[STAFF WORKING DRAFT]

JULY 24, 2013

113TH CONGRESS
1ST SESSION

S. _____

To provide for an ongoing, voluntary public-private partnership to improve cybersecurity, and to strengthen cybersecurity research and development, workforce development and education, and public awareness and preparedness, and for other purposes.

IN THE SENATE OF THE UNITED STATES

Mr. ROCKEFELLER (for himself and Mr. THUNE) introduced the following bill; which was read twice and referred to the Committee on _____

A BILL

To provide for an ongoing, voluntary public-private partnership to improve cybersecurity, and to strengthen cybersecurity research and development, workforce development and education, and public awareness and preparedness, 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 2013''.

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

SEC. 2. DEFINITIONS.

In this Act:

(1) CYBERSECURITY MISSION.—The term ''cybersecurity mission'' means activities that encompass the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy,

military, and intelligence missions as such activities relate to the security and stability of cyberspace.

(2) INFORMATION INFRASTRUCTURE.—The term ''information infrastructure'' means the underlying framework that information systems and assets rely on to process, transmit, receive, or store information electronically, including programmable electronic devices, communications networks, and industrial or supervisory control systems and any associated hardware, software, or data.

(3) INFORMATION SYSTEM.—The term ''information system'' has the meaning given that term in section 3502 of title 44, United States Code.

SEC. 3. NO REGULATORY AUTHORITY.

Nothing in this Act shall be construed to confer any regulatory authority on any Federal, State, tribal, or local department or agency.

TITLE I—PUBLIC-PRIVATE COLLABORATION ON CYBERSECURITY

SEC. 101. PUBLIC-PRIVATE COLLABORATION ON CYBERSECURITY.

(a) CYBERSECURITY.—Section 2(c) of the National Institute of Standards and Technology Act (15 U.S.C. 272(c)) is amended—

(1) by redesignating paragraphs (15) through (22) as paragraphs (16) through (23), respectively; and

(2) by inserting after paragraph (14) the following:

''(15) on an ongoing basis, facilitate and support the development of a voluntary, industry-led set of standards, guidelines, best practices, methodologies, procedures, and processes to reduce cyber risks to critical infrastructure (as defined under subsection (e));''.

(b) SCOPE AND LIMITATIONS.—Section 2 of the National Institute of Standards and Technology Act (15 U.S.C. 272) is amended by adding at the end the following:

''(e) CYBER RISKS.—

''(1) IN GENERAL.—In carrying out the activities under subsection (c)(15), the Director—

''(A) shall—

''(i) coordinate closely and continuously with relevant private sector personnel and entities, critical infrastructure owners and operators, sector coordinating councils, Information Sharing and Analysis Centers,

and other relevant industry organizations, and incorporate industry expertise;

''(ii) consult with the heads of agencies with national security responsibilities, sector-specific agencies, State and local governments, the governments of other nations, and international organizations;

''(iii) identify a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risks;

''(iv) include methodologies—

''(I) to identify and mitigate impacts of the cybersecurity measures or controls on business confidentiality; and

''(II) to protect individual privacy and civil liberties;

''(v) incorporate voluntary consensus standards and industry best practices;

''(vi) align with voluntary international standards to the fullest extent possible;

''(vii) prevent duplication of regulatory processes and prevent conflict with or superseding of regulatory requirements, mandatory standards, and related processes; and

''(viii) include such other similar and consistent elements as the Director considers necessary; and

''(B) shall not prescribe or otherwise require—

''(i) the use of specific solutions;

''(ii) the use of specific information or communications technology products or services; or

''(iii) that information or communications technology products or services be designed, developed, or manufactured in a particular manner.

''(2) LIMITATION.—Information shared with or provided to the Institute for the purpose of the activities described under subsection (c)(15) shall not be used by any Federal, State, tribal, or local de-

partment or agency to regulate the activity of any entity.

''(3) DEFINITIONS.—In this subsection:

''(A) CRITICAL INFRASTRUCTURE.—The term 'critical infrastructure' has the meaning given the term in section 1016(e) of the USA PATRIOT Act of 2001 (42 U.S.C. 5195c(e)).

''(B) SECTOR-SPECIFIC AGENCY.—The term 'sector-specific agency' means the Federal department or agency responsible for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment.''.

TITLE II—CYBERSECURITY RESEARCH AND DEVELOPMENT

SEC. 201. FEDERAL CYBERSECURITY RESEARCH AND DEVELOPMENT.

(a) FUNDAMENTAL CYBERSECURITY RESEARCH.—

(1) IN GENERAL.—The Director of the Office of Science and Technology Policy, in coordination with the head of any relevant Federal agency, shall build upon programs and plans in effect as of the date of

enactment of this Act to develop a Federal cybersecurity research and development plan to meet objectives in cybersecurity, such as—

(A) how to design and build complex software-intensive systems that are secure and reliable when first deployed;

(B) how to test and verify that software and hardware, whether developed locally or obtained from a third party, is free of significant known security flaws;

(C) how to test and verify that software and hardware obtained from a third party correctly implements stated functionality, and only that functionality;

(D) how to guarantee the privacy of an individual, including that individual's identity, information, and lawful transactions when stored in distributed systems or transmitted over networks;

(E) how to build new protocols to enable the Internet to have robust security as one of the key capabilities of the Internet;

(F) how to determine the origin of a message transmitted over the Internet;

(G) how to support privacy in conjunction with improved security;

(H) how to address the growing problem of insider threats;

(I) how improved consumer education and digital literacy initiatives can address human factors that contribute to cybersecurity;

(J) how to protect information processed, transmitted, or stored using cloud computing or transmitted through wireless services; and

(K) any additional objectives the Director of the Office of Science and Technology Policy, in coordination with the head of any relevant Federal agency and with input from stakeholders, including industry and academia, determines appropriate.

(2) REQUIREMENTS.—

(A) IN GENERAL.—The Federal cybersecurity research and development plan shall identify and prioritize near-term, mid-term, and long-term research in computer and information science and engineering to meet the objectives under paragraph (1), including research in the areas described in section 4(a)(1)

of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)(1)).

(B) PRIVATE SECTOR EFFORTS.—In developing, implementing, and updating the Federal cybersecurity research and development plan, the Director of the Office of Science and Technology Policy shall work in close cooperation with industry, academia, and other interested stakeholders to ensure, to the extent possible, that Federal cybersecurity research and development is not duplicative of private sector efforts.

(3) TRIENNIAL UPDATES.—

(A) IN GENERAL.—The Federal cybersecurity research and development plan shall be updated triennially.

(B) REPORT TO CONGRESS.—The Director of the Office of Science and Technology Policy shall submit the plan, not later than 1 year after the date of enactment of this Act, and each updated plan under this section to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science, Space, and Technology of the House of Representatives.

(b) CYBERSECURITY PRACTICES RESEARCH.—The Director of the National Science Foundation shall support research that—

(1) develops, evaluates, disseminates, and integrates new cybersecurity practices and concepts into the core curriculum of computer science programs and of other programs where graduates of such programs have a substantial probability of developing software after graduation, including new practices and concepts relating to secure coding education and improvement programs; and

(2) develops new models for professional development of faculty in cybersecurity education, including secure coding development.

(c) CYBERSECURITY MODELING AND TEST BEDS.—

(1) REVIEW.—Not later than 1 year after the date of enactment of this Act, the Director the National Science Foundation, in coordination with the Director of the Office of Science and Technology Policy, shall conduct a review of cybersecurity test beds in existence on the date of enactment of this Act to inform the grants under paragraph (2). The review shall include an assessment of whether a sufficient number of cybersecurity test beds are avail-

able to meet the research needs under the Federal cybersecurity research and development plan.

(2) ADDITIONAL CYBERSECURITY MODELING AND TEST BEDS.—

(A) IN GENERAL.—If the Director of the National Science Foundation, after the review under paragraph (1), determines that the research needs under the Federal cybersecurity research and development plan require the establishment of additional cybersecurity test beds, the Director of the National Science Foundation, in coordination with the Secretary of Commerce and the Secretary of Homeland Security, may award grants to institutions of higher education or research and development non-profit institutions to establish cybersecurity test beds.

(B) REQUIREMENT.—The cybersecurity test beds under subparagraph (A) shall be sufficiently large in order to model the scale and complexity of real-time cyber attacks and defenses on real world networks and environments.

(C) ASSESSMENT REQUIRED.—The Director of the National Science Foundation, in co-

ordination with the Secretary of Commerce and the Secretary of Homeland Security, shall evaluate the effectiveness of any grants awarded under this subsection in meeting the objectives of the Federal cybersecurity research and development plan under subsection (a) no later than 2 years after the review under paragraph (1) of this subsection, and periodically thereafter.

(d) COORDINATION WITH OTHER RESEARCH INITIATIVES.—In accordance with the responsibilities under section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511), the Director the Office of Science and Technology Policy shall coordinate, to the extent practicable, Federal research and development activities under this section with other ongoing research and development security-related initiatives, including research being conducted by—

(1) the National Science Foundation;

(2) the National Institute of Standards and Technology;

(3) the Department of Homeland Security;

(4) other Federal agencies;

(5) other Federal and private research laboratories, research entities, and universities;

(6) institutions of higher education;

(7) relevant nonprofit organizations; and

(8) international partners of the United States.

(e) NATIONAL SCIENCE FOUNDATION COMPUTER AND NETWORK SECURITY RESEARCH GRANT AREAS.—Section 4(a)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)(1)) is amended—

(1) in subparagraph (H), by striking ''and'' at the end;

(2) in subparagraph (I), by striking the period at the end and inserting a semicolon; and

(3) by adding at the end the following:

''(J) secure fundamental protocols that are integral to 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;

''(N) mitigation and rapid recovery methods;

''(O) security of wireless networks and mobile devices; and

''(P) security of cloud infrastructure and services.''.

(f) RESEARCH ON THE SCIENCE OF CYBERSECURITY.—The head of each agency and department identified under section 101(a)(3)(B) of the High-

Performance Computing Act of 1991 (15 U.S.C. 5511(a)(3)(B)), through existing programs and activities, shall support research that will lead to the development of a scientific foundation for the field of cybersecurity, including research that increases understanding of the underlying principles of securing complex networked systems, enables repeatable experimentation, and creates quantifiable security metrics.

SEC. 202. COMPUTER AND NETWORK SECURITY RESEARCH CENTERS.

Section 4(b) of the Cyber Security Research and Development Act (15 U.S.C. 7403(b)) is amended—

(1) by striking ''the center'' in paragraph (4)(D) and inserting ''the Center''; and

(2) in paragraph (5)—

(A) by striking ''and'' at the end of subparagraph (C);

(B) by striking the period at the end of subparagraph (D) and inserting a semicolon; and

(C) by adding at the end the following:

''(E) the demonstrated capability of the applicant to conduct high performance computation integral to complex computer and net-

work security research, through on-site or off-site computing;

''(F) the applicant's affiliation with private sector entities involved with industrial research described in subsection (a)(1);

''(G) the capability of the applicant to conduct research in a secure environment;

''(H) the applicant's affiliation with existing research programs of the Federal Government;

''(I) the applicant's experience managing public-private partnerships to transition new technologies into a commercial setting or the government user community; and

''(J) the capability of the applicant to conduct interdisciplinary cybersecurity research, such as in law, economics, or behavioral sciences.''.

TITLE III—EDUCATION AND WORKFORCE DEVELOPMENT.

SEC. 301. CYBERSECURITY COMPETITIONS AND CHALLENGES.

(a) IN GENERAL.—The Secretary of Commerce, Director of the National Science Foundation, and Secretary of Homeland Security shall—

(1) support competitions and challenges under section 105 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 3989) or any other provision of law, as appropriate—

(A) to identify, develop, and recruit talented individuals to perform duties relating to the security of information infrastructure in Federal, State, and local government agencies, and the private sector; or

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

(2) ensure the effective operation of the competitions and challenges under this section.

(b) PARTICIPATION.—Participants in the competitions and challenges under subsection (a)(1) may include—

(1) students enrolled in grades 9 through 12;

(2) students enrolled in a postsecondary program of study leading to a baccalaureate degree at an institution of higher education;

(3) students enrolled in a postbaccalaureate program of study at an institution of higher education;

(4) institutions of higher education and research institutions;

(5) veterans; and

(6) other groups or individuals that the Secretary of Commerce, Director of the National Science Foundation, and Secretary of Homeland Security determine appropriate.

(c) AFFILIATION AND COOPERATIVE AGREEMENTS.—Competitions and challenges under this section may be carried out through affiliation and cooperative agreements with—

(1) Federal agencies;

(2) regional, State, or school programs supporting the development of cyber professionals;

(3) State, local, and tribal governments; or

(4) other private sector organizations.

(d) AREAS OF SKILL.—Competitions and challenges under subsection (a)(1)(A) shall be designed to identify, develop, and recruit exceptional talent relating to—

(1) ethical hacking;

(2) penetration testing;

(3) vulnerability assessment;

(4) continuity of system operations;

(5) security in design;

(6) cyber forensics;

(7) offensive and defensive cyber operations; and

(8) other areas the Secretary of Commerce, Director of the National Science Foundation, and Secretary of Homeland Security consider necessary to fulfill the cybersecurity mission.

(e) TOPICS.—In selecting topics for competitions and challenges under subsection (a)(1), the Secretary of Commerce, Director of the National Science Foundation, and Secretary of Homeland Security—

(1) shall consult widely both within and outside the Federal Government; and

(2) may empanel advisory committees.

(f) INTERNSHIPS.—The Director of the Office of Personnel Management may support, as appropriate, internships or other work experience in the Federal Government to the winners of the competitions and challenges under this section.

SEC. 302. FEDERAL CYBER SCHOLARSHIP-FOR-SERVICE PROGRAM.

(a) IN GENERAL.—The Director of the National Science Foundation, in coordination with the Director of

the Office of Personnel Management and Secretary of Homeland Security, shall continue a Federal Cyber Scholarship-for-Service program to recruit and train the next generation of information technology professionals, industrial control system security professionals, and security managers to meet the needs of the cybersecurity mission for Federal, State, local, and tribal governments.

(b) PROGRAM DESCRIPTION AND COMPONENTS.—The Federal Cyber Scholarship-for-Service program shall—

(1) provide scholarships to students who are enrolled in programs of study at institutions of higher education leading to degrees or specialized program certifications in the cybersecurity field;

(2) provide the scholarship recipients with summer internship opportunities or other meaningful temporary appointments in the Federal information technology workforce; and

(3) provide a procedure by which the National Science Foundation or a Federal agency, consistent with regulations of the Office of Personnel Management, may request and fund security clearances for scholarship recipients, including providing for clearances during internships or other temporary appointments and after receipt of their degrees.

(c) SCHOLARSHIP AMOUNTS.—Each scholarship under subsection (b) shall be in an amount that covers the student's tuition and fees at the institution under subsection (b)(1) and provides the student with an additional stipend.

(d) SCHOLARSHIP CONDITIONS.—Each scholarship recipient, as a condition of receiving a scholarship under the program, shall enter into an agreement under which the recipient agrees to work in the cybersecurity mission of a Federal, State, local, or tribal agency for a period equal to the length of the scholarship following receipt of the student's degree.

(e) HIRING AUTHORITY.—

(1) APPOINTMENT IN EXCEPTED SERVICE.—Notwithstanding any provision of chapter 33 of title 5, United States Code, governing appointments in the competitive service, an agency shall appoint in the excepted service an individual who has completed the academic program for which a scholarship was awarded.

(2) NONCOMPETITIVE CONVERSION.—Except as provided in paragraph (4), upon fulfillment of the service term, an employee appointed under paragraph (1) may be converted noncompetitively to term, career-conditional or career appointment.

(3) TIMING OF CONVERSION.—An agency may noncompetitively convert a term employee appointed under paragraph (2) to a career-conditional or career appointment before the term appointment expires.

(4) AUTHORITY TO DECLINE CONVERSION.—An agency may decline to make the noncompetitive conversion or appointment under paragraph (2) for cause.

(f) ELIGIBILITY.—To be eligible to receive a scholarship under this section, an individual shall—

(1) be a citizen or lawful permanent resident of the United States;

(2) demonstrate a commitment to a career in improving the security of information infrastructure; and

(3) have demonstrated a high level of proficiency in mathematics, engineering, or computer sciences.

(g) REPAYMENT.—If a scholarship recipient does not meet the terms of the program under this section, the recipient shall refund the scholarship payments in accordance with rules established by the Director of the National Science Foundation, in coordination with the Director of

the Office of Personnel Management and Secretary of Homeland Security.

(h) EVALUATION AND REPORT.—The Director of the National Science Foundation shall evaluate and report periodically to Congress on the success of recruiting individuals for scholarships under this section and on hiring and retaining those individuals in the public sector workforce.

SEC. 303. STUDY AND ANALYSIS OF EDUCATION, ACCREDITATION, TRAINING, AND CERTIFICATION OF INFORMATION INFRASTRUCTURE AND CYBERSECURITY PROFESSIONALS.

(a) STUDY.—The Director of the National Science Foundation and the Secretary of Homeland Security shall undertake to enter into appropriate arrangements with the National Academy of Sciences to conduct a comprehensive study of government, academic, and private-sector education, accreditation, training, and certification programs for the development of professionals in information infrastructure and cybersecurity. The agreement shall require the National Academy of Sciences to consult with sector coordinating councils and relevant governmental agencies, regulatory entities, and nongovernmental organizations in the course of the study.

(b) SCOPE.—The study shall include—

(1) an evaluation of the body of knowledge and various skills that specific categories of professionals in information infrastructure and cybersecurity should possess in order to secure information systems;

(2) an assessment of whether existing government, academic, and private-sector education, accreditation, training, and certification programs provide the body of knowledge and various skills described in paragraph (1);

(3) an evaluation of—

(A) the state of cybersecurity education at institutions of higher education in the United States;

(B) the extent of professional development opportunities for faculty in cybersecurity principles and practices;

(C) the extent of the partnerships and collaborative cybersecurity curriculum development activities that leverage industry and government needs, resources, and tools;

(D) the proposed metrics to assess progress toward improving cybersecurity education; and

(E) the descriptions of the content of cybersecurity courses in undergraduate computer science curriculum;

(4) an analysis of any barriers to the Federal Government recruiting and hiring cybersecurity talent, including barriers relating to compensation, the hiring process, job classification, and hiring flexibility; and

(5) an analysis of the sources and availability of cybersecurity talent, a comparison of the skills and expertise sought by the Federal Government and the private sector, an examination of the current and future capacity of United States institutions of higher education, including community colleges, to provide current and future cybersecurity professionals, through education and training activities, with those skills sought by the Federal Government, State and local entities, and the private sector.

(c) REPORT.—Not later than 1 year after the date of enactment of this Act, the National Academy of Sciences shall submit to the President and Congress a report on the results of the study. The report shall include—

(1) findings regarding the state of information infrastructure and cybersecurity education, accreditation, training, and certification programs, includ-

ing specific areas of deficiency and demonstrable progress; and

(2) recommendations for further research and the improvement of information infrastructure and cybersecurity education, accreditation, training, and certification programs.

TITLE IV—CYBERSECURITY AWARENESS AND PREPAREDNESS

SEC. 401. NATIONAL CYBERSECURITY AWARENESS AND PREPAREDNESS CAMPAIGN.

(a) NATIONAL CYBERSECURITY AWARENESS AND PREPAREDNESS CAMPAIGN.—The Director of the National Institute of Standards and Technology (referred to in this section as the ''Director''), in consultation with appropriate Federal agencies, shall continue to coordinate a national cybersecurity awareness and preparedness campaign, such as—

(1) a campaign to increase public awareness of cybersecurity, cyber safety, and cyber ethics, including the use of the Internet, social media, entertainment, and other media to reach the public;

(2) a campaign to increase the understanding of State and local governments and private sector entities of—

(A) the benefits of ensuring effective risk management of the information infrastructure versus the costs of failure to do so; and

(B) the methods to mitigate and remediate vulnerabilities;

(3) support for formal cybersecurity education programs at all education levels to prepare skilled cybersecurity and computer science workers for the private sector and Federal, State, and local government; and

(4) initiatives to evaluate and forecast future cybersecurity workforce needs of the Federal government and develop strategies for recruitment, training, and retention.

(b) CONSIDERATIONS.—In carrying out the authority described in subsection (a), the Director, in consultation with appropriate Federal agencies, shall leverage existing programs designed to inform the public of safety and security of products or services, including self-certifications and independently-verified assessments regarding the quantification and valuation of information security risk.

(c) STRATEGIC PLAN.—The Director, in cooperation with relevant Federal agencies and other stakeholders, shall build upon programs and plans in effect as of the date of enactment of this Act to develop and implement

a strategic plan to guide Federal programs and activities in support of the national cybersecurity awareness and preparedness campaign under subsection (a).

(d) REPORT.—Not later than 1 year after the date of enactment of this Act, and every 5 years thereafter, the Director shall transmit the strategic plan under subsection (c) to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science, Space, and Technology of the House of Representatives.