S 773 IS

111th CONGRESS

1st Session

S. 773

To ensure the continued free flow of commerce within the United States and with its global trading partners through secure cyber communications, to provide for the continued development and exploitation of the Internet and intranet communications for such purposes, to provide for the development of a cadre of information technology specialists to improve and maintain effective cyber security defenses against disruption, and for other purposes.

IN THE SENATE OF THE UNITED STATES

April 1, 2009

Mr. ROCKEFELLER (for himself, Ms. SNOWE, and Mr. NELSON of Florida) introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

A BILL

To ensure the continued free flow of commerce within the United States and with its global trading partners through secure cyber communications, to provide for the continued development and exploitation of the Internet and intranet communications for such purposes, to provide for the development of a cadre of information technology specialists to improve and maintain effective cybersecurity defenses against disruption, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE- This Act may be cited as the ‘Cybersecurity Act of 2009’.

(b) TABLE OF CONTENTS- The table of contents for this Act is as follows:

Sec. 1. Short title; table of contents.

Sec. 2. Findings.

Sec. 3. Cybersecurity Advisory Panel.

Sec. 4. Real-time cybersecurity dashboard.

Sec. 5. State and regional cybersecurity enhancement program.

Sec. 6. NIST standards development and compliance.

Sec. 7. Licensing and certification of cybersecurity professionals.

Sec. 8. Review of NTIA domain name contracts.

Sec. 9. Secure domain name addressing system.

Sec. 10. Promoting cybersecurity awareness.

Sec. 11. Federal cybersecurity research and development.

Sec. 12. Federal Cyber Scholarship-for-Service program.

Sec. 13. Cybersecurity competition and challenge.

Sec. 14. Public-private clearinghouse.

Sec. 15. Cybersecurity risk management report.

Sec. 16. Legal framework review and report.

Sec. 17. Authentication and civil liberties report.

Sec. 18. Cybersecurity responsibilities and authorities.

Sec. 19. Quadrennial cyber review.

Sec. 20. Joint intelligence threat assessment.

Sec. 21. International norms and cybersecurity deterrence measures.

Sec. 22. Federal Secure Products and Services Acquisitions Board.

Sec. 23. Definitions.

SEC. 2. FINDINGS.

The Congress finds the following:

(1) America’s failure to protect cyberspace is one of the most urgent national security problems facing the country.

(2) Since intellectual property is now often stored in digital form, industrial espionage that exploits weak cybersecurity dilutes our investment in innovation while subsidizing the research and development efforts of foreign competitors. In the new global competition, where economic strength and technological leadership are vital components of national power, failing to secure cyberspace puts us at a disadvantage.

(3) According to the 2009 Annual Threat Assessment, ‘a successful cyber attack against a major financial service provider could severely impact the national economy, while cyber attacks against physical infrastructure computer systems such as those that control power grids or oil refineries have the potential to disrupt services for hours or weeks’ and that ‘Nation states and criminals target our government and private sector information networks to gain competitive advantage in the commercial sector.’.

(4) The Director of National Intelligence testified before the Congress on February 19, 2009, that ‘a growing array of state and non-state adversaries are increasingly targeting-for exploitation and potentially disruption or destruction-our information infrastructure, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries’ and these trends are likely to continue.

(5) John Brennan, the Assistant to the President for Homeland Security and Counterterrorism wrote on March 2, 2009, that ‘our nation’s security and economic prosperity depend on the security, stability, and integrity of communications and information infrastructure that are largely privately-owned and globally-operated.’.

(6) Paul Kurtz, a Partner and chief operating officer of Good Harbor Consulting as well as a senior advisor to the Obama Transition Team for cybersecurity, recently stated that the United States is unprepared to respond to a ‘cyber-Katrina’ and that ‘a massive cyber disruption could have a cascading, long-term impact without adequate co-ordination between government and the private sector.’.

(7) The Cyber Strategic Inquiry 2008, sponsored by Business Executives for National Security and executed by Booz Allen Hamilton, recommended to ‘establish a single voice for cybersecurity within government’ concluding that the ‘unique nature of cybersecurity requires a new leadership paradigm.’.

(8) Alan Paller, the Director of Research at the SANS Institute, testified before the Congress that ‘the fight against cybercrime resembles an arms race where each time the defenders build a new wall, the attackers create new tools to scale the wall. What is particularly important in this analogy is that, unlike conventional warfare where deployment takes time and money and is quite visible, in the cyber world, when the attackers find a new weapon, they can attack millions of computers, and successfully infect hundreds of thousands, in a few hours or days, and remain completely hidden.’.

(9) According to the February 2003 National Strategy to Secure Cyberspace, ‘our nation’s critical infrastructures are composed of public and private institutions in the sectors of agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking finance, chemicals and hazardous materials, and postal and shipping. Cyberspace is their nervous system--the control system of our country’ and that ‘the cornerstone of America’s cyberspace security strategy is and will remain a public-private partnership.’.

(10) According to the National Journal, Mike McConnell, the former Director of National Intelligence, told President Bush in May 2007 that if the 9/11 attackers had chosen computers instead of airplanes as their weapons and had waged a massive assault on a U.S. bank, the economic consequences would have been ‘an order of magnitude greater’ than those cased by the physical attack on the World Trade Center. Mike McConnell has subsequently referred to cybersecurity as the ‘soft underbelly of this country.’.

(11) The Center for Strategic and International Studies report on Cybersecurity for the 44th Presidency concluded that (A) cybersecurity is now a major national security problem for the United States, (B) decisions and actions must respect privacy and civil liberties, and (C) only a comprehensive national security strategy that embraces both the domestic and international aspects of cybersecurity will make us more secure. The report continued stating that the United States faces ‘a long-term challenge in cyberspace from foreign intelligence agencies and militaries, criminals, and others, and that losing this struggle will wreak serious damage on the economic health and national security of the United States.’.

(12) James Lewis, Director and Senior Fellow, Technology and Public Policy Program, Center for Strategic and International Studies, testified on behalf of the Center for Strategic and International Studies that ‘the United States is not organized and lacks a coherent national strategy for addressing’ cybersecurity.

(13) President Obama said in a speech at Purdue University on July 16, 2008, that ‘every American depends--directly or indirectly--on our system of information networks. They are increasingly the backbone of our economy and our infrastructure; our national security and our personal well-being. But it’s no secret that terrorists could use our computer networks to deal us a crippling blow. We know that cyber-espionage and common crime is already on the rise. And yet while countries like China have been quick to recognize this change, for the last eight years we have been dragging our feet.’ Moreover, President Obama stated that ‘we need to build the capacity to identify, isolate, and respond to any cyber-attack.’.

(14) The President’s Information Technology Advisory Committee reported in 2005 that software is a major vulnerability and that ‘software development methods that have been the norm fail to provide the high-quality, reliable, and secure software that the IT infrastructure requires. . . . Today, as with cancer, vulnerable software can be invaded and modified to cause damage to previously healthy software, and infected software can replicate itself and be carried across networks to cause damage in other systems.’.

SEC. 3. CYBERSECURITY ADVISORY PANEL.

(a) IN GENERAL- The President shall establish or designate a Cybersecurity Advisory Panel.

(b) QUALIFICATIONS- The President--

(1) shall appoint as members of the panel representatives of industry, academic, non-profit organizations, interest groups and advocacy organizations, and State and local governments who are qualified to provide advice and information on cybersecurity research, development, demonstrations, education, technology transfer, commercial application, or societal and civil liberty concerns; and

(2) may seek and give consideration to recommendations from the Congress, industry, the cybersecurity community, the defense community, State and local governments, and other appropriate organizations.

(c) DUTIES- The panel shall advise the President on matters relating to the national cybersecurity program and strategy and shall assess--

(1) trends and developments in cybersecurity science research and development;

(2) progress made in implementing the strategy;

(3) the need to revise the strategy;

(4) the balance among the components of the national strategy, including funding for program components;

(5) whether the strategy, priorities, and goals are helping to maintain United States leadership and defense in cybersecurity;

(6) the management, coordination, implementation, and activities of the strategy; and

(7) whether societal and civil liberty concerns are adequately addressed.

(d) REPORTS- The panel shall report, not less frequently than once every 2 years, to the President on its assessments under subsection (c) and its recommendations for ways to improve the strategy.

(e) TRAVEL EXPENSES OF NON-FEDERAL MEMBERS- Non-Federal members of the panel, while attending meetings of the panel or while otherwise serving at the request of the head of the panel while away from their homes or regular places of business, may be allowed travel expenses, including per diem in lieu of subsistence, as authorized by section 5703 of title 5, United States Code, for individuals in the government serving without pay. Nothing in this subsection shall be construed to prohibit members of the panel who are officers or employees of the United States from being allowed travel expenses, including per diem in lieu of subsistence, in accordance with law.

(f) EXEMPTION FROM FACA SUNSET- Section 14 of the Federal Advisory Committee Act (5 U.S.C. App.) shall not apply to the Advisory Panel.

SEC. 4. REAL-TIME CYBERSECURITY DASHBOARD.

The Secretary of Commerce shall--

(1) in consultation with the Office of Management and Budget, develop a plan within 90 days after the date of enactment of this Act to implement a system to provide dynamic, comprehensive, real-time cybersecurity status and vulnerability information of all Federal Government information systems and networks managed by the Department of Commerce; and

(2) implement the plan within 1 year after the date of enactment of this Act.

SEC. 5. STATE AND REGIONAL CYBERSECURITY ENHANCEMENT PROGRAM.

(a) CREATION AND SUPPORT OF CYBERSECURITY CENTERS- The Secretary of Commerce shall provide assistance for the creation and support of Regional Cybersecurity Centers for the promotion and implementation of cybersecurity standards. Each Center shall be affiliated with a United States-based nonprofit institution or organization, or consortium thereof, that applies for and is awarded financial assistance under this section.

(b) PURPOSE- The purpose of the Centers is to enhance the cybersecurity of small and medium sized businesses in United States through--
(

(1) the transfer of cybersecurity standards, processes, technology, and techniques developed at the National Institute of Standards and Technology to Centers and, through them, to small- and medium-sized companies throughout the United States;

(2) the participation of individuals from industry, universities, State governments, other Federal agencies, and, when appropriate, the Institute in cooperative technology transfer activities;

(3) efforts to make new cybersecurity technology, standards, and processes usable by United States-based small- and medium-sized companies;

(4) the active dissemination of scientific, engineering, technical, and management information about cybersecurity to industrial firms, including small- and medium-sized companies; and

(5) the utilization, when appropriate, of the expertise and capability that exists in Federal laboratories other than the Institute.

(c) ACTIVITIES- The Centers shall--

(1) disseminate cybersecurity technologies, standard, and processes based on research by the Institute for the purpose of demonstrations and technology transfer;

(2) actively transfer and disseminate cybersecurity strategies, best practices, standards, and technologies to protect against and mitigate the risk of cyber attacks to a wide range of companies and enterprises, particularly small- and medium-sized businesses; and

(3) make loans, on a selective, short-term basis, of items of advanced cybersecurity countermeasures to small businesses with less than 100 employees.

(c) Duration and Amount of Support; Program Descriptions; Applications; Merit Review; Evaluations of Assistance-

(1) FINANCIAL SUPPORT- The Secretary may provide financial support, not to exceed 50 percent of its annual operating and maintenance costs, to any Center for a period not to exceed 6 years (except as provided in paragraph (5)(D)).

(2) PROGRAM DESCRIPTION- Within 90 days after the date of enactment of this Act, the Secretary shall publish in the Federal Register a draft description of a program for establishing Centers and, after a 30-day comment period, shall publish a final description of the program. The description shall include--

(A) a description of the program;

(B) procedures to be followed by applicants;

(C) criteria for determining qualified applicants;

(D) criteria, including those described in paragraph (4), for choosing recipients of financial assistance under this section from among the qualified applicants; and

(E) maximum support levels expected to be available to Centers under the program in the fourth through sixth years of assistance under this section.

(3) APPLICATIONS; SUPPORT COMMITMENT- Any nonprofit institution, or consortia of nonprofit institutions, may submit to the Secretary an application for financial support under this section, in accordance with the procedures established by the Secretary. In order to receive assistance under this section, an applicant shall provide adequate assurances that it will contribute 50 percent or more of the proposed Center's annual operating and maintenance costs for the first 3 years and an increasing share for each of the next 3 years.

(4) AWARD CRITERIA- Awards shall be made on a competitive, merit-based review. In making a decision whether to approve an application and provide financial support under this section, the Secretary shall consider, at a minimum--

(A) the merits of the application, particularly those portions of the application regarding technology transfer, training and education, and adaptation of cybersecurity technologies to the needs of particular industrial sectors;

(B) the quality of service to be provided;

(C) geographical diversity and extent of service area; and

(D) the percentage of funding and amount of in-kind commitment from other sources.

(5) Third year evaluation-

(A) IN GENERAL- Each Center which receives financial assistance under this section shall be evaluated during its third year of operation by an evaluation panel appointed by the Secretary.

(B) EVALUATION PANEL- Each evaluation panel shall be composed of private experts, none of whom shall be connected with the involved Center, and Federal officials. An official of the Institute shall chair the panel. Each evaluation panel shall measure the Center's performance against the objectives specified in this section.

(C) POSITIVE EVALUATION REQUIRED FOR CONTINUED FUNDING- The Secretary may not provide funding for the fourth through the sixth years of a Center's operation unless the evaluation by the evaluation panel is positive. If the evaluation is positive, the Secretary may provide continued funding through the sixth year at declining levels.

(D) FUNDING AFTER SIXTH YEAR- After the sixth year, the Secretary may provide additional financial support to a Center if it has received a positive evaluation through an independent review, under procedures established by the Institute. An additional independent review shall be required at least every 2 years after the sixth year of operation. Funding received for a fiscal year under this section after the sixth year of operation may not exceed one third of the annual operating and maintenance costs of the Center.

(6) PATENT RIGHTS TO INVENTIONS- The provisions of chapter 18 of title 35, United States Code, shall (to the extent not inconsistent with this section) apply to the promotion of technology from research by Centers under this section except for contracts for such specific technology extension or

transfer services as may be specified by statute or by the President, or the President's designee.

(d) ACCEPTANCE OF FUNDS FROM OTHER FEDERAL DEPARTMENTS AND AGENCIES- In addition to such sums as may be authorized and appropriated to the Secretary and President, or the President's designee, to operate the Centers program, the Secretary and the President, or the President's designee, also may accept funds from other Federal departments and agencies for the purpose of providing Federal funds to support Centers. Any Center which is supported with funds which originally came from other Federal departments and agencies shall be selected and operated according to the provisions of this section.

SEC. 6. NIST STANDARDS DEVELOPMENT AND COMPLIANCE.

(a) IN GENERAL- Within 1 year after the date of enactment of this Act, the National Institute of Standards and Technology shall establish measurable and auditable cybersecurity standards for all Federal Government, government contractor, or grantee critical infrastructure information systems and networks in the following areas:

(1) CYBERSECURITY METRICS RESEARCH- The Director of the National Institute of Standards and Technology shall establish a research program to develop cybersecurity metrics and benchmarks that can assess the economic impact of cybersecurity. These metrics should measure risk reduction and the cost of defense. The research shall include the development automated tools to assess vulnerability and compliance.

(2) SECURITY CONTROLS- The Institute shall establish standards for continuously measuring the effectiveness of a prioritized set of security controls that are known to block or mitigate known attacks.

(3) SOFTWARE SECURITY- The Institute shall establish standards for measuring the software security using a prioritized list of software weaknesses known to lead to exploited and exploitable vulnerabilities. The Institute will also establish a separate set of such standards for measuring security in embedded software such as that found in industrial control systems.

(4) SOFTWARE CONFIGURATION SPECIFICATION LANGUAGE- The Institute shall, establish standard computer-readable language for completely specifying the configuration of software on computer systems widely used in the Federal Government, by government contractors and grantees, and in private sector owned critical infrastructure information systems and networks.

(5) STANDARD SOFTWARE CONFIGURATION- The Institute shall establish standard configurations consisting of security settings for operating system software and software utilities widely used in the Federal Government, by government contractors and grantees, and in private sector owned critical infrastructure information systems and networks.

(6) VULNERABILITY SPECIFICATION LANGUAGE- The Institute shall establish standard computer-readable language for specifying vulnerabilities in software to enable software vendors to communicate vulnerability data to software users in real time.

(7) National compliance standards for all software-

(A) PROTOCOL- The Institute shall establish a standard testing and accreditation protocol for software built by or for the Federal Government, its contractors, and grantees, and private sector owned critical

infrastructure information systems and networks. to ensure that it--

(i) meets the software security standards of paragraph (2); and

(ii) does not require or cause any changes to be made in the standard configurations described in paragraph (4).

(B) COMPLIANCE- The Institute shall develop a process or procedure to verify that--

(i) software development organizations comply with the protocol established under subparagraph (A) during the software development process; and

(ii) testing results showing evidence of adequate testing and defect reduction are provided to the Federal Government prior to deployment of software.

(b) CRITERIA FOR STANDARDS- Notwithstanding any other provision of law (including any Executive Order), rule, regulation, or guideline, in establishing standards under this section, the Institute shall disregard the designation of an information system or network as a national security system or on the basis of presence of classified or confidential information, and shall establish standards based on risk profiles.

(c) INTERNATIONAL STANDARDS- The Director, through the Institute and in coordination with appropriate Federal agencies, shall be responsible for United States representation in all international standards development related to cybersecurity, and shall develop and implement a strategy to optimize the United States position with respect to international cybersecurity standards.

(d) COMPLIANCE ENFORCEMENT- The Director shall--

(1) enforce compliance with the standards developed by the Institute under this section by software manufacturers, distributors, and vendors; and

(2) shall require each Federal agency, and each operator of an information system or network designated by the President as a critical infrastructure information system or network, periodically to demonstrate compliance with the standards established under this section.

(e) FCC NATIONAL BROADBAND PLAN- In developing the national broadband plan pursuant to section 6001(k) of the American Recovery and Reinvestment Act of 2009, the Federal Communications Commission shall report on the most effective and efficient means to ensure the cybersecurity of commercial broadband networks, including consideration of consumer education and outreach programs.

SEC. 7. LICENSING AND CERTIFICATION OF CYBERSECURITY PROFESSIONALS.

(a) IN GENERAL- Within 1 year after the date of enactment of this Act, the Secretary of Commerce shall develop or coordinate and integrate a national licensing, certification, and periodic recertification program for cybersecurity professionals.

(b) MANDATORY LICENSING- Beginning 3 years after the date of enactment of this Act, it shall be unlawful for any individual to engage in business in the United States, or to be employed in the United

States, as a provider of cybersecurity services to any Federal agency or an information system or network designated by the President, or the President's designee, as a critical infrastructure information system or network, who is not licensed and certified under the program.

SEC. 8. REVIEW OF NTIA DOMAIN NAME CONTRACTS.

(a) IN GENERAL- No action by the Assistant Secretary of Commerce for Communications and Information after the date of enactment of this Act with respect to the renewal or modification of a contract related to the operation of the Internet Assigned Numbers Authority, shall be final until the Advisory Panel--

(1) has reviewed the action;

(2) considered the commercial and national security implications of the action; and

(3) approved the action.

(b) APPROVAL PROCEDURE- If the Advisory Panel does not approve such an action, it shall immediately notify the Assistant Secretary in writing of the disapproval and the reasons therefor. The Advisory Panel may provide recommendations to the Assistant Secretary in the notice for any modifications the it deems necessary to secure approval of the action.

SEC. 9. SECURE DOMAIN NAME ADDRESSING SYSTEM.

(a) IN GENERAL- Within 3 years after the date of enactment of this Act, the Assistant Secretary of Commerce for Communications and Information shall develop a strategy to implement a secure domain name addressing system. The Assistant Secretary shall publish notice of the system requirements in the Federal Register together with an implementation schedule for Federal agencies and information systems or networks designated by the President, or the President's designee, as critical infrastructure information systems or networks.

(b) COMPLIANCE REQUIRED- The President shall ensure that each Federal agency and each such system or network implements the secure domain name addressing system in accordance with the schedule published by the Assistant Secretary.

SEC. 10. PROMOTING CYBERSECURITY AWARENESS.

The Secretary of Commerce shall develop and implement a national cybersecurity awareness campaign that--

(1) is designed to heighten public awareness of cybersecurity issues and concerns;

(2) communicates the Federal Government's role in securing the Internet and protecting privacy and civil liberties with respect to Internet-related activities; and

(3) utilizes public and private sector means of providing information to the public, including public service announcements.

SEC. 11. FEDERAL CYBERSECURITY RESEARCH AND DEVELOPMENT.

(a) FUNDAMENTAL CYBERSECURITY RESEARCH- The Director of the National Science Foundation shall give priority to computer and information science and engineering research to ensure substantial support is provided to meet the following challenges in cybersecurity:

(1) How to design and build complex software-intensive systems that are secure and reliable when first deployed.

(2) How to test and verify that software, whether developed locally or obtained from a third party, is free of significant known security flaws.

(3) How to test and verify that software obtained from a third party correctly implements stated functionality, and only that functionality.

(4) How to guarantee the privacy of an individual's identity, information, or lawful transactions when stored in distributed systems or transmitted over networks.

(5) How to build new protocols to enable the Internet to have robust security as one of its key capabilities.

(6) How to determine the origin of a message transmitted over the Internet.

(7) How to support privacy in conjunction with improved security.

(8) How to address the growing problem of insider threat.

(b) SECURE CODING RESEARCH- The Director shall support research that evaluates selected secure coding education and improvement programs. The Director shall also support research on new methods of integrating secure coding improvement into the core curriculum of computer science programs and of other programs where graduates have a substantial probability of developing software after graduation.

(c) ASSESSMENT OF SECURE CODING EDUCATION IN COLLEGES AND UNIVERSITIES- Within one year after the date of enactment of this Act, the Director shall submit to the Senate Committee on Commerce, Science, and Transportation and the House of Representatives Committee on Science and Technology a report on the state of secure coding education in America's colleges and universities for each school that received National Science Foundation funding in excess of $1,000,000 during fiscal year 2008. The report shall include--

(1) the number of students who earned undergraduate degrees in computer science or in each other program where graduates have a substantial probability of being engaged in software design or development after graduation;

(2) the percentage of those students who completed substantive secure coding education or improvement programs during their undergraduate experience; and

(3) descriptions of the length and content of the education and improvement programs, and a measure of the effectiveness of those programs in enabling the students to master secure coding and design.
S

(d) CYBERSECURITY MODELING AND TESTBEDS- The Director shall establish a program to award grants to institutions of higher education to establish cybersecurity testbeds capable of realistic modeling of real-time cyber attacks and defenses. The purpose of this program is to support the rapid development of new cybersecurity defenses, techniques, and processes by improving understanding and assessing the latest technologies in a real-world environment. The testbeds shall be sufficiently large in order to model the scale and complexity of real world networks and environments.

(e) NSF COMPUTER AND NETWORK SECURITY RESEARCH GRANT AREAS- Section 4(a)(1) of the Cybersecurity Research and Development Act (15 U.S.C. 7403(a)(1)) is amended--

(1) by striking 'and' after the semicolon in subparagraph (H);

(2) by striking 'property.' in subparagraph (I) and inserting 'property;'; and

(3) by adding at the end the following:

'(J) secure fundamental protocols that are at the heart of inter-network communications and data exchange;

'(K) secure software engineering and software assurance, including--

'(i) programming languages and systems that include fundamental security features;

'(ii) portable or reusable code that remains secure when deployed in various environments;

'(iii) verification and validation technologies to ensure that requirements and specifications have been implemented; and

'(iv) models for comparison and metrics to assure that required standards have been met;

'(L) holistic system security that--

'(i) addresses the building of secure systems from trusted and untrusted components;

'(ii) proactively reduces vulnerabilities;

'(iii) addresses insider threats; and

'(iv) supports privacy in conjunction with improved security;

'(M) monitoring and detection; and

'(N) mitigation and rapid recovery methods.'.

(f) NSF COMPUTER AND NETWORK SECURITY GRANTS- Section 4(a)(3) of the Cybersecurity Research and Development Act (15 U.S.C. 7403(a)(3)) is amended--

(1) by striking 'and' in subparagraph (D);

(2) by striking ‘2007’ in subparagraph (E) and inserting ‘2007;’; and

(3) by adding at the end of the following:

‘(F) $150,000,000 for fiscal year 2010;

‘(G) $155,000,000 for fiscal year 2011;

‘(H) $160,000,000 for fiscal year 2012;

‘(I) $165,000,000 for fiscal year 2013; and

‘(J) $170,000,000 for fiscal year 2014.’.

(g) COMPUTER AND NETWORK SECURITY CENTERS- Section 4(b)(7) of such Act (15 U.S.C. 7403(b)(7)) is amended--

(1) by striking ‘and’ in subparagraph (D);

(2) by striking ‘2007’ in subparagraph (E) and inserting ‘2007;’; and

(3) by adding at the end of the following:

‘(F) $50,000,000 for fiscal year 2010;

‘(G) $52,000,000 for fiscal year 2011;

‘(H) $54,000,000 for fiscal year 2012;

‘(I) $56,000,000 for fiscal year 2013; and

‘(J) $58,000,000 for fiscal year 2014.’.

(h) COMPUTER AND NETWORK SECURITY CAPACITY BUILDING GRANTS- Section 5(a)(6) of such Act (15 U.S.C. 7404(a)(6)) is amended--

(1) by striking ‘and’ in subparagraph (D);

(2) by striking ‘2007’ in subparagraph (E) and inserting ‘2007;’; and

(3) by adding at the end of the following:

‘(F) $40,000,000 for fiscal year 2010;

‘(G) $42,000,000 for fiscal year 2011;

‘(H) $44,000,000 for fiscal year 2012;

‘(I) $46,000,000 for fiscal year 2013; and

‘(J) $48,000,000 for fiscal year 2014.’.

(i) SCIENTIFIC AND ADVANCED TECHNOLOGY ACT GRANTS- Section 5(b)(2) of such Act (15 U.S.C. 7404(b)(2)) is amended--

(1) by striking ‘and’ in subparagraph (D);

(2) by striking ‘2007’ in subparagraph (E) and inserting ‘2007;’; and

(3) by adding at the end of the following:

‘(F) $5,000,000 for fiscal year 2010;

‘(G) $6,000,000 for fiscal year 2011;

‘(H) $7,000,000 for fiscal year 2012;

‘(I) $8,000,000 for fiscal year 2013; and

‘(J) $9,000,000 for fiscal year 2014.’.

(j) GRADUATE TRAINEESHIPS IN COMPUTER AND NETWORK SECURITY RESEARCH- Section 5(c)(7) of such Act (15 U.S.C. 7404(c)(7)) is amended--

(1) by striking ‘and’ in subparagraph (D);

(2) by striking ‘2007’ in subparagraph (E) and inserting ‘2007;’; and

(3) by adding at the end of the following:

‘(F) $20,000,000 for fiscal year 2010;

‘(G) $22,000,000 for fiscal year 2011;

‘(H) $24,000,000 for fiscal year 2012;

‘(I) $26,000,000 for fiscal year 2013; and

‘(J) $28,000,000 for fiscal year 2014.’.

(k) CYBERSECURITY FACULTY DEVELOPMENT TRAINEESHIP PROGRAM- Section 5(e)(9) of such Act (15 U.S.C. 7404(e)(9)) is amended by striking ‘2007.’ and inserting ‘2007 and for each of fiscal years 2010 through 2014.’.

(l) NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT PROGRAM- Section 204(a)(1) of the High-Performance Computing Act of 1991 (15 U.S.C. 5524(a)(1)) is amended--

‘

(1) by striking ‘and’ after the semicolon in subparagraph (B); and

(2) by inserting after subparagraph (C) the following:

‘(D) develop and propose standards and guidelines, and develop measurement techniques and test methods, for enhanced cybersecurity for computer networks and common user interfaces to systems; and’.

SEC. 12. FEDERAL CYBER SCHOLARSHIP-FOR-SERVICE PROGRAM.

(a) IN GENERAL- The Director of the National Science Foundation shall establish a Federal Cyber Scholarship-for-Service program to recruit and train the next generation of Federal information technology workers and security managers.

(b) PROGRAM DESCRIPTION AND COMPONENTS- The program--

(1) shall provide scholarships, that provide full tuition, fees, and a stipend, for up to 1,000 students per year in their pursuit of undergraduate or graduate degrees in the cybersecurity field;

(2) shall require scholarship recipients, as a condition of receiving a scholarship under the program, to agree to serve in the Federal information technology workforce for a period equal to the length of the scholarship following graduation if offered employment in that field by a Federal agency;

(3) shall provide opportunities for students to receive temporary appointments for meaningful employment in the Federal information technology workforce during school vacation periods and for internships;

(4) shall provide a procedure for identifying promising K-12 students for participation in summer work and internship programs that would lead to certification of Federal information technology workforce standards and possible future employment; and

(5) shall examine and develop, if appropriate, programs to promote computer security awareness in secondary and high school classrooms.

(c) HIRING AUTHORITY- For purposes of any law or regulation governing the appointment of individuals in the Federal civil service, upon the successful completion of their studies, students receiving a scholarship under the program shall be hired under the authority provided for in section 213.3102(r) of title 5, Code of Federal Regulations, and be exempt from competitive service. Upon fulfillment of the service term, such individuals shall be converted to a competitive service position without competition if the individual meets the requirements for that position.

(d) ELIGIBILITY- To be eligible to receive a scholarship under this section, an individual shall--

(1) be a citizen of the United States; and

(2) demonstrate a commitment to a career in improving the Nation’s cyber defenses.

(e) CONSIDERATION AND PREFERENCE- In making selections for scholarships under this section, the Director shall--

(1) consider, to the extent possible, a diverse pool of applicants whose interests are of an interdisciplinary nature, encompassing the social scientific as well as the technical dimensions of cyber security; and

(2) give preference to applicants that have participated in the competition and challenge described in section 13.

(f) EVALUATION AND REPORT- The Director shall evaluate and report to the Senate Committee on Commerce, Science, and Transportation and the House of Representatives Committee on Science and Technology on the success of recruiting individuals for the scholarships.

(g) AUTHORIZATION OF APPROPRIATIONS- There are authorized to be appropriated to the National Science Foundation to carry out this section--

(1) $50,000,000 for fiscal year 2010;

(2) $55,000,000 for fiscal year 2011;

(3) $60,000,000 for fiscal year 2012;

(4) $65,000,000 for fiscal year 2013; and

(5) $70,000,000 for fiscal year 2014.

SEC. 13. CYBERSECURITY COMPETITION AND CHALLENGE.

(a) IN GENERAL- The Director of the National Institute of Standards and Technology, directly or through appropriate Federal entities, shall establish cybersecurity competitions and challenges with cash prizes in order to--

(1) attract, identify, evaluate, and recruit talented individuals for the Federal information technology workforce; and

(2) stimulate innovation in basic and applied cybersecurity research, technology development, and prototype demonstration that have the potential for application to the Federal information technology activities of the Federal Government.

(b) TYPES OF COMPETITIONS AND CHALLENGES- The Director shall establish different competitions and challenges targeting the following groups:

(1) High school students.

(2) Undergraduate students.

(3) Graduate students.

(4) Academic and research institutions.
t

(c) TOPICS- In selecting topics for prize competitions, the Director shall consult widely both within and outside the Federal Government, and may empanel advisory committees.

(d) ADVERTISING- The Director shall widely advertise prize competitions, in coordination with the awareness campaign under section 10, to encourage participation.

(e) REQUIREMENTS AND REGISTRATION- For each prize competition, the Director shall publish a notice in the Federal Register announcing the subject of the competition, the rules for being eligible to participate in the competition, the amount of the prize, and the basis on which a winner will be selected.

(f) ELIGIBILITY- To be eligible to win a prize under this section, an individual or entity--

(1) shall have registered to participate in the competition pursuant to any rules promulgated by the Director under subsection (d);

(2) shall have complied with all the requirements under this section;

(3) in the case of a private entity, shall be incorporated in and maintain a primary place of business in the United States, and in the case of an individual, whether participating singly or in a group, shall be a citizen or permanent resident of the United States; and

(4) shall not be a Federal entity or Federal employee acting within the scope of his or her employment.

(g) JUDGES- For each competition, the Director, either directly or through an agreement under subsection (h), shall assemble a panel of qualified judges to select the winner or winners of the prize competition. Judges for each competition shall include individuals from the private sector. A judge may not--

(1) have personal or financial interests in, or be an employee, officer, director, or agent of any entity that is a registered participant in a competition; or

(2) have a familial or financial relationship with an individual who is a registered participant.

(h) ADMINISTERING THE COMPETITION- The Director may enter into an agreement with a private, nonprofit entity to administer the prize competition, subject to the provisions of this section.

(i) Funding-

(1) PRIZES- Prizes under this section may consist of Federal appropriated funds and funds provided by the private sector for such cash prizes. The Director may accept funds from other Federal agencies for such cash prizes. The Director may not give special consideration to any private sector entity in return for a donation.

(2) USE OF UNEXPENDED FUNDS- Notwithstanding any other provision of law, funds appropriated for prize awards under this section shall remain available until expended, and may be transferred, reprogrammed, or expended for other purposes only after the expiration of 10 fiscal years after the fiscal year for which the funds were originally appropriated. No provision in this section permits obligation or payment of funds in violation of the Anti-Deficiency Act (31 U.S.C. 1341).

(3) FUNDING REQUIRED BEFORE PRIZE ANNOUNCED- No prize may be announced until all the funds needed to pay out the announced amount of the prize have been appropriated or committed in writing by a private source. The Director may increase the amount of a prize after an initial announcement is made under subsection (d) if--

(A) notice of the increase is provided in the same manner as the initial notice of the prize; and

(B) the funds needed to pay out the announced amount of the increase have been appropriated or committed in writing by a private source.

(4) NOTICE REQUIRED FOR LARGE AWARDS- No prize competition under this section may offer a prize in an amount greater than $5,000,000 unless 30 days have elapsed after written notice has been transmitted to the Senate Committee on Commerce, Science, and Transportation and the House of Representatives Committee on Science and Technology.

(5) DIRECTOR'S APPROVAL REQUIRED FOR CERTAIN AWARDS- No prize competition under this section may result in the award of more than $1,000,000 in cash prizes without the approval of the Director.

(j) USE OF FEDERAL INSIGNIA- A registered participant in a competition under this section may use any Federal agency's name, initials, or insignia only after prior review and written approval by the Director.

(k) COMPLIANCE WITH EXISTING LAW- The Federal Government shall not, by virtue of offering or providing a prize under this section, be responsible for compliance by registered participants in a prize competition with Federal law, including licensing, export control, and non-proliferation laws and related regulations.

(l) AUTHORIZATION OF APPROPRIATIONS- There are authorized to be appropriated to the National Institute of Standards and Technology to carry out this section $15,000,000 for each of fiscal years 2010 through 2014.

SEC. 14. PUBLIC-PRIVATE CLEARINGHOUSE.

(a) DESIGNATION- The Department of Commerce shall serve as the clearinghouse of cybersecurity threat and vulnerability information to Federal Government and private sector owned critical infrastructure information systems and networks.

(b) FUNCTIONS- The Secretary of Commerce--

(1) shall have access to all relevant data concerning such networks without regard to any provision of law, regulation, rule, or policy restricting such access;

(2) shall manage the sharing of Federal Government and other critical infrastructure threat and vulnerability information between the Federal Government and the persons primarily responsible for the operation and maintenance of the networks concerned; and

(3) shall report regularly to the Congress on threat information held by the Federal Government that is

not shared with the persons primarily responsible for the operation and maintenance of the networks concerned.

(c) INFORMATION SHARING RULES AND PROCEDURES- Within 90 days after the date of enactment of this Act, the Secretary shall publish in the Federal Register a draft description of rules and procedures on how the Federal Government will share cybersecurity threat and vulnerability information with private sector critical infrastructure information systems and networks owners. After a 30 day comment period, the Secretary shall publish a final description of the rules and procedures. The description shall include--

(1) the rules and procedures on how the Federal Government will share cybersecurity threat and vulnerability information with private sector critical infrastructure information systems and networks owners;

(2) the criteria in which private sector owners of critical infrastructure information systems and networks shall share actionable cybersecurity threat and vulnerability information and relevant data with the Federal Government; and

(3) any other rule or procedure that will enhance the sharing of cybersecurity threat and vulnerability information between private sector owners of critical infrastructure information systems and networks and the Federal Government.

SEC. 15. CYBERSECURITY RISK MANAGEMENT REPORT.

Within 1 year after the date of enactment of this Act, the President, or the President's designee, shall report to the Senate Committee on Commerce, Science, and Transportation and the House of Representatives Committee on Science and Technology on the feasibility of--

(1) creating a market for cybersecurity risk management, including the creation of a system of civil liability and insurance (including government reinsurance); and

(2) requiring cybersecurity to be a factor in all bond ratings.

SEC. 16. LEGAL FRAMEWORK REVIEW AND REPORT.

(a) IN GENERAL- Within 1 year after the date of enactment of this Act, the President, or the President's designee, through an appropriate entity, shall complete a comprehensive review of the Federal statutory and legal framework applicable to cyber-related activities in the United States, including--

(1) the Privacy Protection Act of 1980 (42 U.S.C. 2000aa);

(2) the Electronic Communications Privacy Act of 1986 (18 U.S.C. 2510 note);

(3) the Computer Security Act of 1987 (15 U.S.C. 271 et seq.; 40 U.S.C. 759);

(4) the Federal Information Security Management Act of 2002 (44 U.S.C. 3531 et seq.);

(5) the E-Government Act of 2002 (44 U.S.C. 9501 et seq.);

(6) the Defense Production Act of 1950 (50 U.S.C. App. 2061 et seq.);

(7) any other Federal law bearing upon cyber-related activities; and

(8) any applicable Executive Order or agency rule, regulation, guideline.

(b) REPORT- Upon completion of the review, the President, or the President's designee, shall submit a report to the Senate Committee on Commerce, Science, and Transportation, the House of Representatives Committee on Science and Technology, and other appropriate Congressional Committees containing the President's, or the President's designee's, findings, conclusions, and recommendations.

SEC. 17. AUTHENTICATION AND CIVIL LIBERTIES REPORT.

Within 1 year after the date of enactment of this Act, the President, or the President's designee, shall review, and report to Congress, on the feasibility of an identity management and authentication program, with the appropriate civil liberties and privacy protections, for government and critical infrastructure information systems and networks.

SEC. 18. CYBERSECURITY RESPONSIBILITIES AND AUTHORITY.

The President--

(1) within 1 year after the date of enactment of this Act, shall develop and implement a comprehensive national cybersecurity strategy, which shall include--

(A) a long-term vision of the Nation's cybersecurity future; and

(B) a plan that encompasses all aspects of national security, including the participation of the private sector, including critical infrastructure operators and managers;

(2) may declare a cybersecurity emergency and order the limitation or shutdown of Internet traffic to and from any compromised Federal Government or United States critical infrastructure information system or network;

(3) shall designate an agency to be responsible for coordinating the response and restoration of any Federal Government or United States critical infrastructure information system or network affected by a cybersecurity emergency declaration under paragraph (2);

(4) shall, through the appropriate department or agency, review equipment that would be needed after a cybersecurity attack and develop a strategy for the acquisition, storage, and periodic replacement of such equipment;

(5) shall direct the periodic mapping of Federal Government and United States critical infrastructure information systems or networks, and shall develop metrics to measure the effectiveness of the mapping process;

(6) may order the disconnection of any Federal Government or United States critical infrastructure

information systems or networks in the interest of national security;

(7) shall, through the Office of Science and Technology Policy, direct an annual review of all Federal cyber technology research and development investments;

(8) may delegate original classification authority to the appropriate Federal official for the purposes of improving the Nation's cybersecurity posture;

(9) shall, through the appropriate department or agency, promulgate rules for Federal professional responsibilities regarding cybersecurity, and shall provide to the Congress an annual report on Federal agency compliance with those rules;

(10) shall withhold additional compensation, direct corrective action for Federal personnel, or terminate a Federal contract in violation of Federal rules, and shall report any such action to the Congress in an unclassified format within 48 hours after taking any such action; and

(11) shall notify the Congress within 48 hours after providing a cyber-related certification of legality to a United States person.

SEC. 19. QUADRENNIAL CYBER REVIEW.

(a) IN GENERAL- Beginning with 2013 and in every fourth year thereafter, the President, or the President's designee, shall complete a review of the cyber posture of the United States, including an unclassified summary of roles, missions, accomplishments, plans, and programs. The review shall include a comprehensive examination of the cyber strategy, force structure, modernization plans, infrastructure, budget plan, the Nation's ability to recover from a cyberemergency, and other elements of the cyber program and policies with a view toward determining and expressing the cyber strategy of the United States and establishing a revised cyber program for the next 4 years.

(b) INVOLVEMENT OF CYBERSECURITY ADVISORY PANEL-

(1) The President, or the President's designee, shall apprise the Cybersecurity Advisory Panel established or designated under section 3, on an ongoing basis, of the work undertaken in the conduct of the review.

(2) Not later than 1 year before the completion date for the review, the Chairman of the Advisory Panel shall submit to the President, or the President's designee, the Panel's assessment of work undertaken in the conduct of the review as of that date and shall include in the assessment the recommendations of the Panel for improvements to the review, including recommendations for additional matters to be covered in the review.

(c) ASSESSMENT OF REVIEW- Upon completion of the review, the Chairman of the Advisory Panel, on behalf of the Panel, shall prepare and submit to the President, or the President's designee, an assessment of the review in time for the inclusion of the assessment in its entirety in the report under subsection (d).

(d) REPORT- Not later than September 30, 2013, and every 4 years thereafter, the President, or the President's designee, shall submit to the relevant congressional Committees a comprehensive report on the review. The report shall include--

(1) the results of the review, including a comprehensive discussion of the cyber strategy of the United States and the collaboration between the public and private sectors best suited to implement that strategy;

(2) the threats examined for purposes of the review and the scenarios developed in the examination of such threats;

(3) the assumptions used in the review, including assumptions relating to the cooperation of other countries and levels of acceptable risk; and

(4) the Advisory Panel's assessment.

SEC. 20. JOINT INTELLIGENCE THREAT ASSESSMENT.

The Director of National Intelligence and the Secretary of Commerce shall submit to the Congress an annual assessment of, and report on, cybersecurity threats to and vulnerabilities of critical national information, communication, and data network infrastructure.

SEC. 21. INTERNATIONAL NORMS AND CYBERSECURITY DETERRANCE MEASURES.

The President shall--

(1) work with representatives of foreign governments--

(A) to develop norms, organizations, and other cooperative activities for international engagement to improve cybersecurity; and

(B) to encourage international cooperation in improving cybersecurity on a global basis; and

(2) provide an annual report to the Congress on the progress of international initiatives undertaken pursuant to subparagraph (A).

SEC. 22. FEDERAL SECURE PRODUCTS AND SERVICES ACQUISITIONS BOARD.

(a) ESTABLISHMENT- There is established a Secure Products and Services Acquisitions Board. The Board shall be responsible for cybersecurity review and approval of high value products and services acquisition and, in coordination with the National Institute of Standards and Technology, for the establishment of appropriate standards for the validation of software to be acquired by the Federal Government. The Director of the National Institute of Standards and Technology shall develop the review process and provide guidance to the Board. In reviewing software under this subsection, the Board may consider independent secure software validation and verification as key factor for approval.

(b) ACQUISITION STANDARDS- The Director, in cooperation with the Office of Management and Budget and other appropriate Federal agencies, shall ensure that the Board approval is included as a prerequisite to the acquisition of any product or service--

(1) subject to review by the Board; and
t

(2) subject to Federal acquisition standards.

(c) ACQUISITION COMPLIANCE- After the publication of the standards developed under subsection (a), any proposal submitted in response to a request for proposals issued by a Federal agency shall demonstrate compliance with any such applicable standard in order to ensure that cybersecurity products and services are designed to be an integral part of the overall acquisition.

SEC. 23. DEFINITIONS.

In this Act:

(1) ADVISORY PANEL- The term ‘Advisory Panel’ means the Cybersecurity Advisory Panel established or designated under section 3.

(2) CYBER- The term ‘cyber’ means--

(A) any process, program, or protocol relating to the use of the Internet or an intranet, automatic data processing or transmission, or telecommunication via the Internet or an intranet; and

(B) any matter relating to, or involving the use of, computers or computer networks.

(3) FEDERAL GOVERNMENT AND UNITED STATES CRITICAL INFRASTRUCTURE INFORMATION SYSTEMS AND NETWORKS- The term ‘Federal Government and United States critical infrastructure information systems and networks’ includes--

(A) Federal Government information systems and networks; and

(B) State, local, and nongovernmental information systems and networks in the United States designated by the President as critical infrastructure information systems and networks.

(4) INTERNET- The term ‘Internet’ has the meaning given that term by section 4(4) of the High-Performance Computing Act of 1991 (15 U.S.C. 5503(4)).

(5) NETWORK- The term ‘network’ has the meaning given that term by section 4(5) of such Act (15 U.S.C. 5503(5)).

This bill is very large, and loading it may cause your web browser to perform sluggishly, or even freeze. This is especially true for old and/or bad browsers. As an alternative you can download the PDF of the bill or read the text on THOMAS.

Continue on to the bill...

GovTrack.us is not affiliated with the U.S. government or any other group. It is a pet project of a regular joe. (More About GovTrack) / Feedback (but not political opining) is welcome to operations@govtrack.us, but I can't do your research for you, nor can I pass on messages to Members of Congress. This site is "copyleft": You are encouraged to reuse any material on this site. Developers