

## MEMORANDUM

TO: Committee on Science, Space, and Technology Members and Staff  
FROM: Science, Space, and Technology Committee Staff  
DATE: March 11, 2013  
RE: Full Committee Markup

The Committee on Science, Space, and Technology will meet on **Thursday, March 14, 2013, at 10:00 a.m.** in Room 2318 of the Rayburn House Office Building to consider the following:

- **H.R. 756, *Cybersecurity Enhancement Act of 2013***
- **H.R. 967, *Advancing America's Networking and Information Technology Research and Development Act of 2013***

### **H.R. 756, *Cybersecurity Enhancement Act of 2013***

#### **Background and Need**

Information technology (IT) has evolved rapidly over the last decade, leading to markedly increased connectivity and productivity. The benefits provided by these advancements have led to the widespread use and incorporation of information technologies across major sectors of the economy. This level of connectivity and the dependence of our critical infrastructures on IT have also increased the vulnerability of these systems. Reports of cyber criminals and nation-states accessing sensitive information and disrupting services have risen steadily over the last decade, heightening concerns over the adequacy of our cybersecurity measures.

According to the Office of Management and Budget, Federal agencies spent \$8.6 billion in FY 2010 on cybersecurity and the Federal government has spent more than \$600 billion on information technology in the last decade. In addition, the Federal government funds nearly \$400 million in cybersecurity research and development each year.

In January 2008, the Bush Administration established, through a series of classified executive directives, the *Comprehensive National Cybersecurity Initiative* (CNCI). The Obama Administration has continued this initiative, with the goal of securing Federal systems and fostering public-private cooperation.

On May 29, 2009, the Obama Administration released its *Cyberspace Policy Review*. The Review recommended an increased level of interagency cooperation among all departments and agencies, highlighted the need for information sharing concerning attacks and vulnerabilities, and highlighted the need for an exchange of research and security strategies essential to the efficient and effective defense of Federal computer systems.

Furthermore, it stressed the importance of advancing cybersecurity research and development, and the need for the Federal Government to partner with the private sector to

guarantee a secure and reliable infrastructure. The Review also called for increased public awareness, improved education and expansion of the number of information technology professionals.

In June 2009, GAO found that the Federal agencies responsible for protecting the U.S. Information Technology (IT) infrastructure were not satisfying their responsibilities, leaving the Nation's IT infrastructure vulnerable to attack. In an effort to strengthen the work of those Federal agencies, the U.S. House of Representatives passed the *Cybersecurity Enhancement Act of 2011* (H.R. 2096) in the 112<sup>th</sup> Congress. H.R. 2096 required increased coordination and prioritization of Federal cybersecurity research and development activities, and the development and advancement of cybersecurity technical standards. It also strengthened cybersecurity education and talent development and industry partnership initiatives. The Senate did not act on the legislation.

The bill was reintroduced in the 113<sup>th</sup> Congress as H.R. 756, the *Cybersecurity Enhancement Act of 2013*.

## **Major Provisions**

### ***Cybersecurity Strategic Coordination***

- Cybersecurity R&D agencies are tasked to work through the National Science and Technology Council and National Coordination Office of the National Information Technology Research and Development (NITRD) program to develop a strategic plan to guide the overall direction of federal cybersecurity and information assurance R&D.
- The bill requires that the Director of the Office of Science and Technology Policy (OSTP) convene a university-industry task force to explore mechanisms for carrying out collaborative R&D.
- The bill also requires the President to conduct an assessment of cybersecurity workforce needs across the federal government

### ***National Science Foundation (NSF)***

- The bill reauthorizes cybersecurity workforce and traineeship programs at NSF and formally codifies NSF to carry out the "Scholarship for Service" program, detailing the components of the program.
- The bill reauthorizes and updates cybersecurity research areas and grants at NSF through the *Cybersecurity R&D Act* (15 U.S.C. 7406(c)), including the "Secure and Trustworthy Cyberspace" program and other research grants.

## ***National Institute of Standards and Technology (NIST)***

- The bill updates provisions of the *Cybersecurity R&D Act* (15 U.S.C. 7406(c)) by requiring the Director of NIST to develop or identify checklists, configuration profiles, and deployment recommendations for cybersecurity software and hardware used by the Federal government. The bill also amends the *NIST Act* (15 U.S.C. 278g-3), to update NIST's research program aimed at creating a standardized identity, privilege, and access control management framework and directs NIST to conduct research on how to improve the security of information systems, networks, and industrial control systems.
- *The NIST Act* (15 U.S.C. 278g-3) is amended to codify NIST cybersecurity research and development activities; NIST is authorized to conduct research on a standardized identity management framework and to conduct research related to improving the security of information and networked systems, including the security of industrial control systems.
- The bill directs NIST to develop and implement a proactive plan to ensure coordinated Federal agency engagement in international cybersecurity technical standards development. This plan is due to Congress within one year of enactment.
- NIST is required to collaborate with other entities to develop a strategy to encourage the use of cloud computing services by the Federal Government.
- NIST is also required to deliver a plan to Congress, within one year of enactment, describing how it will develop and implement a cybersecurity awareness and education program. NIST is to collaborate with relevant federal agencies, industry and educational institutions in developing this program.

## **Legislative History**

In the 112<sup>th</sup> Congress, the Subcommittees on Technology and Innovation and Research and Science Education held a joint hearing on May 25, 2011, to review how NSF, NIST, DHS, and the NITRD program continue to respond to and address cybersecurity issues, including any potential updates to H.R. 4061, which was the Cybersecurity Enhancement Act of 2010. On June 2, 2011, Representatives Mike McCaul and Dan Lipinski reintroduced H.R. 4061 as H.R. 2096, the *Cybersecurity Enhancement Act of 2011*. H.R. 2096 passed the House of Representatives on April 27, 2012 by a vote of 395-10.

In the 113<sup>th</sup> Congress, H.R. 756, the "Cybersecurity Enhancement Act of 2013" was introduced on February 15, 2013, by Rep. McCaul, Rep. Lipinski, Rep. Smith, Rep. Langevin, Rep. Meehan, Rep. Matsui, Rep. Hall, and Rep. Lujan.

On February 26, 2013, the Technology and Research Subcommittees held a joint hearing on “Cybersecurity Research and Development: Challenges and Solutions,” which also investigated H.R. 756.

***H.R. 967, Advancing America’s Networking and Information Technology Research and Development Act of 2013***

**Background and Need**

Advances in networking and information technology (NIT) continue to transform the world in which we live. We increasingly rely on the systems, tools, and services of this ever-growing and ever-changing domain. It is not only as a matter of convenience in our daily lives, but critical to our future economic prosperity, health, and security.

Federal support for research and development (R&D) in NIT originally stemmed from an interest in and the challenge of developing computers capable of addressing complex problems, primarily those focused on national security and global competition. Today, NIT encompasses a broad array of technologies from smart phones to digital libraries and cloud computing.

R&D in NIT provides a greater understanding of how to protect essential systems and networks, systems and networks that support fundamental sectors of our economy, from emergency communications and power grids to air-traffic control networks and national defense systems in an effort to support a more stable and secure Nation. NIT R&D works to prevent or minimize disruptions to critical information infrastructure, to protect public and private services and to detect and respond to threats while mitigating the severity of and assisting in the recovery from those threats.

***Networking and Information Technology Research and Development Program (NITRD)***

Congress originally authorized the Networking and Information Technology Research and Development (NITRD) program in the High-Performance Computing Act of 1991 (P.L. 102-194), after recognizing that a number of federal agencies had ongoing high-performance computing programs without a coordinating body. The Act established that coordinating body to improve interagency coordination, cooperation, and planning among those agencies with high-performance computing programs. In addition, it authorized a multi-agency research effort, called the High-Performance Computing and Communications program, 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 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 Act has since been amended through the Next Generation Internet Research Act of 1998 and the America COMPETES Act of 2007.

The NITRD program is the main federal R&D investment portfolio in networking, computing, software, cyber security, and related information technologies. NITRD coordinates this unclassified R&D across 14 federal agencies. Additional agencies that do not contribute funding also participate in NITRD planning activities.

The NITRD program has played a role in several important technological advances including the computational decoding of the human genome; modeling and simulation of complex physical systems (aircraft, automobiles, power grids, and pharmaceuticals); unmanned aerial vehicles, search-and-rescue robots; and computer-based education and training.

The Subcommittee on NITRD of the National Science and Technology Council (NSTC) is the internal deliberative organization for NITRD policy, program, and budget guidance.<sup>1</sup> NITRD research activities are organized in eight Program Component Areas (PCAs). The PCAs also align the NITRD program budget categories.<sup>2</sup> NITRD research areas and activities shift regularly as the NIT field creates and develops new R&D challenges.

The NITRD National Coordination Office (NCO) provides staff support for the NITRD program. The NCO provides program and financial management services, technical and subject matter expertise in facilitation, strategic planning, technical writing, networking and information technology services, and administrative staff support for the NITRD Subcommittee and other NITRD subgroups. The National Science Foundation (NSF) serves as the host agency for the NCO.<sup>3</sup>

In December 2010, the President's Council of Advisors on Science and Technology (PCAST) completed a legislatively required report on NITRD. The report, *Designing a Digital Future: Federally Funded Research and Development in Networking and Information Technology*, found that "NITRD is well coordinated and that the U.S. computing research community, coupled with a vibrant Networking and Information Technology (NIT) industry, has made seminal discoveries and advanced new technologies that are helping meet many societal challenges."<sup>4</sup>

The 2010 report made several assessments about the role of the NIT field in answering the Nation's challenges and priorities:

- Advances in NIT are a key driver of economic competitiveness. They create new markets and increase productivity.

---

<sup>1</sup> About the Subcommittee on Networking and Information Technology Research and Development (NITRD Subcommittee), <http://www.nitrd.gov/subcommittee/program.aspx>

<sup>2</sup> NITRD Program PCA Definitions, <http://www.nitrd.gov/subcommittee/pca-definitions.aspx>

<sup>3</sup> About the Subcommittee on Networking and Information Technology Research and Development (NITRD Subcommittee), <http://www.nitrd.gov/subcommittee/program.aspx>

<sup>4</sup> President's Council of Advisors on Science and Technology, Report to the President and Congress December 2010, *Designing a Digital Future: Federally Funded Research and Development in Networking and Information Technology*, p. v

- Advances in NIT are crucial to achieving our major national and global priorities in energy and transportation, education and life-long learning, healthcare, and national and homeland security.
- Advances in NIT accelerate the pace of discovery in nearly all other fields.
- Advances in NIT are essential to achieving the goals of open government.<sup>5</sup>

Stressing the need that federal investments be in NIT basic research, since the private sector is heavily involved in the development side, the report suggests that an investment of at least \$1 billion annually will be required for new, potentially transformative research. The report also recognizes that in the current economic uncertainty, repurposing and reprioritization of funding will be necessary, but does not rule out new funding and indicates a lower level of investment “could seriously jeopardize America’s national security and economic competitiveness.”<sup>6</sup>

The PCAST report includes recommendations for increased investments in long-term, multi-agency research initiatives in health, energy and transportation, and cybersecurity. It emphasizes, “Where fundamental NIT advances are needed to support these initiatives, mission agencies should invest in fundamental research in NIT, either alone or in collaboration with NSF, and should not limit their programs to application-specific research.”<sup>7</sup>

The report also calls for exercising leadership to bring about changes in K-12 STEM education; enhancing the effectiveness of government coordination of NIT research and development; and redefining NITRD budget categories to separate NIT infrastructure for R&D in other fields from NIT R&D.

### **Summary of Major Provisions**

- Reauthorizes the Networking and Information Technology Research and Development (NITRD) program, the federal government’s central R&D investment portfolio for unclassified networking, computing, software, cybersecurity, and related information technologies. NITRD includes 15 member agencies, and more than a dozen other participating agencies.
- Specific to cybersecurity, the NITRD program focuses on R&D to detect, prevent, resist, respond to, and recover from actions that compromise or threaten to compromise the availability, integrity, or confidentiality of computer-and network-based systems.

---

<sup>5</sup> President’s Council of Advisors on Science and Technology, Report to the President and Congress December 2010, *Designing a Digital Future: Federally Funded Research and Development in Networking and Information Technology*, p. vii

<sup>6</sup> Ibid, p. x.

<sup>7</sup> Ibid, p. xiii.

- Implements recommendations from the President’s Council of Advisors on Science and Technology (PCAST) including improving interagency coordination and planning with input from policy and technical experts.
- Rebalances R&D portfolios to focus less on short-term goals and place more emphasis on large-scale, long-term interdisciplinary research.
- Updates research areas to reflect new terminologies.
- Puts in place a university-industry task force to explore possible options for carrying out public-private cyber-physical systems research partnerships.
- Convenes an interagency working group to identify cloud computing research gaps and examine the potential for using the cloud for federally funded research.
- Updates the High Performance Computing Act of 1991 as recommended by the Speaker and Majority Leader’s Cybersecurity Task Force.

### **Legislative History**

In the 112<sup>th</sup> Congress, the Subcommittee on Research and Science Education held a hearing to review the networking and information technology research and development (NITRD) program to ensure U.S. leadership in networking and information technology and to receive input on legislative language for reauthorization of the program. Legislation was introduced in the 112<sup>th</sup> Congress, H.R. 3834, the *Advancing America’s Networking and Information Technology Research and Development Act of 2012*. On April 27, 2012, the House passed H.R. 3834 on a voice vote.

On March 5, 2013, H.R. 967, the *Advancing America’s Networking and Information Technology Research and Development Act of 2013* was reintroduced by Rep. Cynthia Lummis, Rep. Lamar Smith, and Rep. Eddie Bernice Johnson, and referred to the Committee on Science, Space, and Technology.