THE REPUBLICAN STUDY COMMITTEE
Rep. Jim Jordan, Chairman
Paul Teller, Executive Director
RSC
202.226.9717
rsc.jordan.house.gov

Legislative Bulletin……...Thursday, April 26, 2012

Contents:

H.R. 2096 – Cybersecurity Enhancement Act of 2011 (McCaul, R-TX)

Order of Business: The bill is scheduled to be considered on April 26, 2012, under a motion to suspend the rules and pass the bill.

Summary: This legislation would reauthorize several Nation Science Foundation (NSF) programs which are involved with enhancing cybersecurity. It would also continue a National Institute of Standards and Technology (NIST) program to promote cybersecurity awareness, and NIST would be required to develop standards for the management of personal identifying information.

H.R. 2096 also amends the Cyber Security Research Development Act and the National Institute of Standards and Technology Act as follows:

- Provides strategic planning for cybersecurity R&D needs across the federal government.
- Reauthorizes funding for established cybersecurity basic research and education grants at NSF.
- Enhances NSF scholarships to increase the size and skills of the cybersecurity workforce and repeals unused programs.
- Provides for an assessment of the federal government's current and future cybersecurity workforce needs.
- Establishes a university-industry task force to explore mechanisms and models for carrying out public-private cybersecurity research partnerships.
- Strengthens R&D, standards development and coordination, and public outreach at the National Institute of Standards and Technology (NIST) related to cybersecurity.

Committee Action: The legislation was introduced to the House on June 2, 2011, and it was referred to the House Committee on Science, Space, and Technology. The

Committee held a consideration and mark-up session on July 21, 2011, and the current legislation was then reported to the House, as amended, on October 31, 2011.

Administration Position: No Statement of Administration Policy is available.

Cost to Taxpayers: CBO estimates the cost of implementation to be $382 million over the 2012-2016 period and $39 million after 2016, subject to the appropriations process. Six existing NSF grant programs in statute are reauthorized for 3 years (FY13-FY15) in H.R. 2096. Authorizations for these programs expired in 2007, but NSF has been utilizing appropriations to conduct them under their general authorities. In FY10, NSF spent $148.6 million dollars on these activities. H.R. 2096 authorizes these activities for FY13 at $140 million, a savings of $8.6 million (5.8 percent) compared to FY10 spending. These activities are flat-lined for FY14 and FY15, for a total authorization in the bill of $420 million, or $508 million less than the 111th Congress version of the bill.

Does the Bill Expand the Size and Scope of the Federal Government?: The legislation expands the size of the federal government by increasing governmental role to include a larger role in cyber security research and development.

Does the Bill Contain Any New State-Government, Local-Government, or Private-Sector Mandates?: No. CBO states: "H.R. 2096 contains no intergovernmental or private-sector mandates as defined in UMRA and would impose no costs on state, local, or tribal governments."

Does the Bill Comply with House Rules Regarding Earmarks/Limited Tax Benefits/Limited Tariff Benefits?: Yes. House Report 112-264 states: "In compliance with clause 9(e), 9(f), and 9(g) of rule XXI, the Committee finds that H.R. 2096, the Cybersecurity Enhancement Act of 2011, contains no earmarks."

Constitutional Authority: Rep. McCaul states: "Congress has the power to enact this legislation pursuant to the following: This legislation is authorized by the United States Constitution under Article I, Section 8, 'Congress shall have the power To . . . provide for the common Defense and general Welfare of the United States" and ``To make all Laws which shall be necessary and proper for carrying into execution the forgoing Powers.'"

RSC Staff Contact: Derek S. Khanna, Derek.Khanna@mail.house.gov, (202) 226-0718

H.R. 3834 – Advancing America's Networking and Information Technology Research and Development Act of 2012 (Hall, R-TX)

Order of Business: The bill is scheduled to be considered on April 26, 2012, under a motion to suspend the rules and pass the bill.

Summary: This legislation implements several recommendations from the President's Council of Advisors on Science and Technology (PCAST) 2007 and 2010 assessments, including:

- Improving program planning and coordination through strategic planning and the Advisory Council with appropriate policy and technical expertise.
- Rebalancing portfolios to focus less on short-term goals and more on large-scale, long-term, interdisciplinary research with the potential to make significant contributions to society and US competitiveness.
- Requiring the program to support R&D in cyber-physical systems and human-computer interactions, visualization, and information management. This includes the convening of a university/industry task force to explore collaborative R&D activities with participants from universities, federal labs, industry and other partners.

H.R. 3834 convenes an interagency working group to examine outstanding cloud computing research issues and the potential for using the cloud for federally-funded science and engineering research, including funding mechanisms and policies. The working group is required to report on recommended guidelines for agencies to provide guidance to organizations and researchers on these issues.

Formally codifies and stresses the role of the National Coordination Office, which provides staff and serves as the interface for the program, and specifies the source of funding for the office (consistent with current practice).

Background: This legislation operates through the NITRD program.

What is the NITRD program?

- Originally authorized in the High Performance Computing Act of 1991 (P.L. 102-194), the NITRD program is the main Federal R&D investment portfolio in unclassified networking, computing, software, cybersecurity, and related information technologies. Fifteen agencies contribute expertise and funding to the program.
- NITRD Program Component Areas (PCA) areas include: Cybersecurity and Information Assurance; High Confidence Software and Systems; High-End Computing Infrastructure and Applications; High-End Computing R&D; Human-Computer Interaction and Information Management; Large-Scale Networking; Software Design and Productivity; and Social, Economic, and Workforce Implications of IT.

- The NITRD agencies' collaborative efforts increase the overall effectiveness and productivity of federal NIT R&D investments, leveraging strengths, avoiding duplication, and increasing interoperability of R&D products.

How does the NITRD program help protect our nation's cybersecurity?

- While cybersecurity R&D implications exist across all NITRD PCAs, the Cybersecurity and Information Assurance (CSIA) PCA is the major cybersecurity component of the NITRD program.
- CSIA 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.
- Broad areas of concern include Internet and network security; security of information and computer-based systems; approaches to achieving hardware and software security; testing and assessment of computer-based systems security; and reconstitution of computer-based systems and data.

Committee Action: The legislation was introduced on January 27, 2012, and it was referred to the House Committee on Science, Space, and Technology. It was reported to the House as amended on March 22, 2012 and placed on the Union Calendar.

Administration Position: No Statement of Administration Policy is available.

Cost to Taxpayers: The CBO estimates that this legislation costs about $2 million over the 2012-2017 period, subject to the availability of appropriated funds. This affects already allocated funds.

Does the Bill Expand the Size and Scope of the Federal Government?: The legislation expands the size of the federal government by increasing governmental role to include a larger role in cyber security research and development.

Does the Bill Contain Any New State-Government, Local-Government, or Private-Sector Mandates?: No, the CBO finds that the legislation contains no intergovernmental or private-sector mandates as defined in UMRA and would impose no costs on state, local, or tribal governments.

Does the Bill Comply with House Rules Regarding Earmarks/Limited Tax Benefits/Limited Tariff Benefits?: House Report 112-420 states: "In compliance with clause 9(e), 9(f), and 9(g) of rule XXI, the Committee finds that H.R. 3834, the *Advancing America's Networking and Information Technology Research and Development Act of 2012,* contains no earmarks."

Constitutional Authority: Rep. Hall statement can be found here: "Congress has the power to enact this legislation pursuant to the following: Article I, Section 8, Clause 3 'To regulate commerce with foreign Nations, and among the several States, and with the Indian Tribes;' and Article I, Section 8, Clause 18 'To make all Laws which shall be necessary and proper for carrying into Execution the foregoing Powers, and all other

Powers vested by this Constitution in the Government of the United States, or in any Department or officer thereof.'"

RSC Staff Contact: Derek S. Khanna, Derek.Khanna@mail.house.gov, (202) 226-0718

H.R. 4257 – Federal Information Security Amendments Act of 2012
(Issa, R-CA)

Order of Business: The bill is scheduled to be considered on April 26, 2012, under a motion to suspend the rules and pass the bill.

Summary: This legislation enhances the Federal Information Security Management Act (FISMA) of 2002 by improving the framework for securing information technology systems. It also establishes a mechanism for stronger oversight of information technology systems by focusing on "automated and continuous monitoring" of cybersecurity threats and regular "threat assessments."

The Director of the Office of Management and Budget (OMB) is directly responsible for "overseeing agency information security policies and practices," including the full implementation of FISMA. Because some confusion currently exists as to: 1) who is actually in charge of FISMA and; 2) to what degree one agency must be responsive to another agency, HR 4257 reaffirms the current law stipulation that OMB -- part of the Executive Office of the President (EOP) -- is primarily responsible for FISMA activity.

Given the Federal Government's current push to digitize data and push that information to the "cloud" as opposed to local servers, this legislation is particularly timely (Read here for part of Vivek Kundra's Cloud Computing Strategy). Eventually all of our Social Security and Veterans Affairs records will be on government, or private sector owned and Government licensed, servers. Having all this data on these servers presents a major cyber security danger, especially given the previously demonstrated vulnerability of some government servers. Having the government set standards for its own agencies is a step in the right direction.

Here is a link to Chairman Issa (R-CA) talking about the legislation.

Background: The Government Accountability Office recently found that security incidents among 24 key agencies had increased more than 650% during the last five years. To address these challenges, HR 4257 calls for automated and continuous monitoring and ensures that control monitoring finally incorporates regular threat assessments. HR 4257 also emphasizes the importance to national security of commercially developed information security products.

Committee Action: This legislation was introduced on March 26, 2012, and it was referred to the House Committee on Oversight and Government Reform. After the

Committee held a markup session on April 18, 2012, the legislation was ordered to be reported as amended by a voice vote, but the legislation has yet to be reported to the House.

Administration Position: No Statement of Administration Policy is available.

Cost to Taxpayers: The CBO estimates that implementation of this legislation would cost $710 million over the 2013-2017 period, assuming appropriation of the necessary amounts.

Does the Bill Expand the Size and Scope of the Federal Government?: Marginally, but in order to restrain the Federal Government. This would create new requirements for government agencies to meet for their own records, databases and data facilities. This legislation would use the existing apparatus of the OMB. This would bolster OMB's involvement in a number of new arenas, or have them task another agency with the oversight (e.g. GSA).

Does the Bill Contain Any New State-Government, Local-Government, or Private-Sector Mandates?: No, the CBO finds that the legislation contains no intergovernmental or private-sector mandates as defined in UMRA and would impose no costs on state, local, or tribal governments.

Constitutional Authority: Rep. Issa's statement can be found here: "Congress has the power to enact this legislation pursuant to the following: Art. I, Sec. 8 The Congress shall have Power To lay and collect Taxes, Duties, Imposts and Excises, to pay the Debts and provide for the common Defence and general Welfare of the United States; To make all Laws which shall be necessary and proper for carrying into Execution the foregoing Powers, and all other Powers vested by this Constitution in Government of the United States or in any Department or Officer thereof."

RSC Staff Contact: Derek S. Khanna, Derek.Khanna@mail.house.gov, (202) 226-0718