The Federal Networking and Information Technology Research and Development Program: Funding Issues and Activities

Patricia Moloney Figliola
Specialist in Internet and Telecommunications Policy

December 15, 2009

Congressional Research Service
7-5700
www.crs.gov
RL33586

CRS Report for Congress
Prepared for Members and Committees of Congress

c11173008

Summary

In the early 1990s, Congress recognized that several federal agencies had ongoing high-performance computing programs, but no central coordinating body existed to ensure long-term coordination and planning. To provide such a framework, Congress passed the High-Performance Computing and Communications Program Act of 1991 (P.L. 102-194) to enhance the effectiveness of the various programs. In conjunction with the passage of the act, the White House Office of Science and Technology Policy (OSTP) released *Grand Challenges: High-Performance Computing and Communications*. That document outlined a research and development (R&D) strategy for high-performance computing and a framework for a multiagency program, the High-Performance Computing and Communications (HPCC) Program. The HPCC Program has evolved over time and is now called the Networking and Information Technology Research and Development (NITRD) Program, to better reflect its expanded mission.

Proponents assert that federal support of information technology (IT) R&D has produced positive outcomes for the country and played a crucial role in supporting long-term research into fundamental aspects of computing. Such fundamentals provide broad practical benefits, but generally take years to realize. Additionally, the unanticipated results of research are often as important as the anticipated results. Another aspect of government-funded IT research is that it often leads to open standards, something that many perceive as beneficial, encouraging deployment and further investment. Industry, on the other hand, is more inclined to invest in proprietary products and will diverge from a common standard when there is a potential competitive or financial advantage to do so. Finally, proponents of government support believe that the outcomes achieved through the various funding programs create a synergistic environment in which both fundamental and application-driven research are conducted, benefitting government, industry, academia, and the public. Supporters also believe that such outcomes justify government's role in funding IT R&D, as well as the growing budget for the NITRD Program. Critics assert that the government, through its funding mechanisms, may be picking "winners and losers" in technological development, a role more properly residing with the private sector. For example, the size of the NITRD Program may encourage industry to follow the government's lead on research directions rather than selecting those directions itself.

The President's FY2010 budget request calls for $3.926 billion for the NITRD Program, an increase of $3.925 billion, or approximately 1%, over the 2009 estimate. The FY2009 budget estimate is $3.882 billion for the NITRD Program, an increase of $0.334 billion, or approximately 9%, over the President's request.

Under the American Recovery and Reinvestment Act (ARRA) of 2009, five Federal agencies report preliminary allocations of $706 million to investments in NITRD research areas (these figures may change). The NITRD agencies will use their ARRA funds to modernize, expand, and upgrade networking and high-end computing infrastructures and facilities for advanced scientific research; expand R&D in cyber security, human-computer interaction and information management, high-confidence software and systems, and software design; and increase investments in education and training for a diverse, highly skilled IT workforce.

Contents

Figures

Contacts

Overview of the Federal NITRD Program

The federal government has long played a key role in the country's information technology (IT) research and development (R&D) activities. The government's support of IT R&D began because it had an important interest in creating computers that would be capable of addressing the problems and issues the government needed to solve and study. One of the first such problems was planning the trajectories of artillery and bombs; more recently, such problems include simulations of nuclear testing, cryptanalysis, and weather modeling. That interest continues today. Such complexity requires there be adequate coordination to ensure the government's evolving needs (e.g., homeland security) will continue to be met in the most effective manner possible.

NITRD Structure

The Networking and Information Technology Research and Development (NITRD) Program is a collaborative effort in which 13 agencies coordinate and cooperate to help increase the overall effectiveness and productivity of federal IT R&D.[1] Of those 13 members, the majority of funding, in descending order, goes to the National Science Foundation, National Institutes of Health, Department of Energy (DOE) Office of Science, Defense Advanced Research Projects Agency (DARPA), and DOE National Nuclear Security Administration. Dr. Christopher Greer was named as the director of the NITRD Program in October 2007. **Figure 1** illustrates the organizational structure of the NITRD Program.

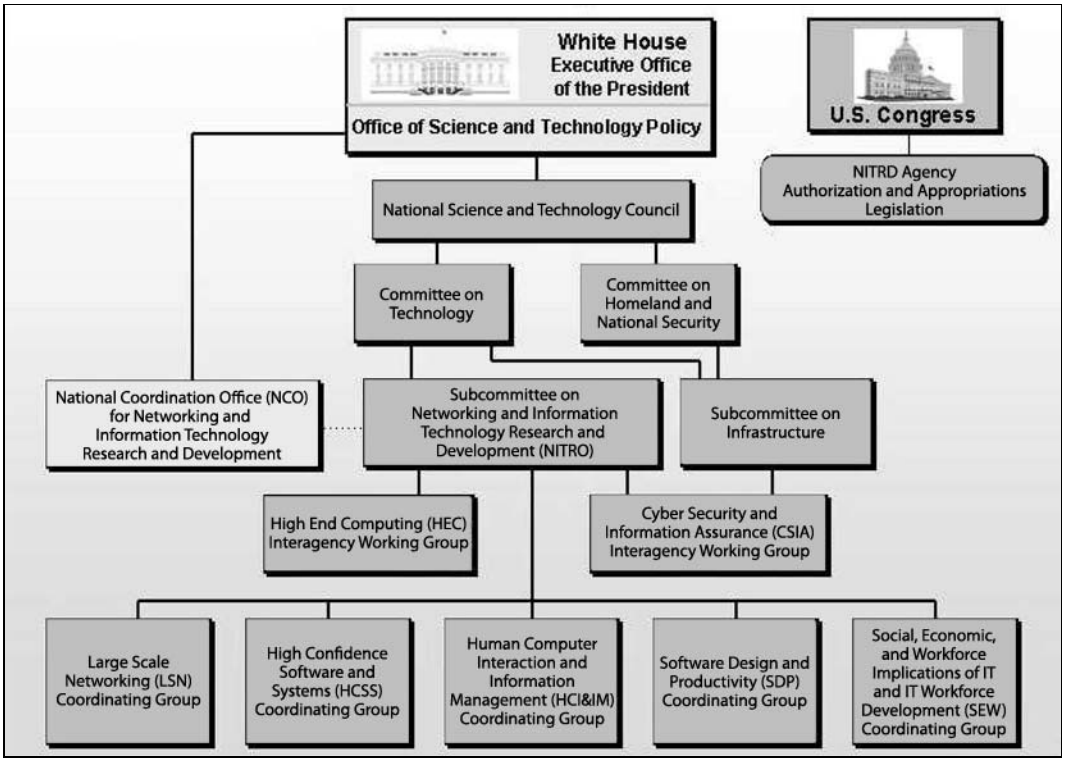
The National Coordinating Office (NCO) coordinates the activities of the NITRD Program. On July 1, 2005, the NCO became the "National Coordination Office for Networking and Information Technology Research and Development." The Director of the NCO reports to the Director of the White House Office on Science and Technology Policy (OSTP). The NCO supports the Subcommittee on NITRD (also called the NITRD Subcommittee)[2] and the President's Information Technology Advisory Committee (PITAC).[3]

[1] The members of the NITRD Program, as listed in the FY2006 Supplement to the President's Budget, are: Agency for Healthcare Research and Quality (AHRQ); Defense Advanced Research Projects Agency (DARPA); Office of the Secretary of Defense, Defense Research & Engineering, and the DOD service research organizations; Department of Energy, National Nuclear Security Administration (DOE/NNSA); Department of Energy, Office of Science (DOE/SC); Department of Homeland Security (DHS); Environmental Protection Agency (EPA); National Aeronautics and Space Administration (NASA); National Institutes of Health (NIH); National Institute of Standards and Technology (NIST); National Oceanic and Atmospheric Administration (NOAA); National Security Agency (NSA); and National Science Foundation (NSF). The history of agency participation can be found at http://www.nitrd.gov/about/history/agency-participants.pdf.

[2] The NITRD Subcommittee was previously called the Interagency Working Group for IT R&D (IWG/IT R&D).

[3] The PITAC was established on February 11, 1997, to provide the President, OSTP, and the federal agencies involved in IT R&D with guidance and advice on all areas of high performance computing, communications, and information technologies. Representing the research, education, and library communities and including network providers and representatives from critical industries, the committee advises the Administration's effort to accelerate development and adoption of information technologies. Additional information about the PITAC is available at http://www.nitrd.gov/pitac. The most recent PITAC Executive Order expired on June 1, 2005.

Figure 1. Management Structure of the NITRD Program



Source: NITRD Program website, http://www.nitrd.gov.

- The NITRD Subcommittee provides policy, program, and budget planning for the NITRD Program and is composed of representatives from each of the participating agencies, OSTP, Office of Management and Budget, and the NCO. Two Interagency Working Groups and five Coordination Groups reporting to the NITRD Subcommittee focus their work in eight Program Component Areas (PCAs).[4]

[4] The eight PCAs are (1) *High-End Computing Infrastructure and Applications (HEC I&A)*—to extend the state of the art in high-end computing systems, applications, and infrastructure; (2) *High-End Computing R&D (HEC R&D)*—to optimize the performance of today's high-end computing systems and develop future generations of high-end computing systems; (3) *Cyber Security and Information Assurance*—to perform fundamental and applied R&D to improve the security and assurance of information systems; (4) *Human Computer Interaction and Information Management (HCI&IM)*—to develop new user interaction technologies, cognitive systems, information systems, and robotics that benefit humans; (5) *Large Scale Networking (LSN)*—to develop leading-edge network technologies, services, and techniques to enhance performance, security, and scalability; (6) *Software Design and Productivity (SDP)*—to advance concepts, methods, techniques, and tools that improve software design, development, and maintenance to produce more usable, dependable and cost-effective software-based systems; (7) *High Confidence Software and Systems (HCSS)*—to develop the scientific foundations and IT to achieve affordable and predictable high levels of safety, security, reliability, and survivability, especially in U.S. national security and safety-critical systems; and (8) n *Social, Economic, and Workforce Implications of IT and IT Workforce Development (SEW)*—to study the impact of IT on people and social and economic systems; develop the IT workforce; and develop innovative IT applications in education and training. Additional information about the program component areas is available at http://www.nitrd.gov/subcommittee/index.html. HEC R&D and HEC I&A are both covered by the HEC Interagency Working Group. A diagram illustrating the evolution of the PCAs, 1992-present, is available at http://www.nitrd.gov/ about/history/new-pca-names.pdf.

- The PITAC is composed of representatives of private industry and academia who are appointed by the President. The group provides expert independent advice to the President on the federal role in maintaining U.S. preeminence in advanced IT and works with the NITRD Program agencies and the NITRD Subcommittee.
- The NITRD Program is funded out of each member agency's individual budget, rather than in a single appropriations bill (e.g., NITRD Program activities conducted by the National Institutes of Health (NIH) are funded through the NIH appropriations bill). The program's NCO is not explicitly funded; rather, the NITRD member agencies contribute toward NCO operations.

The NITRD Program has undergone a series of structural changes since its inception in 1991 and both it and the NCO have had a number of different names over the years. When the Program was created in December 1991, it was named the High Performance Computing and Communications (HPCC) Program, and when the NCO was created in September 1992, it was named the NCO for HPCC. The name was changed to the National Coordination Office for Computing, Information, and Communications per the FY1997 Supplement to the President's Budget (also known at that time as the "Blue Book"). The name was changed to the National Coordination Office for Information Technology Research and Development per the FY2001 Blue Book.[5] Most recently, on July 1, 2005, the name was changed to the National Coordination Office for Networking and Information Technology Research and Development. These changes were made to reflect the evolution of the program as it came to encompass a broader range of related topics.

NITRD Funding

The President's FY2010 budget request calls for $3.926 billion for the NITRD Program, an increase of $3.925 billion, or approximately 1%, over the 2009 estimate. The FY2009 budget estimate is $3.882 billion for the NITRD Program, an increase of $0.334 billion, or approximately 9%, over the President's request.[6]

American Recovery and Reinvestment Act of 2009

Under the American Recovery and Reinvestment Act (ARRA) of 2009, five Federal agencies report preliminary allocations of $706 million to investments in NITRD research areas (these figures may change). The NITRD agencies will use their ARRA funds to modernize, expand, and upgrade networking and high-end computing infrastructures and facilities for advanced scientific research; expand R&D in cyber security, human-computer interaction and information management, high-confidence software and systems, and software design; and increase investments in education and training for a diverse, highly skilled IT workforce.[7]

---

[5] That change was effective October 2000.

[6] Supplement to the President's Budget, The Networking and Information Technology Research and devekopment Program, online at http://www.nitrd.gov/Pubs/2010supplement/FY10Supp-FINALFormat-Web.pdf.

[7] Ibid.

American Competitiveness Initiative

The American Competitiveness Initiative has increased the NITRD budgets of agencies that are part of the Initiative. The Initiative calls for a doubling over 10 years of the investment in three federal agencies that support basic research programs in the physical sciences and engineering: the National Science Foundation (NSF), the Department of Energy's Office of Science (DOE/SC), and the National Institute of Science and Technology (NIST)—are NITRD Program member agencies. All three received FY2007 NITRD budget increases that exceed the percentage increase in the overall Program budget, as follows: NSF, 12%; DOE/SC, 35%; and NIST, 10%. The aggregated NITRD budget increase for these three agencies from 2006 estimates to 2007 request is $186 million (17% above 2006 estimates), which accounts for over 85% of the overall NITRD Program budget increase for 2007.[8]

NCO, PITAC, and Related Reports and Activities

As explained earlier, the NCO provides technical and administrative support to the NITRD Program, the NITRD Subcommittee, and the PITAC. This includes supporting meetings and workshops and preparing reports. The NCO interacts with OSTP and OMB on NITRD Program and PITAC matters.

National Cyber Leap Year Summit

Between August 17th and 19th of this year, the NITRD Program, with guidance from OSTP and the Office of the Assistant Secretary for Defense Networks and Information Integration, held a National Cyber Leap Year Summit in Arlington, VA. The Summit gathered commercial and academic innovators for an unconventional exploration of five game-changing strategies in cyber security:

- Basing trust decisions on verified assertions (Digital Provenance)
- Attacks only work once if at all (Moving-target Defense)
- Knowing when we have been had (Hardware-enabled Trust)
- Move from forensics to real-time diagnosis (Nature-inspired Cyber Health)
- Crime does not pay (Cyber Economics)

Participants discussed how to initiate and sustain fundamental cyber security changes within those five strategies. The Summit's outcomes are provided as input to the Administration's cyber security R&D agenda and as strategies for public-private actions to secure the Nation's digital future.[9]

---

[8] The FY2007 NITRD Budget request is at http://www.nitrd.gov/pubs/2007supplement/.

[9] The reports from the summit are available at http://www.qinetiq-na.com/.

High-Confidence Medical Devices: Cyber-Physical Systems for 21st Century Health Care

This report, published in February 2009, presents the perspectives of the senior scientists of the NITRD Program's High Confidence Software and Systems (HCSS) Coordinating Group (CG), with input from experts from other Federal agencies, on the R&D challenges, needs, and strategies for developing and deploying the next generations of high-confidence medical devices, software, and systems.[10] HCSS agencies whose missions are not medical device-specific have found it beneficial to partner in this area because medical device research challenges are similar, if not identical, to those within their purview. Digital technologies are increasingly being assigned high-level control over the monitoring, sensing, actuation, and communications of medical devices—often with human life in the balance. Through this report and associated HCSS-sponsored national workshops, the HCSS agencies are seeking to illuminate fundamental scientific and technical challenges that must be addressed before we can design and build high-confidence devices, software, and systems that operate flawlessly from end to end. The report authors sought to paint the landscape of the evolution of medical device technology and the federal investments that have benefitted medical device R&D over time.

The authors noted a number of key findings:

Today's medical device architectures are typically proprietary, not interoperable, and rely on professionals to provide inputs and assess outputs; "families" of such devices also tend to be stove-piped and not interoperable with other "families" of devices.

- In the frequent circumstance that a patient is connected to multiple devices at once, such as in an operating room, clinicians now must monitor all devices independently, synthesize data, and act on their observations, which can be affected by stress, fatigue, or other human factors.
- Medical device architecture is beginning to include wired and wireless interfaces to facilitate networked communication of patient data. But ad hoc efforts to aggregate data across devices designed to operate separately can lead to unintended or accidental results.
- The growing interest in such capabilities as home health care services, delivery of expert medical practice remotely (telemedicine), and online clinical lab analysis underscores the central role of advanced networking and distributed communication of medical information in the health systems of the future. Increased R&D focus on the specialized engineering of networked medical device systems is needed.
- Neither past nor current development methods are adequate for the high-confidence design and manufacture of highly complex, interoperable medical device software and systems ("intelligent" prosthetics, minimally invasive surgical devices, implants, "operating room of the future"), which in years to come will likely include nano/bio devices, bionics, or even pure (programmable) biological systems.

[10] This report is available online at http://www.nitrd.gov/About/MedDevice-FINAL1-web.pdf.

- Today's verification and validation (V&V) efforts are driven by system-life-cycle development activities that rely primarily on methods of post-hoc inspection and testing; these approaches are inadequate in the face of the diversity and complexity of components and interactions in emerging medical devices and systems.
- Today, scientific principles and engineering foundations are lacking that could enable both the design and assurance of high-confidence medical device cyber-physical systems.

Based on their findings, the authors drew the following conclusions:

- Clearly, there is a need for rationally designed high-confidence medical device cyber-physical architectures; a strategic focus on R&D in compositional modeling and design is needed to address the open systems needs, respond to technological innovation, and bridge the jointly cyber and physical aspects of this complex systems problem.
- An open research community of academics and medical device manufacturers is needed to create strategies for development of end-to-end, principled, engineering-based design and development tools. Certifying component devices is necessary, but not sufficient; a key area of research needed is the incremental certified composition of certified components.
- Manufacturers will need access to open, formally composable V&V technology that relies on computational models unifying cyber and physical systems to help establish sufficient evidence. A key V&V research challenge is to understand what is meant by the term "sufficient evidence,"7 its properties, and how this can be accepted in the global economy.
- The HCSS group recommends that a strategic R&D focus on high-confidence networking and IT for the design, implementation, and certification of open medical technologies be undertaken, both to meet the goals of cost-effective, improved patient care and to spur innovation that promotes U.S. leadership in biomedical technology.
- To enable the necessary holistic cyber-physical systems understanding, barriers must fall among the relevant disciplines: medicine, discrete and continuous mathematics of dynamics and control; real-time computation and communication; medical robotics; learning; computational models and the supporting systems engineering design, analysis, and implementation technologies; and formal and algorithmic methods for stating, checking, and reasoning about system properties.
- Incentives are needed to enable effective cooperation between government, industry, and academia to build the underpinning standards and networking and information technology frameworks (e.g., testbeds) for developing open, interoperable medical cyber-physical systems.

Harnessing the Power of Digital Data for Science and Society

This report, published in January 2009, provides a strategy to promote preservation and access to digital scientific data.[11] The report lays out a strategic vision for "a digital scientific data universe in which data creation, collection, documentation, analysis, preservation, and dissemination can be appropriately, reliably, and readily managed, thereby enhancing the return on our nation's research and development investment by ensuring that digital data realize their full potential as catalysts for progress in our global information society." The report includes three key recommendations to pursue this vision. The first is to create an Interagency Subcommittee under NSTC that will focus on goals that are best addressed through continuing broad cooperation and coordination across agencies. The second key element of the strategic framework is for departments and agencies to lay the foundations for agency digital scientific data policy and make the policy publicly available. In laying these foundations, agencies should consider all components of a comprehensive policy to address the full data management life cycle. The third key element is for all agencies to promote a data management planning process for projects that generate scientific data for preservation.

Federal Plan for Advanced Networking Research and Development

This plan, released in September 2008, was developed by the Interagency Task Force on Advanced Networking, established under the NITRD National Science and Technology Council by the Director of the OSTP to provide a strategic vision for future networked environments.[12] The overall conclusions of the Task Force can be summarized as follows:

- Improved networking security and reliability are strategic national priorities;
- New paths to advanced networking are required;
- Federal R&D efforts will support a spectrum of advanced networking capabilities;
- Close cooperation is needed to integrate Federal R&D efforts with the full technology development cycle—this cycle includes basic and applied research, and partnerships with researchers, application developers, users, and other stakeholders; and
- Testbeds and prototype networks enable research on network challenges in realistic environments.

The report notes that

> The Internet's phenomenal growth and elasticity have exceeded all expectations. At the same time, we have become captive to the limitations and vulnerabilities of the current generation of networking technologies. Because vital U.S. interests—for example, national defense communications, financial markets, and the operation of critical infrastructures such as power grids—now depend on secure, reliable, highspeed network connectivity, these limitations and vulnerabilities can threaten our national security and economic competitiveness. Research and development to create the next generation of networking technologies is needed to address these threats.

[11] This report is available online at http://www.nitrd.gov/About/Harnessing_Power_Web.pdf.

[12] This report is available at http://www.nitrd.gov/pubs/ITFAN-FINAL.pdf.

> The plan is centered on a vision for advanced networking based on a design and architecture for security and reliability that provides for heterogeneous, anytime-anywhere networking with capabilities such as federation of networks across domains and widely differing technologies; dynamic mobile networking with autonomous management; effective quality of service (QoS) management; support for sensornets; near-realtime autonomous discovery, configuration, and management of resources; and end-to-end security tailored to the application and user.

The report outlines four goal for realizing this vision:

- Provide secure network services anytime, anywhere;
- Make secure global federated networks possible;
- Manage network complexity and heterogeneity; and
- Foster innovation among the Federal, research, commercial, and other sectors through development of advanced network systems and technologies.

Leadership Under Challenge: Information Technology R&D in a Competitive World

This August 2007 report assesses global U.S. competitiveness in networking and information technology and provides recommendations aimed at ensuring that the NITRD Program is appropriately focused and implemented. The report makes specific recommendations for Federal R&D that would enhance U.S. competitiveness in this economically critical area. In developing the report, the PCAST consulted extensively with experts from industry and academia. The PCAST concluded that while the United States is still in a leadership position, other nations are challenging that lead in a number of areas and that the NITRD Program must focus on visionary research and work with universities to keep the United States at the cutting edge. Some of the report recommendation areas follows:

- Both the U.S. federal government and the private sector need to address the demand for skilled IT professionals, including such steps as updating curricula, increasing fellowships, and simplifying visa processes.
- With respect to the federally-funded research portfolio, the NITRD Program should emphasize larger-scale and longer-term, multidisciplinary IT R&D and innovative, higher-risk projects.
- The United States should give priority to R&D in economically important areas, including IT systems connected with and embedded in the physical world, software, use and management of digital data, and advanced Internet capabilities. The PCAST noted that with an annual federal investment of over $3 billion in the NITRD Program, changes in the Program's interagency process to strengthen assessment and planning are needed.[13]

[13] This report responds to reporting requirements of the High-Performance Computing Act of 1991 P.L. 102-194) and the Next Generation Internet Research Act of 1998 (P.L. 105-305). The laws call for a President's Information Technology Advisory Committee (PITAC) to assess periodically what is now known as the NITRD Program. Executive Order 13385, signed on September 29, 2005, assigned the PITAC's responsibilities to PCAST. This report is available at http://www.nitrd.gov/pcast/reports/PCAST-NIT-FINAL.pdf.

Federal Plan for Cyber Security and Information Assurance Research and Development

In April 2006, the NITRD Subcommittee released its "Federal Plan for Cyber Security and Information Assurance Research and Development."[14] This report sets out a framework for multi-agency coordination of federal R&D investments in technologies that can better secure the interconnected computing systems, networks, and information that together make up the U.S. IT infrastructure. The plan outlines strategic objectives for coordinated federal R&D in cyber security and information assurance (CSIA) and presents a broad range of CSIA R&D technical topics, identifying those topics that are multi-agency technical and funding priorities. The plan's findings and recommendations address R&D priority setting, coordination, fundamental R&D, emerging technologies, roadmapping, and metrics.

NSA Superconducting Technology Assessment

In August 2005, NSA released its "Superconducting Technology Assessment"[15] as part of its participation in the High-End Computing PCA of the NITRD Program. NSA had been concerned about projected limitations of conventional technology and wanted to explore possible alternatives to meet its future mission-critical computational needs. This report presented the results of the technology assessment, which found the following.

- Government investment is necessary, because private industry currently has no compelling financial reason to develop alternative technologies for mainstream commercial applications.
- With aggressive federal investment (estimated between $372 and $437 million over five years), by 2010 next generation technologies would be sufficiently mature to allow the initiation of the design and construction of an operational petaflops[16]-scale system.
- Although significant risks exist, the panel has developed a roadmap that identifies the needed technology developments with milestones and demonstration vehicles.

Computational Science: Ensuring America's Competitiveness

In June 2005, the PITAC released "Computational Science: Ensuring America's Competitiveness."[17] The report identified obstacles to progress in this field, including "rigid disciplinary silos in academia that are mirrored in federal research and development agency organizational structures." According to the report, these "silos stifle the development of multi-disciplinary research and educational approaches essential to computational science." The report recommends the following.

---

[14] This report is available at http://www.nitrd.gov/pubs/csia/csia_federal_plan.pdf.

[15] This report is available at http://www.nitrd.gov/pubs/nsa/sta.pdf.

[16] In computing, "flops" or "FLOPS" is an abbreviation of Floating Point Operations Per Second. This is used as a measure of a computer's performance, especially in fields of scientific calculations that make heavy use of floating point calculations. A petaflops-scale machine operates at 10^{15} flops.

[17] This report is available at http://www.nitrd.gov/pitac/reports/20050609_computational/computational.pdf.

- Both academia and government fundamentally change their organizational structures so that they promote and reward collaborative research.
- The National Science and Technology Council commission the National Academies to convene one or more task forces to develop and maintain a multi-decade roadmap for computational science, with a goal of assuring continuing U.S. leadership in science, engineering, and the humanities.
- The federal government establish national software sustainability centers to harden, document, support, and maintain long-term vital computational science software.
- The federal government provide long-term support for computational science community data repositories. These should include defined frameworks, metadata structures, algorithms, data sets, applications, and review and validation infrastructure. It should also require funded researchers to deposit their data and research software in these repositories or with other approved access providers.
- The federal government provide long-term funding for national high-end computing centers at levels sufficient to ensure the regularly scheduled deployment and operation of the fastest and most capable high-end computing systems that address the most demanding computational problems.
- The federal government implement coordinated, long-term computational science programs that include funding for interconnecting the software sustainability centers, national data and software repositories, and national high-end leadership centers with the researchers who use those resources.
- The federal government should rebalance its R&D investments to: (a) create a new generation of well-engineered, scalable, easy-to-use software suitable for computational science that can reduce the complexity and time to solution for today's challenging scientific applications and can create accurate simulations that answer new questions; (b) design, prototype, and evaluate new hardware architectures that can deliver larger fractions of peak hardware performance on scientific applications; and (c) focus on sensor-and data-intensive computational science applications in light of the explosive growth of data.

Cyber Security: A Crisis of Prioritization

In February 2005, the PITAC released "Cyber Security: A Crisis of Prioritization."[18] That report outlined four key findings and recommendations on how the federal government could "foster new architectures and technologies to secure the Nation's IT infrastructure." Specifically, the PITAC urged the government to

- significantly increase support for fundamental research in civilian cyber security in 10 priority areas;
- intensify federal efforts to promote the recruitment and retention of cyber security researchers and students at research universities;

[18] This report is available at http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf.

- increase support for the rapid transfer of federally-developed cybersecurity technologies to the private sector; and
- strengthen the coordination of federal cybersecurity R&D activities.

Also in February 2005, the NCO released the FY2006 Supplement to the President's Budget.[19] The supplement provides a brief technical outline of the FY2006 budget request for the NITRD Program. The FY2007 Supplement has not yet been released.

NITRD Enabling and Governing Legislation

The NITRD Program is governed by two laws. The first, the High-Performance Computing Act of 1991, P.L. 102-194,[20] expanded federal support for high-performance computing R&D and called for increased interagency planning and coordination. The second, the Next Generation Internet Research Act of 1998, P.L. 105-305,[21] amended the original law to expand the mission of the NITRD Program to cover Internet-related research, among other goals.

High-Performance Computing Act of 1991

This law was the original enabling legislation for what is now the NITRD Program. Among other requirements, it called for the following.

- Setting goals and priorities for federal high-performance computing research, development, and networking.
- Providing for the technical support and research and development of high-performance computing software and hardware needed to address fundamental problems in science and engineering.
- Educating undergraduate and graduate students.
- Fostering and maintaining competition and private sector investment in high-speed data networking within the telecommunications industry.
- Promoting the development of commercial data communications and telecommunications standards.
- Providing security, including protecting intellectual property rights,
- Developing accounting mechanisms allowing users to be charged for the use of copyrighted materials.

This law also requires an annual report to Congress on grants and cooperative R&D agreements and procurements involving foreign entities.[22]

---

[19] This report is available at http://www.nitrd.gov/pubs/2006supplement.

[20] High Performance Computing Act of 1991, P.L. 102-194, 15 U.S.C. 5501, 105 Stat. 1595, December 9, 1991. The full text of this law is available at http://www.nitrd.gov/congressional/laws/pl_102-194.html.

[21] Next Generation Internet Research Act of 1998, P.L. 105-305, 15 U.S.C. 5501, 112 Stat. 2919, October 28, 1998. The full text of this law is available at http://www.nitrd.gov/congressional/laws/pl_h_105-305.html.

[22] The first report mandated information on the "Supercomputer Agreement" between the United States and Japan be included in this report. A separate one-time only report was required on network funding, including user fees, industry (continued...)

Next Generation Internet Research Act of 1998

This law amended the High-Performance Computing Act of 1991. The act had two overarching purposes. The first was to authorize research programs related to high-end computing and computation, human-centered systems, high confidence systems, and education, training, and human resources. The second was to provide for the development and coordination of a comprehensive and integrated U.S. research program to focus on (1) computer network infrastructure that would promote interoperability among advanced federal computer networks, (2) economic high-speed data access that does not impose a "geographic penalty." and (3) flexible and extensible networking technology.

Context of Federal Technology Funding

In the early 1990s, Congress recognized that several federal agencies had ongoing high-performance computing programs,[23] but no central coordinating body existed to ensure long-term coordination and planning. To provide such a framework, Congress passed the High-Performance Computing Program Act of 1991 to improve the interagency coordination, cooperation, and planning of agencies with high performance computing programs.

In conjunction with the passage of the act, OSTP released, "Grand Challenges: High-Performance Computing and Communications." That document outlined an R&D strategy for high-performance computing and communications and a framework for a multi-agency program, the HPCC Program.

The NITRD Program is part of the larger federal effort to promote fundamental and applied IT R&D. The government sponsors such research through a number of channels, including

- federally funded research and development laboratories, such as Lawrence Livermore National Laboratory;
- single-agency programs;
- multi-agency programs, including the NITRD Program, but also programs focusing on nanotechnology R&D and combating terrorism;
- funding grants to academic institutions; and
- funding grants to industry.

In general, supporters contend that federal funding of IT R&D has produced positive results. In 2003, the Computer Science and Telecommunications Board (CSTB) of the National Research

(...continued)

support, and federal investment.

[23] "High-performance" computing is a term that encompasses both "supercomputing" and "grid computing." In general, high-performance computers are defined as stand-alone or networked computers that can perform "very complex computations very quickly." Supercomputing involves a single, stand-alone computer located in a single location. Grid computing involves a group of computers, in either the same location or spread over a number of locations, that are networked together (e.g., via the Internet or a local network). House of Representatives, Committee on Science, *Supercomputing: Is the United States on the Right Path* (Hearing Transcript), http://commdocs.house.gov/committees/science/hsy88231.000/hsy88231_0f.htm, 2003, pp. 5-6.

Council (NRC) released a "synthesis report" based on eight previously released reports that examined "how innovation occurs in IT, what the most promising research directions are, and what impacts such innovation might have on society."[24] One of the most significant of the CSTB's observations was that the unanticipated results of research are often as important as the anticipated results. For example, electronic mail and instant messaging were by-products of [government-funded] research in the 1960s that was aimed at making it possible to share expensive computing resources among multiple simultaneous interactive users.

Additionally, the report noted that federally funded programs have played a crucial role in supporting long-term research into fundamental aspects of computing. Such "fundamentals" provide broad practical benefits, but generally take years to realize. Furthermore, supporters state that the nature and underlying importance of fundamental research makes it less likely that industry would invest in and conduct more fundamental research on its own. As noted by the CSTB, "companies have little incentive to invest significantly in activities whose benefits will spread quickly to their rivals."[25] Further, in the Board's opinion:

> government sponsorship of research, especially in universities, helps develop the IT talent used by industry, universities, and other parts of the economy. When companies create products using the ideas and workforce that result from federally-sponsored research, they repay the nation in jobs, tax revenues, productivity increases, and world leadership.[26]

Another aspect of government-funded IT R&D is that it often leads to open standards, something that many perceive as beneficial, encouraging deployment and further investment. Industry, on the other hand, is more likely to invest in proprietary products and will diverge from a common standard if it sees a potential competitive or financial advantage; this has happened, for example with standards for instant messaging.[27]

Finally, proponents of government R&D support believe that the outcomes achieved through the various funding programs create a synergistic environment in which both fundamental and application-driven research are conducted, benefitting government, industry, academia, and the public. Supporters also believe that such outcomes justify government's role in funding IT R&D, as well as the growing budget for the NITRD Program.

Critics assert that the government, through its funding mechanisms, may be setting itself up to pick "winners and losers" in technological development, a role more properly residing with the private sector.[28] For example, the size of the NITRD Program may encourage industry to follow the government's lead on research directions rather than selecting those directions itself.

---

[24] National Research Council, *Innovation in Information Technology*, 2003, p. 1. This report discusses all federal funding for R&D, not only the NITRD Program.

[25] Ibid, p. 4.

[26] Ibid, p. 4.

[27] Ibid, p. 18.

[28] Cato Institute, *Encouraging Research: Taking Politics Out of R&D*, September 13, 1999, http://www.cato.org/pubs/wtpapers/990913catord.html.

Overall, CSTB states that, government funding appears to have allowed research on a larger scale and with greater diversity, vision, and flexibility than would have been possible without government involvement.[29]

Congressional Activity

In the 111th Congress, four bills have been introduced that relate to the NITRD Program.

H.R. 1, the American Recovery and Reinvestment Act of 2009 (P.L. 111-5), was signed into law on February 17, 2009. Prior to being signed by the President, H.R. 1 was amended to include two other related bills, H.R. 598 and H.R. 629.

The fourth bill, H.R. 2020, the Networking and Information Technology Research and Development Act of 2009, was introduced by Representative Bart Gordon on April 22, 2009; it was passed by the House of Representatives and referred to the Senate Committee on Commerce, Science, and Transportation on May 13, 2009 (see H.Rept. 111-102). The purpose of this bill is to strengthen the planning and coordination mechanisms of the NITRD Program and to update the research content of the program. The legislation implements a number of recommendations made in a recent PCAST assessment of the program.

Issues for Congress

Federal IT R&D is a multi-dimensional issue, involving many government agencies working together towards shared and complementary goals. Most observers believe that success in this arena requires ongoing coordination among government, academia, and industry.

Through hearings, the House Committee on Science has been investigating issues related to U.S. competitiveness in high-performance computing and the direction the IT R&D community has been taking. Those issues and others remain salient and may merit further investigation if the United States is to maintain a comprehensive IT R&D policy. Included among the possible issues Congress may wish to pursue are: the United States' status as the global leader in high-performance computing research; the apparent bifurcation of the federal IT R&D research agenda between grid computing and supercomputing capabilities; the possible over-reliance on commercially available hardware to satisfy U.S. research needs; and the potential impact of deficit cutting on IT R&D funding.

Many Members of Congress as well as those in the research community have expressed concern over whether the United States is maintaining its position as the global leader in high-performance computing R&D. That concern was highlighted in 2003 when Japan briefly surpassed the United States in possessing the fastest and most efficient supercomputer in the world.[30] While this was a reason for some concern, it was also viewed by some as an indicator of how the United States' research agenda had become bifurcated, with some in the R&D community focusing on traditional supercomputing capabilities, and others focusing more on

[29] National Research Council, *Innovation in Information Technology*, 2003, p. 22.

[30] House of Representatives, Committee on Science, *Supercomputing: Is the United States on the Right Path*? (Hearing Transcript), http://commdocs.house.gov/committees/science/hsy88231.000/hsy88231_0f.htm, 2003, p. 13.

cluster computing or grid computing. Each type of computing has its advantages, based on its application. Stand-alone supercomputers are often faster and are generally used to work on a specific problem. For example, cryptanalysis and climate modeling applications require significant computing power and are best accomplished using specialized, stand-alone computers. Cluster computing, however, allows the use of commercially available hardware, which helps contain costs. The cluster configuration is useful for applications in which a problem can be broken into smaller independent components.[31] Therefore, one possible course for Congress could be to monitor closely the work that was begun by the High-End Computing Revitalization Task Force and is now being performed by the NITRD Program's High-End Computing Interagency Working Group and provide ongoing feedback and guidance.

Without a clear plan as to how to proceed, pursuing two disparate research agendas (with goals that could be viewed as being at odds with each other) could split the research community further, damaging its ability to provide leadership in either area. The NITRD Program already is working on a "roadmap" for future directions in supercomputing; therefore, one possible course for Congress at this time would be to monitor closely the work of the High-End Computing Revitalization Task Force and provide input or a more visible forum for discussion (i.e., additional hearings involving task force participants). Congress may wish to conduct its own inquiry into the debate over grid versus stand-alone computing.

Another issue is whether the United States is relying too heavily on commercially available hardware to satisfy its R&D needs. While use of computers designed for mass-market commercial applications can certainly be a part of a successful high-end computing R&D plan, Congress may wish to monitor how this reliance may be driving the new emphasis on grid computing.

As noted earlier, critics of IT R&D funding often state that industry should conduct more fundamental R&D on their own, without government backing, and that fiscal restraint dictates that less funding should be made available. Conversely, supporters of government funding would point out that IT R&D has a very long cycle from inception to application and that any reductions in funding now could have a significant negative impact for many years to come in terms of innovation and training of researchers. Therefore, Congress may monitor and assess the potential impact of deficit-cutting plans on progress in IT R&D.

Author Contact Information

Patricia Moloney Figliola
Specialist in Internet and Telecommunications Policy
pfigliola@crs.loc.gov, 7-2508

[31] Ibid, p. 6-7.