

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

Patricia Moloney Figliola
Specialist in Internet and Telecommunications Policy

August 30, 2012

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.

Current concerns are the role of the federal government in supporting IT R&D and the level of funding to allot to it. Proponents of federal support of information technology (IT) R&D assert that it 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. 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 FY2013 budget request for the NITRD Program is $3.808 billion, an increase of $69 million more than the $3.739 billion FY2012 estimate. Actual NITRD spending in FY2011 totaled $3.727 billion.

Three pieces of legislation have been introduced in the 112th Congress that would have an effect on the NITRD Program and its member agencies: H.R. 3834, the Advancing America's Networking and Information Technology Research and Development Act of 2012; H.R. 2096, the Cybersecurity Enhancement Act of 2011; and S. 1152, also called the Cybersecurity Enhancement Act of 2011. H.R. 2096 and S. 1152 are identical.

Two hearings have been held related to the NITRD Program, the first on federal R&D efforts to protect information in the digital age (May 25, 2011) and the second on program oversight (September 21, 2011).

Contents

The Federal NITRD Program 1
Structure 1
Budget, Funding, and Spending 3
Reports, 2010-2012 3
NITRD Program 2012 Strategic Plan 3
Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program 4
Designing a Digital Future: Federally Funded Research and Development in Networking Information and Technology 5
Federal Technology Funding: Background and Context 6
Activity in the 112th Congress 7
Legislation 8
H.R. 3834—Advancing America's Networking and Information Technology Research and Development Act of 2012 8
H.R. 2096 and S. 1152—Cybersecurity Enhancement Act of 2011 9
Hearings 10
Protecting Information in the Digital Age: Federal Cybersecurity Research and Development Efforts 10
Oversight of the Networking and Information Technology Research and Development Program and Priorities for the Future 10
Potential Issues for Congress 10

Figures

Figure 1. Management Structure of the NITRD Program 2

Appendixes

Appendix. NITRD Enabling and Governing Legislation 11

Contacts

Author Contact Information 12

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 and software that would be capable of addressing the problems and issues the government needed to solve and study. One of the first such problems was calculating the trajectories of artillery and bombs; more recently, such problems include simulations of nuclear testing, cryptanalysis, and weather modeling. That interest continues today. These complex issues have led to calls for coordination to ensure the government's evolving needs (e.g., homeland security) will continue to be met in the most effective manner possible.

Structure

Established by the High-Performance Computing Act of 1991 (P.L. 102-194), the Networking and Information Technology Research and Development (NITRD) Program is the primary mechanism by which the federal government coordinates its unclassified networking and information technology (NIT) R&D investments. Eighteen federal agencies, including all of the large science and technology agencies, are formal members of the NITRD Program,[1] with many other federal entities participating in NITRD activities. The program aims to ensure that the nation effectively leverages its strengths, avoids duplication, and increases interoperability in such critical areas as supercomputing, high-speed networking, cybersecurity, software engineering, and information management. **Figure 1** illustrates the organizational structure of the NITRD Program.

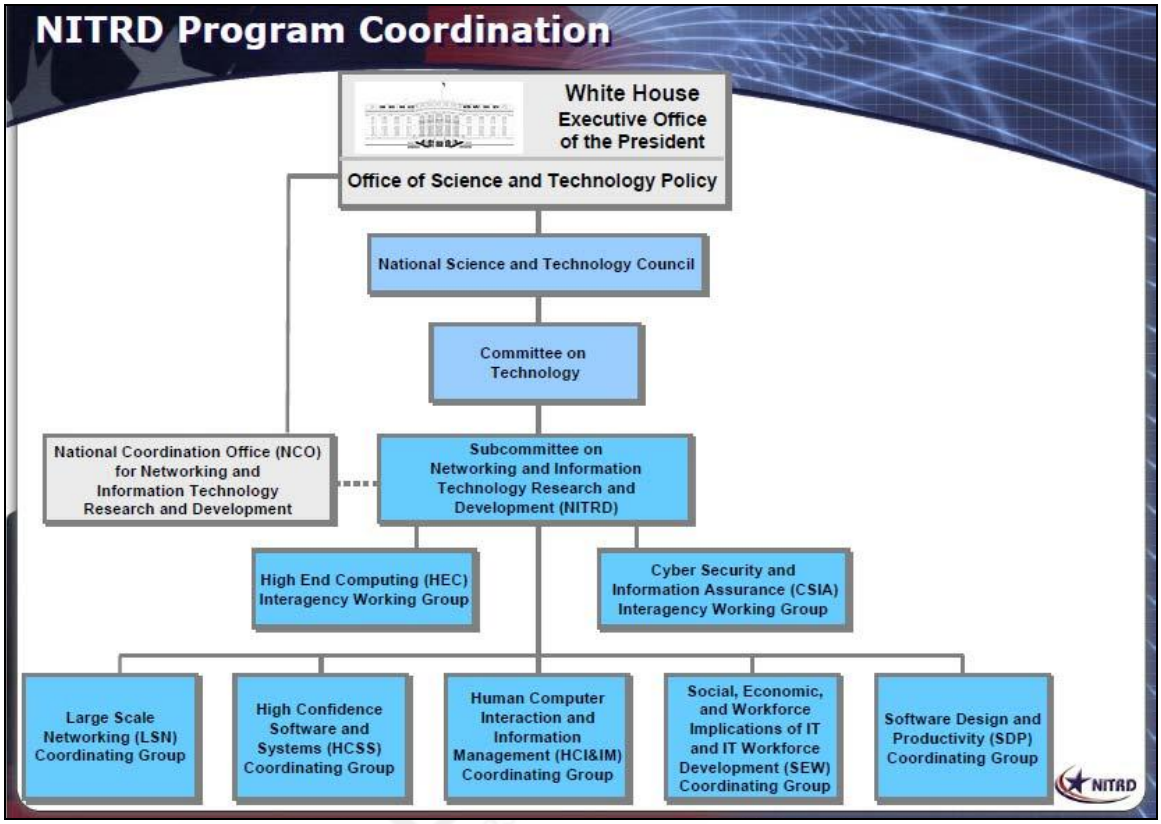
The National Coordinating Office (NCO) coordinates the activities of the NITRD Program. The NCO was first established in September 1992 and was initially called the National Coordination Office for High Performance Computing and Communications (NCO/HPCC). Its name has changed several times over the years; as of July 2005, it is referred to as the National Coordination Office for Networking and Information Technology Research and Development (NCO/NITRD). The NCO/NITRD supports the planning, coordination, budget, and assessment activities of the Program. The NCO's role in the NITRD enterprise is recognized in the National Science and Technology Council (NSTC) charters, authorizing NITRD Program structures as well as in legislation and congressional hearings. The Director of the White House Office of Science Technology and Policy (OSTP) appoints a Director for the NCO. The Director of the NCO reports to the Director of the White House Office on Science and Technology Policy (OSTP). The NCO supports the National Science and Technology Council's Subcommittee on NITRD (also called the NITRD Subcommittee).[2] The NITRD Subcommittee provides policy,

[1] Department of Commerce (DOC): National Institute of Standards and Technology (NIST), National Oceanic and Atmospheric Administration (NOAA); Department of Defense (DOD): Defense Advanced Research Projects Agency (DARPA), National Security Agency (NSA), Office of the Secretary of Defense (OSD) and Service Research Organizations (Air Force Office of Scientific Research (AFOSR), Air Force Research Laboratory (AFRL), Army Research Laboratory (ARL), Office of Naval Research (ONR); Department of Energy (DOE): National Nuclear Security Administration (DOE/NNSA), Office of Science (DOE/SC); Department of Homeland Security (DHS); Department of Health and Human Services (HHS): Agency for Healthcare Research and Quality (AHRQ), National Institutes of Health (NIH), Office of the National Coordinator for Health Information Technology (ONC); Environmental Protection Agency (EPA); National Aeronautics and Space Administration (NASA); National Archives and Records Administration (NARA); National Science Foundation (NSF).

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

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.

Figure 1. Management Structure of the NITRD Program



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

NITRD Program activities are described under a set of eight Program Component Areas (PCAs),[3] four Senior Steering Groups (SSGs),[4] and a Community of Practice (CoP).[5] The PCAs are identified as an Interagency Working Group (IWG) or a Coordinating Group (CG) and report their R&D budgets as a crosscut of the NITRD agencies. They are charged with facilitating interagency program planning, developing and periodically updating interagency roadmaps, developing recommendations for establishing federal policies and priorities, summarizing annual activities for the NITRD program's Supplement to the President's Budget, and identifying potential opportunities for collaboration which has been identified by OMB and OSTP as priorities for federal coordination and collaboration. In addition to the PCAs, NITRD has

[3] Cyber Security and Information Assurance (CSIA); High-Confidence Software and Systems (HCSS); High-End Computing Infrastructure and Applications (HEC I&A); High-End Computing Research and Development (HEC R&D); Human-Computer Interaction and Information Management (HCI&IM); Large-Scale Networking (LSN); Social, Economic, and Workforce Implications of IT and IT Workforce Development (SEW); Software Design and Productivity (SDP).

[4] Big Data SSG; Cyber Security and Information Assurance R&D SSG; Health Information Technology R&D SSG; Wireless Spectrum R&D SSG.

[5] Faster Administration of Science and Technology Education and Research (FASTER) Community of Practice (CoP).

established several Senior Steering Groups (SSGs). The SSGs allow a more flexible model for NITRD collaboration and are formed to focus on emerging issues as required by a mandate from OSTP. SSGs do not report an R&D budget under NITRD. The CoP's goal is to enhance collaboration and accelerate agencies' adoption of advanced IT capabilities developed by government-sponsored IT research. The NITRD Subcommittee convenes three times a year and the working groups meet approximately 12 times annually and provide input to the NITRD Supplement to the President's Budget.

Budget, Funding, and Spending[6]

The NITRD budget is an aggregation of the IT R&D components of the individual budgets of NITRD-participating agencies and is reported in the annual release of *The Networking and Information Technology Research and Development Program Supplement to the President's Budget*. The NITRD budget is not a single, centralized source of funds that is allocated to individual agencies. In fact, the agency IT R&D budgets are developed internally as part of each agency's overall budget development process. These budgets are subjected to review, revision, and approval by the Office of Management and Budget and become part of the President's annual budget submission to Congress. The NITRD budget is then calculated by aggregating the IT R&D components of the appropriations provided by Congress to each federal agency.

The President's FY2013 budget request for the NITRD Program is $3.808 billion, an increase of $69 million more than the $3.739 billion FY2012 estimate. Actual NITRD spending in FY2011 totaled $3.727 billion.[7] Differences between the President's Budget request for a given year and estimated spending for that year reflect revisions to program budgets due to evolving priorities, as well as congressional actions and appropriations. In addition, the NITRD agencies have continued to work collectively on improving the PCA definitions, as reflected by changes in the definitions outlined in OMB Circular A-11, and individually on improving the classification of investments within the PCAs, resulting in changes in the NITRD Program.

Reports, 2010-2012[8]

As explained earlier, the NCO provides technical and administrative support to the NITRD Program and the NITRD Subcommittee. This includes supporting meetings and workshops and preparing reports. The NCO interacts with OSTP and Office of Management and Budget (OMB) on NITRD Program matters. Additionally, in accordance with a presidential executive order and law, the NITRD Program is reviewed biannually.

NITRD Program 2012 Strategic Plan

In July 2012, the NTSC and NCO released the five-year strategic plan for the NITRD Program. This plan responds to the August 2007 assessment of the NITRD Program by the PCAST,

[6] The full history of NITRD Program funding, dating to 1991, is available online at http://www.nitrd.gov/pubs/2009supplement/nitrd_history/NITRD-crosscut.pdf.

[7] NITRD Supplement to the President's Budget, FY2013, online at http://www.nitrd.gov/PUBS/2013supplement/FY13NITRDSupplement.pdf.

[8] All NITRD reports are available online at http://www.nitrd.gov/Publications/index.aspx.

Leadership Under Challenge: Information Technology R&D in a Competitive World.[9] In this report, the PCAST recommended that NITRD "develop, maintain, and implement a cohesive strategic plan" that includes "a comprehensive technology vision and strategy that identify the next generation and future generations of important networking and information technology challenges and describe how to meet those challenges."

This plan presents the NCO's overarching vision for the digital world in the 21st century—a world in which high-speed networks, systems, software, devices, data, and applications are fully secure, safe, reliable, multimodal, and easy to use. In the envisioned future, next-generation IT infrastructure and capabilities will enable continued U.S. leadership in economic innovation, scientific discovery, national security, education, and quality of life. To realize this vision, the plan calls for advancing U.S. capabilities in three broad areas identified as the essential "foundations" for sustained leadership in a digital world:

- WeCompute—Expanded human-computer partnerships, including more capable, available, and affordable systems; more powerful digital tools for people; and new forms of collaboration between the two.
- Trust and Confidence—The ability to design and build systems with levels of security, safety, privacy, reliability, predictability, and dependability that "you can bet your life on."
- Cyber Capable—Transformed education and training to ensure that current generations benefit fully from cyber capabilities and to inspire a diverse, prepared, and highly productive next-generation workforce of cyber innovators.

The strategic plan discusses the topical elements of each foundation and summarizes the principal research and education challenges that need to be addressed, providing a comprehensive research and education strategy for the future. The plan concludes that the NITRD Program should pursue expanded multiagency collaboration; cultivate new forms of partnership with academia and industry; and continue to lead by example in multidisciplinary activities and identification of critical-path research needs.

Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program

In December 2011, the NSTC released, *Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program*.[10] The report defines a set of interrelated priorities for the agencies of the U.S. government that conduct or sponsor R&D in cybersecurity. The priorities are organized into four thrusts: Inducing Change, Developing Scientific Foundations, Maximizing Research Impact, and Accelerating Transition to Practice.

The thrusts provide a framework for prioritizing cybersecurity R&D in a way that concentrates research efforts on limiting current cyberspace deficiencies, precluding future problems, and expediting the infusion of research accomplishments into the marketplace. The principal objectives of the thrusts include achieving greater cyberspace resiliency, improving attack

[9] This report is available online at http://www.nsf.gov/geo/geo-data-policies/pcast-nit-final.pdf.

[10] This report is available online at http://www.whitehouse.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf.

prevention, developing new defenses, and enhancing U.S. capabilities to design software that is resistant to attacks.

The Inducing Change thrust includes a new priority theme named Designed-in Security, together with the existing themes of Tailored Trustworthy Spaces, Moving Target, and Cyber Economic Incentives. The Designed-in Security theme focuses on developing capabilities to design and evolve high-assurance systems resistant to cyberattacks, whose assurance properties can be verified. Such development capabilities offer the path to dramatic increases in the security and safety of software systems.

Explicit in the execution of this plan is the coordination process across government agencies through the NITRD Program and the leadership function of the NITRD Cyber Security and Information Assurance Interagency Working Group (CSIA IWG), the federal government's principal group for coordinating cybersecurity R&D activities. In conjunction with OSTP, the NITRD Senior Steering Group for Cybersecurity R&D, and the Special Cyber Operations Research and Engineering SCORE Interagency Working Group, the CSIA IWG assures that the execution of this plan by individual federal research agencies is coordinated, cohesive, and complementary.

Designing a Digital Future: Federally Funded Research and Development in Networking Information and Technology

In December 2010, the President's Council of Advisors on Science and Technology (PCAST)[11] released, *Designing a Digital Future: Federally Funded Research and Development in Networking and Information Technology*.[12] This report fulfilled PCAST's responsibility to report on the status of the NITRD Program under Executive Order 13539 and the High-Performance Computing Act of 1991 (P.L. 102-194).[13] PCAST appointed an expert 14-member Working Group, which consulted with more than 50 individuals, including government officials, industry representatives, and experts from academia, to develop a comprehensive review of the program. PCAST found that NITRD is well coordinated and that the U.S. computing research community, coupled with a vibrant NIT industry, has made seminal discoveries and advanced new technologies that are helping to meet many societal challenges. Importantly, however, PCAST also found that:

> a substantial fraction of the NITRD multi-agency spending summary represents spending that supports R&D in other fields, rather than spending on R&D in the field of NIT itself. As a result, the United States is actually investing far less in NIT R&D than the $4 billion-plus indicated in the Federal budget. To achieve America's priorities and advance key research frontiers to support economic competitiveness in NIT, this report calls for a more accurate accounting of this national investment and recommended additional investments in NIT R&D, including research in networking and information technology for health, energy and transportation, and cyber-infrastructure.[14]

[11] The PCAST was acting in its role as the President's Innovation and Technology Advisory Council (PITAC).

[12] This report is available online at http://www.nitrd.gov/pcast-2010/report/nitrd-program/pcast-nitrd-report-2010.pdf.

[13] As amended by the Next Generation Internet Research Act of 1998 (P.L. 105-305) and by the America COMPETES Act of 2007 (P.L. 110-69).

[14] Designing a Digital Future: Federally Funded Research and Development in Networking and Information Technology, p. v.

The PCAST stated its belief that NIT has yielded enormous benefits for the nation's economic competitiveness, national security, and quality of life. It stressed the importance of maintaining the country's leadership in NIT in an ever more competitive global environment, encouraging the federal government to be bold in its investments, including funding of high risk/high reward research with the potential to move NIT in unanticipated directions.

Federal Technology Funding: Background and Context

In the early 1990s, Congress recognized that several federal agencies had ongoing high-performance computing programs,[15] 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 of federal funding of IT R&D contend that it has produced positive results. In 2003, the Computer Science and Telecommunications Board (CSTB) of the National Research 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."[16] The CSTB's observation was that the

[15] "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.

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

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."[17] 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.[18]

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 typically diverge from a common standard if it sees a potential competitive or financial advantage; this happened, for example, with standards for instant messaging.[19]

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 have asserted that the government, through its funding mechanisms, may set itself up to pick "winners and losers" in technological development, a role more properly residing with the private sector.[20] For example, the size of the NITRD Program could encourage industry to follow the government's lead on research directions rather than selecting those directions itself.

Overall, CSTB stated 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.[21]

Activity in the 112th Congress

Two bills have been introduced that would affect the NITRD Program and one hearing has been held that addressed the activities of the NITRD Program member agencies.

[17] Ibid, p. 4.

[18] Ibid, p. 4.

[19] Ibid, p. 18.

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

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

Legislation

Three pieces of legislation have been introduced in the 112th Congress that would have an effect on the NITRD member agencies: H.R. 3834, the Advancing America's Networking and Information Technology Research and Development Act of 2012; H.R. 2096, the Cybersecurity Enhancement Act of 2011; and S. 1152, also called the Cybersecurity Enhancement Act of 2011. H.R. 2096 and S. 1152 are identical.

H.R. 3834—Advancing America's Networking and Information Technology Research and Development Act of 2012[22]

H.R. 3834 was introduced by Representative Ralph Hall on January 27, 2012. The bill was reported (H.Rept. 112-420)[23] by the Committee on Science, Space, and Technology on March 22, 2012, and passed April 27, 2012. It was referred to the Senate Committee on Commerce, Science, and Transportation on May 7, 2012. This bill would:

- Amend the High-Performance Computing Act of 1991 to rename the National High-Performance Computing Program as the NITRD Program.
- Direct the federal agencies participating in the Program to (1) periodically assess the contents and funding levels of program component areas and restructure the Program when warranted; and (2) ensure that the Program includes large-scale, long-term, interdisciplinary R&D activities.
- Require the participating federal agencies to develop, and update every three years, a five-year strategic plan to guide activities provided for under the Program.
- Require the Director of the OSTP to encourage and monitor the efforts of participating agencies to allocate the resources and management attention necessary to ensure that the strategic plan is executed effectively and that Program objectives are met.
- Require the Program, in addition to its current requirements, to provide for (1) increased understanding of the scientific principles of cyber-physical systems and improve the methods available for the design, development, and operation of such systems; and (2) research and development on human-computer interactions, visualization, and big data.
- Require continuation of an NCO and require the Director of the Office to convene (1) a task force to explore mechanisms for carrying out collaborative R&D activities on cyber-physical systems; and (2) through the NTSC, an interagency working group to examine issues around funding mechanisms and

[22] H.R. 4263, the SECURE IT Act of 2012, is a related bill to H.R. 3834. Section 407 of the bill contains conforming and technical amendments to the High-Performance Computing Act of 1991. However, it does not change the functions of the program or its management structure. That bill was introduced by Representative Mary Bono on March 27, 2012, and referred to the House Committees on Science, Space, and Technology; Oversight and Government Reform; Judiciary; Armed Services; and Intelligence (Permanent Select). It was referred to the House Subcommittee on Crime, Terrorism, and Homeland Security on April 9, 2012.

[23] This document is available online at http://www.gpo.gov/fdsys/pkg/CRPT-112hrpt420/pdf/CRPT-112hrpt420.pdf.

policies for the use of cloud computing services for federally funded science and engineering research.

H.R. 2096 and S. 1152—Cybersecurity Enhancement Act of 2011

H.R. 2096 was introduced by Representative Michael McCaul on June 2, 2011. The bill was reported (amended) on October 31, 2011 (H.Rept. 112-264). It was passed by the House and referred to the Senate Committee on Commerce, Science, and Transportation on May 7, 2012.

S. 1152 was introduced by Senator Robert Menendez on June 7, 2011. The bill was referred to the Senate Committee on Commerce, Science, and Transportation, and no further action has been taken.

These bills would—

- Require NITRD member agencies to provide to Congress a cybersecurity strategic research and development plan and triennial updates, and develop and annually update an implementation roadmap for such plan.
- Expand permitted National Science Foundation (NSF) grants for basic research on innovative approaches to the structure of computer and network hardware and software that are aimed at enhancing computer security to include research into identity management, crimes against children, and organized crime.
- Require applications for the establishment of Computer and Network Security Research Centers to include a description of how such Centers will partner with government laboratories, for-profit entities, other institutions of higher education, or nonprofit research institutions.
- Repeal the Cyber Security Faculty Development Traineeship Program.
- Require the NSF Director to continue carrying out a Scholarship for Service program under the Cyber Security Research and Development Act.
- Direct the President to transmit a report to Congress addressing the cybersecurity workforce needs of the federal government.
- Require the Office of Science and Technology Policy (OSTP) Director to convene a cybersecurity university-industry task force to explore mechanisms for carrying out collaborative R&D activities.
- Revise provisions concerning the development and dissemination by the National Institute of Standards and Technology (NIST) of security risk checklists associated with computer systems that are, or are likely to become, widely used within the federal government.
- Require conducting intramural security research activities under NIST's computing standards program.
- Require the NIST Director to (1) ensure coordination of U.S. government representation in the international development of technical standards related to cybersecurity; (2) maintain a cybersecurity awareness and education program through the Hollings Manufacturing Extension Partnership program; and (3) continue a program to support development of technical standards, metrology,

testbeds, and conformance criteria with regard to identity management research and development.

Hearings

Two hearings have been held related to the NITRD Program.

Protecting Information in the Digital Age: Federal Cybersecurity Research and Development Efforts

"Protecting Information in the Digital Age: Federal Cybersecurity Research and Development Efforts," was held by the House Committee on Science and Technology Subcommittees on Technology and Innovation and Research and Science Education, on May 25, 2011, on issues relating specifically to cybersecurity R&D.[24]

Oversight of the Networking and Information Technology Research and Development Program and Priorities for the Future

"Oversight of the Networking and Information Technology Research and Development Program and Priorities for the Future," was held by the House Committee on Science and Technology Subcommittee Research and Science Education, on September 21, 2011, on issues relating to future research directions.[25]

Potential Issues for Congress

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

Issues related to U.S. competitiveness in high-performance computing and the direction the IT R&D community has been taking have remained salient over the last 5 to 10 years and include:

- the United States' status as the global leader in high-performance computing research;
- the apparent ongoing bifurcation of the federal IT R&D research agenda between grid computing and supercomputing capabilities;
- 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.

[24] The hearing main page can be found at http://science.house.gov/hearing/subcommittee-research-and-science-education-subcommittee-technology-and-innovation-%E2%80%93-joint. Information includes the hearing charter, the opening statements, and the witness testimony.

[25] The hearing main page can be found at http://science.house.gov/hearing/research-and-science-education-subcommittee-hearing-oversight-networking-information-tech.

Appendix. 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,[26] 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,[27] 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.[28]

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

[26] 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.

[27] 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.

[28] 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 support, and federal investment.

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.

Author Contact Information

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