R&D activities.

Classified Versus Unclassified Research and Development Activities

NITRD funds unclassified activities. Nearly all U.S. Government funding for NIT research should occur at an unclassified level. In certain areas government-use cases of technology must remain legitimately classified, but the fundamental research behind these networking and information technology efforts must occur at the unclassified level. The vast majority of promising researchers do not hold adequate security clearances, which serves to significantly limit the talent pool for classified research. Fundamental research efforts when classified also prevent the Nation from leveraging the innovation outside of the privileged few. This holds true for adoption by the private sector, NIT advantage and growth in private industry and consequently also a decrease in overall economic efficiency and competitiveness of the Nation. Classified research programs lack the adequate public review and debate necessary to assure that the programs are designed optimally, contain the highest level of innovation, and are well-aligned with and informed by the total body of knowledge of the NIT community. In the rare cases where R&D projects must be classified, The White House Office of Science and Technology Policy (OSTP), which has the appropriate clearances, should work to ensure proper coordination and non-duplication with unclassified R&D efforts.

Cyber Security R&D

The current paradigm in cyber security is not likely to change significantly through private sector efforts in areas such as improved security products, monitoring and incident response capabilities. While the private sector makes significant investment in needed incremental product, application and protocol improvements; fundamental research is required to meaningfully improve the security of the cyber and critical infrastructures.

According to the CSIS Commission work, "The Federal Government plans to spend about $143 billion in 2009 on R&D. We estimate that two-tenths of one percent of that will go to cyber security." An inherently government investment must drive long-term research agendas in cyber security, where private sector focus on shorter-term commercialization limits gains to those of a more tactical and incremental nature.

NITRD programs will receive $3.5 billion for research and development, and cyber R&D will receive approximately $300 million. Beyond the $260 million reported by NITRD as being focused on cyber R&D, the Department of Homeland Security allocated an additional $19.5 million for 2009 in S&T programs for cyber that is not included in NITRD figures. Funding for research and development is politically complex and many of the groups who should be benefiting from it are not. A $300 million investment in cyber security is inadequate. DHS' embarrassing lack of attention to cyber programs simply fails any semblance of judgment and mocks their role as sector specific or lead agency on cyber matters. As cyber R&D portfolio manager at DHS, Doug Maughan has been very successful given an untenable lack of resources.

The Comprehensive National Cyber Initiative (CNCI) calls for increased near- and longer-term R&D activities. Care must be taken to not expend limited resources trying to enter the security product development business, especially via classified venues. Rather, the government must guide and assist in articulating functional requirements for the development of technologies that can help us best address the sophisticated cyber threat environment. These requirements must inform a broad reform of our sourcing methods for networking and information technologies so that they are procured, deployed and maintained in a more secured state. By appropriately relying on industry for development, we can avoid the problem of government development efforts stranding enterprise cyber defenders without the benefits of product management, maintenance or professional support. The resulting improvement in security technologies will not only benefit the government in protecting its systems, but will also benefit the Nation's critical infrastructure operators and rest of the shared Internet fabric that joins our digital world.

A national research and development technology agenda must both identify the most promising ideas and describe the strategy that brings those ideas into fruition, recognizing that these activities must work hand in glove with private industry. The agenda must also jump-start a multi-disciplinary effort. By incorporating other disciplines that are greatly affected by cyber, we can better understand the security implications of their reliance on cyber and also help identify creative methods for addressing critical shortcomings.

The INFOSEC Research Council's "Hard Problems" list identifies several areas in need of immediate funding and action;

1. Global-Scale Identity—Identification required to produce an infrastructure capable of and reliable for commercial and national security purposes
2. Insider Threat—All security technologies and approaches rely practically on modeled behavior of external bad actors. This runs contrary to a majority of the security data, which shows damaged caused by insiders to be orders of magnitude more frequent and costly
3. Availability of Time-Critical Systems—Implementing effective security for systems where timeliness, performance and availability are higher priority services than security (i.e., control systems)
4. Scalable Secure Systems—The development of large-scale secure systems where individual components or dependencies may be flawed or compromised
5. Situational Understanding and Attack Attribution—Determining the current state of security for large scale and complex systems and being able to conduct assessments and provide attribution for security incidents
6. Information Provenance—Developing systems and methods to determine and manage the integrity of information and information systems
7. Security with Privacy—Designing methods and processes to improve security while preserving or enhancing privacy through granularity of activities and systems improvements
8. Enterprise-Level Security Metrics—Scalable methods to determine or represent security or risk are needed in order to optimize resource allocation and decision-making.

Conclusions

In the areas of networking and information technologies Congress and the Obama Administration can meaningfully improve the impact of federal investment.

1. Focus on fundamental research that is currently unfunded, but necessary to assure America's long-term competitiveness.
2. Except in rare instances, networking and information technology research and development should be conducted in an unclassified fashion.
3. While spending more on cyber security research and development activities in their aggregate is desirable, a redistribution of resources from government custom cyber security technology development to research activities would substantively increase the likelihood of discovering the paradigm changing methods which might take us out of the current cycle of tactical cat and mouse increments.
4. The Department of Homeland Security should invest meaningfully in cyber security research and development. The Intelligence Advanced Research Projects Activity (IARPA) should focus on top intelligence community problems, such as attack attribution, which may represent a hard problem, but does not represent significant overlap with the research needs of many other federal department and agency missions. Nor is attribution a research requirement of the private sector.
5. In a much needed redistribution of priorities from tactical government development efforts to the funding of fundamental research, a series of creative and lower cost programs can help the government better understand and leverage the emerging development efforts of private industry. As an innovative example of one such program, In-Q-Tel, a government funded, non-profit, venture capital entity actively reviews hundreds of innovative, venture capital-backed, emerging technologies each year from around the Nation and selectively brings them to the Intelligence Community. These technologies can address near-term requirements or solutions the IC would otherwise likely fund costly development efforts to address. This innovative model not only assures efforts are informed by private industry, it also helps the government leverage capital already invested in the development of new technologies and spurs economic growth. Such innovative approaches can be used for greater alignment with industry.

BIOGRAPHY FOR AMIT YORAN

Amit Yoran serves as the Chairman and CEO of NetWitness Corporation, a leading provider of network security analytic products. He is a Commissioner of the

CSIS Commission on Cyber Security advising the 44th Presidency and serves on several industry and national advisory bodies. Prior to NetWitness Mr. Yoran served Director of the National Cyber Security Division at the Department of Homeland Security, and as CEO and advisor to In-Q-Tel, the venture capital arm of the CIA. Formerly he served as the Vice President of Worldwide Managed Security Services at the Symantec Corporation. Mr. Yoran was the co-founder of Riptech, a market leading IT security company, and served as it's CEO until the company was acquired by Symantec in 2002. He formerly served an officer in the United States Air Force in the Department of Defense's Computer Emergency Response Team.

Mr. Yoran is an independent director on the boards of innovative security technology companies Boards, including; Guardium, Digital Sandbox, and IronKey. He previously served on the board of Cyota until the company's acquisition by RSA in 2006, Guidance Software (GUID) through the company's successful IPO in 2007 and as an advisor to Intruvert Networks until the company's acquisition by McAfee in 2003.

Mr. Yoran received a Master of Science degree from the George Washington University and Bachelor of Science from the United States Military Academy at West Point.

○