RSC Republican Study Committee
REP. TOM PRICE, M.D. (R-GA), CHAIRMAN
PAUL TELLER, EXECUTIVE DIRECTOR
424 CANNON HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
rsc.price.house.gov
ph (202) 226-9717 / fax (202) 226-1633

Legislative Bulletin…….February 3, 2010

Contents:

H.R. 4061—Cybersecurity Enhancement Act of 2009
(Lipinski, D-IL)

Order of Business: The bill is scheduled to be considered on Wednesday, February 3, 2010, under an expected structured rule that will provide for one hour of general debate and make in order several amendments. The RSC will summarize the rule and each amendment made in order in a separate document.

Summary: Authorizing a total of $959 million over five years (FY 2010 - FY 2014), H.R. 4061 would reauthorize several programs under the National Science Foundation (NSF) and seek to improve on current practices for the protection of computer networks and computers from access by unauthorized users. The bill authorizes $396 million to require the NSF to update and implement a strategic plan for cyber security research and development. In addition, the bill authorizes $96 million for the NSF to provide scholarships to students who pursue higher education in fields related to cyber security and commit to public service after graduation. The bill also authorizes approximately $438 million for other NSF programs, including grants to institutions of higher education that support professional development of faculty, the development of cyber security-related curricula and courses, and facility construction.

The bill also authorizes approximately $30 million for the National Institutes of Science and Technology (NIST) to produce a cyber security awareness and education program for the public. Some of highlights of the major provisions of the bill are as follows:

TITLE I--RESEARCH AND DEVELOPMENT

- ***Cyber Security Research & Development Plan:*** Requires (within one year of enactment), the National Coordination Office for the Networking and Information Technology Research and Development (NITRD) provide Congress a strategic plan based on an assessment of cyber security risk to guide the overall direction of federal cyber security research and development for information technology and networking systems. The plan will be updated every three years. The plan will prioritize near-term, mid-term and long-term research objectives established under the Cyber Security Research and Development Act of 2002.

  The plan will include information on transformational technologies with the potential to enhance the security of the digital infrastructure, information technologies and applications

for the benefit of society, and information on providing access to academic researchers for the creating, testing, and evaluating of secure networking and information technology systems.

NITRD will also develop an annual implementation "roadmap" for the strategic plan to specify the role of each federal agency to carry out research and development activities, funding allocations, and recommendations to implement standardized best practices. The legislation authorizes $68.7 million for FY 2010, $73.5 million for FY 2011, $78.6 million for FY 2012, $84.2 million for FY 2013, and $90 million for FY 2014.

- ***Federal Cyber Scholarship for Service Program:*** Requires the Director of the National Science Foundation (NSF) to implement a scholarship program to increase the information technology workforce. The programs will produce scholarships that provide tuition, fees, and a stipend for up to 2 years to students pursing a bachelor's or master's degree and up to 3 years to students pursuing a doctoral degree in a cyber security field. In order to qualify for a scholarship the individual must serve as a cyber security professional within the federal workforce for a period of time equal to the length of the scholarship. If an individual who has received a scholarship fails to complete the program or fails to fulfill the service obligation, they must participate in a scholarship repayment program. The bill authorizes $18.7 million for FY 2010, $20.1 million for FY 2011, $21.6 million for FY 2012, $23.3 million for FY 2013, and $25 million for FY 2014.

- ***Cyber Security Workforce Assessment:*** Within 180 days of enactment, the bill requires the President to submit a report on the workforce needs of the federal government on cyber security. The report is to include a comparison of the different agencies and departments, barriers relating to compensation, and an examination of institutions of higher education to provide cyber security professionals with those skills sought by the federal government.

- ***University/Industry Task Force:*** The bill also requires the Director of the Office of Science and Technology Policy to convene a task force to provide research and development activities for cyber security with equal participants from institutions of higher education and industry. The purpose will be to provide a research and development agenda, propose guidelines for assigning intellectual property rights, and make recommendations for how entities could be funded from federal, state, and nongovernmental sources.

- ***Cyber Security Checklist:*** H.R. 4061 requires the Director of the National Institute of Standards and Technology (NIST) to implement checklists, configuration profiles, and deployment recommendations for products and protocols that minimize the security risks associated with each computer hardware or software system that is, or is likely to become, widely used within the federal government.

- ***NIST Cyber Security Research & Development:*** Requires NIST to conduct a research program to develop a standardized management framework for the execution of a variety of resource protection policies in the security of information systems and networks.

TITLE II--ADVANCEMENT OF CYBERSECURITY TECHNICAL STANDARDS

- ***International Standards:*** Requires NIST to ensure cooperation within the international community in the development of technical standards related to cyber security and provide Congress a strategic plan to accomplish this goal within one year of enactment.

- ***Promoting Cyber Security Awareness & Development:*** Requires NIST to develop a cyber security awareness and education program to increase public awareness of cyber security risks, consequences, and best practices. The section requires NIST to submit a progress report to Congress within 90 days. The bill also requires NIST to establish a program to support the development of technical standards to improve interoperability, strengthen authentication methods, and improve privacy protection in identity management systems.

Additional Background: Over the past decade, the interconnectivity and interdependence of information technology (IT) has dramatically increased the vulnerability of many different networks - making them susceptible to a cyber attack. Today, IT comprises a significant cross section of industries that include the finance, energy, telecommunications, transportation, chemical production, food distribution, and government services, among others.

A recent report that surveyed a wide array of companies determined that cyber attacks are becoming more common. "89 percent (of the surveyed companies) reported attacks involving malware, 60 percent reported theft-of-service attacks, and over 70 percent reported a range of other attacks including phishing and pharming. Around 30 percent of the companies surveyed also said that they had little faith in their banks and telecom providers' ability to withstand attack." Just last week, a large number of Members of the U.S. House of Representatives had their own websites hacked during the State of the Union. Reports of more attacks that allow unauthorized users to access sensitive information and disrupt government services has caused greater concern over the adequacy of cyber security measures. The Government Accountability Office concluded, "Cyber-based threats to federal systems and critical infrastructure are evolving and growing."

The 2002 Federal Information Security Management Act (P.L.107-347) required agencies to identify computer systems and deploy security controls on government networks. However, last year, the GAO stated that the information agencies collect does not accurately reflect the security of each network and determined the processes to collect the information is cumbersome and time-intensive. Ultimately, they concluded the Federal agencies tasked with the protection of IT services are not fulfilling their responsibilities.

Congress also passed the Cyber Security Research and Development Act (P.L. 107-305) in 2002 that created new and expanded upon existing programs at the National Science Foundation (NSF) and National Institute of Standards and Technology (NIST) for computer and network security. Among other provisions, it required NIST to establish a program of assistance to institutions of higher education that enter into partnerships with for-profit entities, institute programs to award post-doctoral research fellowships to individuals seeking cyber security research positions, and develop checklists that minimize security risks associated with Federal government computer hardware or software systems.

According to the Science & Technology Committee, the Office of Management and Budget (OMB) states that federal agencies have spent $6 billion on cyber security measures to protect a $72 billion IT infrastructure. Despite this significant funding, the GAO determined that nearly all 24 major agencies that submit FISMA reports identified weaknesses in one or more areas of information security controls in 2008. Thirteen agencies reported significant deficiencies, and seven agencies told of material weaknesses in information security.

The NSF is the principal agency supporting unclassified cyber security, R&D, and education. It is primarily funded through the Directorate for Computer & Information Science & Engineering (CISE). NIST is tasked with protecting the federal information technology network by developing and promulgating cyber security standards for federal non-classified network systems, identifying

methods for assessing effectiveness of security requirements, conducting tests to validate security in information systems, and conducting outreach exercises.

In May of 2009, the Administration released a review of cyberspace policies across the federal government. The general conclusion of this review was to strengthen partnerships between the federal government and the private sector, increase public awareness of the risks associated with cyber security, expand and train the federal cyber security workforce, advancing cyber security R&D, and provide better coordination between federal agencies.

Committee Action: On November 7, 2009, the bill was introduced and referred to the Committee on Science and Technology. On November 18, 2009, the full committee held a mark-up and ordered the bill to be reported, as amended, by voice vote.

Administration Position: A Statement of Administration Policy (SAP) is unavailable at press time.

Cost to Taxpayers: According to CBO, assuming appropriation of the necessary amounts, implementing H.R. 4061 would cost $639 million over the 2010-2014 period and $320 million after 2014, for a total cost of $959 million.

Does the Bill Expand the Size and Scope of the Federal Government? : Yes, the bill authorizes several new programs under the NSF and NIST with the intended purpose of increasing cyber security in the federal government and public.

Does the Bill Contain Any New State-Government, Local-Government, or Private-Sector Mandates? No.

Does the Bill Comply with House Rules Regarding Earmarks/Limited Tax Benefits/Limited Tariff Benefits?: According to Committee Report 111-405 does not contain any congressional earmarks, limited tax benefits, or limited tariff benefits as defined in House Rule XXI, clause 9(d), 9(e), and 9(f).

Constitutional Authority: The committee report for H.R. 4061 cites Constitutional Authority in Article I, Section 8, but *fails* to cite a foregoing power to what this clause reflects.

RSC Staff Contact: Bruce F. Miller, bruce.miller@mail.house.gov, (202)-226-9720.