THE REPUBLICAN STUDY COMMITTEE
Rep. Steve Scalise, Chairman
Paul Teller, Executive Director
202.226.9717
rsc.scalise.house.gov

Legislative Bulletin……..……...April 16, 2013

Contents:

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. 1163 – Federal Information Security Amendments Act of 2013

H.R. 756 — Cybersecurity Enhancement Act of 2013 (McCaul, R-TX)

Order of Business: The bill is scheduled to be considered on April 16, 2013, under a motion to suspend the rules and pass the bill, which requires a two-thirds majority vote for passage.

Major Changes Since the Last Time This Legislation Was Before the House: H.R. 756 as introduced by Congressman McCaul is identical to H.R. 2096, which passed the House in the 112th Congress by floor vote of 395 to 10. See the Legislative Bulletin for H.R. 2096 from the 112th Congress here. The House Committee on Space, Science, and Technology held a markup on H.R. 756 on March 14, 2013, where several amendments were offered and approved by voice votes. The Committee approved H.R. 756 as amended by a voice vote. Amendment 009, offered by Chairman Smith, created a cybersecurity research database which "shall establish, in coordination with the Office of Management and Budget, a mechanism to track ongoing and completed Federal cybersecurity research and development projects and associated funding, and shall make such information publically available." See Chairman Smith's press release regarding the amendment here. The remaining amendments incorporated into the legislation created minor changes to the version that was passed by the House in the 112th Congress, including a requirement to describe how veterans will be recruited and prepared for the "Federal cybersecurity workforce". See amendments 03, 057, 002, 056, 054, 002.

Summary: H.R. 756 would amend the Cyber Security Research and Development Act (15 U.S.C. 7401) to:

- Coordinate research across the Federal government to better address cyber threats.
- Create a strategic cybersecurity research and development plan that addresses cybersecurity risks across the Federal government. The plan must specify how research and development programs address current objectives through long-term objectives.
- Establish and make publically available a cybersecurity research database to track current and completed cybersecurity research and development projects across the Federal government and funding information.

- Establish a university-industry taskforce that will deliver a report to Congress with recommendations on how the private sector and educational institutions can best collaborate and how to transfer the results of the collaborative work to the private sector.
- Create a cybersecurity workforce assessment to be delivered to Congress that details the "cybersecurity workforce needs of the Federal government."
- Require research on the science of cybersecurity

H.R. 756 also continues several programs or initiatives, including:

- A program designed to improve identify management protections
- An educational program designed to enhance cybersecurity awareness
- Development of a "comprehensive strategy" for cloud computing across the Federal government
- Development of international cybersecurity technical standards

Additional Background: See House Committee on Science, Space, and Technology press release regarding H.R. 756 here.

RSC Bonus Fact: The President's Cyberspace Policy Review from 2009 stated: "The government needs to increase investment in research that will help address cybersecurity vulnerabilities while also meeting our economic needs and national security requirements."

Committee Action: H.R. 756 was amended and reported out of the House Committee on Science, Space, and Technology on March 14, 2013 by a voice vote.

Administration Position: At time of press there was no Statement of Administration Position (SAP) for H.R. 756.

Cost to Taxpayers: CBO estimates that implementing H.R. 756 will cost taxpayers $504 million from 2014-2018 and $52 million after 2018. Authorizations for these programs expired in 2007 but NSF has continued to fund them under their general authority. H.R. 756 flat-lines current-level program funding for three years. The overall amount of money appropriated does not increase under H.R. 756, just the amount directed to cybersecurity efforts. Section 206 of H.R. 756 states, "No additional funds are authorized to carry out this Act, and the amendments made by this Act. This Act, and the amendments made by this Act, shall be carried out using amounts otherwise authorized or appropriated. This legislation directs more funding to cybersecurity but does not increase the overall amount of money appropriated."

Does the Bill Expand the Size and Scope of the Federal Government?: Yes. The scope of federal government involvement in the research and development in cybersecurity is increased.

Does the Bill Contain Any New State-Government, Local-Government, or Private-Sector Mandates?: No. CBO states, "H.R. 756 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 Contain Any Federal Encroachment into State or Local Authority in Potential Violation of the 10th Amendment?: No

Does the Bill Delegate Any Legislative Authority to the Executive Branch?: No

Does the Bill Contain Any Earmarks/Limited Tax Benefits/Limited Tariff Benefits?: No. Committee Report 113-33 states, "In compliance with clause 9(e), 9(f), and 9(g) of rule XXI, the Committee finds that H.R. 756, the *Cybersecurity Enhancement Act of 2013,* contains no earmarks."

What Is the Constitutional Authority for the Legislation?: The Constitutional Authority Statement accompanying the legislation cites the authority as, "Article 1, Section 8, Clause 1; and Article 1, Section 8, Clause 18 of the United States Constitution."

Outside Organizations in Support: Chamber of Commerce of the United States of America, National Association of Manufacturers, The Financial Services Roundtable, TechAmerica, the Computing Research Association (CRA), Institute of Electrical and Electronic Engineers – USA (IEEE-USA), Society for Industrial and Applied Mathematics (SIAM), and U.S. Public Policy Council of the Association for Computing Machinery (USACM).

RSC Staff Contact: W. Scott Herndon, Scott.Herndon@mail.house.gov, 202-226-2076.

H.R. 967 Advancing America's Networking and Information Technology Research and Development Act of 2013 (Lummis, R- WY)

Order of Business: The bill is scheduled to be considered on April 16, 2013, under a motion to suspend the rules and pass the bill, which requires a two-thirds majority vote for passage.

Major Changes Since the Last Time This Legislation Was Before the House: H.R. 967, as introduced, was identical to H.R. 3834 that passed the House in the 112th Congress by a voice vote. See Legislative Bulletin for H.R. 3834 from the 112th Congress. H.R. 967 was amended four times by the House Committee on Science, Space, and Technology. Amendment 440 offered by Congressman Johnson (R-TX) codifies the National Coordination office creation of a university/industry workshop. This differs from H.R. 3834, Section 105, which authorized the creation of a "University/Industry Task Force". See Amendments 013, 055, 441.

Summary: H.R. 967 amends the High-Performance Computing Act of 1991 (P.L. 102-194) to codify authorization for programs that support information technology research and networking, including a National Coordination Office. The programs created and reauthorized operate under the Networking and Information Technology Research and Development (NITRD) program. The legislation requires the creation and periodic update of a strategic plan for the (NITRD) program and codifies recommendations from by the President's Council of Advisors on Science

and Technology (PCAST) from 2007 and 2010. Some of the key recommendations that the legislation implements include:

- Refocusing programs toward more long-term, large-scale, interdisciplinary research goals with an increased focus on ways to enhance US competitiveness and make contributions to society
- The creation of a university/industry workshop comprised of industry, Federal laboratory, and university participants to study mechanisms for implementing collaborative research and development activities of cyber-physical systems.
- Improving interagency coordination and planning through collaboration with technical and policy experts.

The legislation also convenes an interagency working group under the National Science and Technology Council that will examine ways to enhance the effectiveness and trustworthiness of cloud computing environments and close research gaps. In addition, the legislation focuses research and development to prevent, detect, resist, and respond to threats of network and computer-based systems.

Additional Background: The NITRD program was originally authorized in the High-Performance Computing Act of 1991 (P.L. 102-194) to create a coordinating body for Federal agency high-performance computing programs. The NITRD program coordinates unclassified research and development across 14 Federal agencies and is the main research and development investment portfolio in cybersecurity, software, computing, networking, and related technologies.

See House Committee on Science, Space, and Technology press release regarding H.R. 967.

RSC Bonus Fact: The NITRD has produced devices for assisted living, near-real-time-weather forecasts, unmanned aerial vehicles, search-and-rescue robots, and computational decoding of the human genome.

Committee Action: The House Committee on Science, Space, and Technology held a markup on March 14, 2013, where the bill was amended and reported out by voice vote.

Administration Position: At time of press a Statement of Administrative Position (SAP) was not available.

Cost to Taxpayers: CBO estimates the H.R. 967 would cost about $1 million to implement during the 2014-2018 period subject to the fund availability.

Does the Bill Expand the Size and Scope of the Federal Government?: Yes. The size and scope of the federal government is increased through greater involvement in cybersecurity research and development.

Does the Bill Contain Any New State-Government, Local-Government, or Private-Sector Mandates?: CBO states, "H.R. 967 contains no intergovernmental or private-sector mandates as

defined in the Unfunded Mandates Reform Act and would not affect the budgets of state, local, or tribal governments."

Does the Bill Contain Any Federal Encroachment into State or Local Authority in Potential Violation of the 10th Amendment?: No.

Does the Bill Delegate Any Legislative Authority to the Executive Branch?: No.

Does the Bill Contain Any Earmarks/Limited Tax Benefits/Limited Tariff Benefits?: No. Committee Report 113-34 states, "In compliance with clause 9(e), 9(f), and 9(g) of rule XXI, the Committee finds that H.R. 967, the 'Advancing America's Net- working and Information Technology Research and Development Act of 2013', contains no earmarks."

What Is the Constitutional Authority for the Legislation?: The Constitutional Authority Statement accompanying the bill upon introduction states, "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."

Outside Organizations in Support: National Association of Manufacturers, TechAmerica, the Computing Research Association (CRA), Institute of Electrical and Electronic Engineers – USA (IEEE-USA), Society for Industrial and Applied Mathematics (SIAM), and U.S. Public Policy Council of the Association for Computing Machinery (USACM).

RSC Staff Contact: W. Scott Herndon, Scott.Herndon@mail.house.gov, 202-226-2076

H.R. 1163 – Federal Information Security Amendments Act of 2013 (Issa, R-CA)

Order of Business: The legislation is scheduled to be considered on April 16, 2013, under a motion to suspend the rules and pass the bill, which requires a two-thirds majority vote for passage.

Summary: The legislation contains multiple requirements for federal agencies in order to improve the security of information that is handled by the federal government.

The legislation directs federal agencies to develop and oversee the implementation of policies and guidelines with respect to information security.

The legislation directs the federal agencies to provide information security protections that are proportionate to the risk associated with the unauthorized access, use, disclosure, disruption, modification and destruction of information collected by the agency. Federal agencies are also directed to abide with the information security standards within the National Institute of

Standards and Technology Act, as well as information security standards. Federal agencies are also required to include information security performance indicators are included in the annual performance evaluations of all managers, senior managers, senior executive service personnel and political appointees.

Agencies are required to develop and implement an agencywide information security program to provide information security for the operations and assets of the agency. Federal agencies are required to delegate, to a sole individual, the authority and primary responsibility to develop, implement, and oversee an agencywide information security program to ensure and enforce compliance from the agency. This individual will be responsible for overseeing the establishment and maintenance of a security operations protocol that though automated monitoring can:

- Detect, report, respond to, contain, and mitigate incidents that impair information security and agency information systems;
- Commensurate with the risk to information security, monitor and mitigate the vulnerabilities of every information system within the agency;
- Continually evaluate risks posed to information collected or maintained by the agency and hold senior agency officials accountable for ensuring information security;
- Collaborate with the Director of the Office of Management and Budget (OMB) to detect, report, respond to, and mitigate incidents that impact the security of information and information systems; and
- Report any incident to the federal information security incident center with 24 hours after discovery.

Each agency shall submit an annual report on the adequacy and effectiveness of information security policies, procedures, and practices, and compliance with the legislation. The report shall address the adequacy and effectiveness of information security policies, procedures, and practices. The report shall also include any significant deficiency in a policy, procedure, or practice adopted.

The legislation creates a central federal information security incident center to, among other tasks, will provide timely technical assistance to operators of agency information systems regarding security incidents, including guidance on detecting and handling information security incidents. Each federal agency operating or exercising control of a national security system shall share information about information security incidents with the federal information security incident center.

Section 4 of the legislation states that no additional funds are authorized to carry out the requirements of this legislation. The legislation directs that the requirements are to be carried out using amounts otherwise authorized or appropriated.

Additional Information: During the 112th Congress, the House of Representatives approved similar legislation, H.R. 4257, by voice vote on April 26, 2012. The Senate then took no action on the bill. The RSC's Legislative Bulletin for H.R. 4257 can be viewed here.

Committee Action: H.R. 1163 introduced on March 14, 2013, and was referred to the House Committee on Oversight and Government Reform. The committee held a markup on March 20, 2013, and reported the legislation by voice vote, without amendment.

Administration Position: No Statement of Administration Policy (SAP) is available.

Cost to Taxpayers: CBO estimates that implementing H.R. 1163 would cost $620 million over the 2014-2018 period. CBO's full report can be viewed here.

Does the Bill Expand the Size and Scope of the Federal Government?: No. The legislation creates new requirements for government agencies to meet for their own records, databases and data facilities.

Does the Bill Contain Any New State-Government, Local-Government, or Private-Sector Mandates?: According to CBO, H.R. 1163 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act (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?: The legislation contains no earmarks, limited tax benefits, or limited tariff benefits.

Constitutional Authority: According the sponsor, "Congress has the power to enact this legislation pursuant to the following: Article I Sec. 8 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." Rep. Issa's statement in the Congressional Record can be viewed here.

RSC Staff Contact: Curtis Rhyne, Curtis.Rhyne@mail.house.gov, (202) 226-8576.