AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. 1353

One Hundred Thirteenth Congress of the United States of America

AT THE SECOND SESSION

Begun and held at the City of Washington on Friday, the third day of January, two thousand and fourteen

An Act

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 Enhancement Act of 2014".

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

Sec. 1. Short title; table of contents.
Sec. 2. Definitions.
Sec. 3. No regulatory authority.
Sec. 4. No additional funds authorized.

TITLE I—PUBLIC-PRIVATE COLLABORATION ON CYBERSECURITY

Sec. 101. Public-private collaboration on cybersecurity.

TITLE II—CYBERSECURITY RESEARCH AND DEVELOPMENT

Sec. 201. Federal cybersecurity research and development.
Sec. 202. Computer and network security research centers.
Sec. 203. Cybersecurity automation and checklists for government systems.
Sec. 204. National Institute of Standards and Technology cybersecurity research and development.

TITLE III—EDUCATION AND WORKFORCE DEVELOPMENT

Sec. 301. Cybersecurity competitions and challenges.
Sec. 302. Federal cyber scholarship-for-service program.

TITLE IV—CYBERSECURITY AWARENESS AND PREPAREDNESS

Sec. 401. National cybersecurity awareness and education program.

TITLE V—ADVANCEMENT OF CYBERSECURITY TECHNICAL STANDARDS

Sec. 501. Definitions.
Sec. 502. International cybersecurity technical standards.
Sec. 503. Cloud computing strategy.
Sec. 504. Identity management research and development.

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 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.

SEC. 4. NO ADDITIONAL FUNDS AUTHORIZED.

No additional funds are authorized to carry out this Act, and the amendments made by this Act. This Act, and the amendments made by this Act, shall be carried out using amounts otherwise authorized or appropriated.

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, consensus-based, industry-led set of standards, guidelines, best practices, methodologies, procedures, and processes to cost-effectively 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 regularly with relevant private sector personnel and entities, critical infrastructure owners and operators, and other relevant industry organizations, including Sector Coordinating Councils and Information Sharing and Analysis Centers, and incorporate industry expertise;

"(ii) consult with the heads of agencies with national security responsibilities, sector-specific agencies and other appropriate 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 department or agency to regulate the activity of any entity. Nothing in this paragraph shall be construed to modify any regulatory requirement to report or submit information to a Federal, State, tribal, or local department or agency.

"(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.".

(c) STUDY AND REPORTS.—

(1) STUDY.—The Comptroller General of the United States shall conduct a study that assesses—

(A) the progress made by the Director of the National Institute of Standards and Technology in facilitating the development of standards and procedures to reduce cyber risks to critical infrastructure in accordance with section 2(c)(15) of the National Institute of Standards and Technology Act, as added by this section;

(B) the extent to which the Director's facilitation efforts are consistent with the directive in such section that the

development of such standards and procedures be voluntary and led by industry representatives;

(C) the extent to which other Federal agencies have promoted and sectors of critical infrastructure (as defined in section 1016(e) of the USA PATRIOT Act of 2001 (42 U.S.C. 5195c(e))) have adopted a voluntary, industry-led set of standards, guidelines, best practices, methodologies, procedures, and processes to reduce cyber risks to critical infrastructure in accordance with such section 2(c)(15);

(D) the reasons behind the decisions of sectors of critical infrastructure (as defined in subparagraph (C)) to adopt or to not adopt the voluntary standards described in subparagraph (C); and

(E) the extent to which such voluntary standards have proved successful in protecting critical infrastructure from cyber threats.

(2) REPORTS.—Not later than 1 year after the date of the enactment of this Act, and every 2 years thereafter for the following 6 years, the Comptroller General shall submit a report, which summarizes the findings of the study conducted under paragraph (1), to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science, Space, and Technology of the House of Representatives.

TITLE II—CYBERSECURITY RESEARCH AND DEVELOPMENT

SEC. 201. FEDERAL CYBERSECURITY RESEARCH AND DEVELOPMENT.

(a) FUNDAMENTAL CYBERSECURITY RESEARCH.—

(1) FEDERAL CYBERSECURITY RESEARCH AND DEVELOPMENT STRATEGIC PLAN.—The heads of the applicable agencies and departments, working through the National Science and Technology Council and the Networking and Information Technology Research and Development Program, shall develop and update every 4 years a Federal cybersecurity research and development strategic plan (referred to in this subsection as the "strategic plan") based on an assessment of cybersecurity risk to guide the overall direction of Federal cybersecurity and information assurance research and development for information technology and networking systems. The heads of the applicable agencies and departments shall build upon existing programs and plans to develop the strategic 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 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 heads of the applicable agencies and departments, in coordination with the head of any relevant Federal agency and with input from stakeholders, including appropriate national laboratories, industry, and academia, determine appropriate.

(2) REQUIREMENTS.—

(A) CONTENTS OF PLAN.—The strategic plan shall—

(i) specify and prioritize near-term, mid-term, and long-term research objectives, including objectives associated with the research identified in section 4(a)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)(1));

(ii) specify how the near-term objectives described in clause (i) complement research and development areas in which the private sector is actively engaged;

(iii) describe how the heads of the applicable agencies and departments will focus on innovative, transformational technologies with the potential to enhance the security, reliability, resilience, and trustworthiness of the digital infrastructure, and to protect consumer privacy;

(iv) describe how the heads of the applicable agencies and departments will foster the rapid transfer of research and development results into new cybersecurity technologies and applications for the timely benefit of society and the national interest, including through the dissemination of best practices and other outreach activities;

(v) describe how the heads of the applicable agencies and departments will establish and maintain a national research infrastructure for creating, testing, and evaluating the next generation of secure networking and information technology systems; and

(vi) describe how the heads of the applicable agencies and departments will facilitate access by academic researchers to the infrastructure described in clause (v), as well as to relevant data, including event data.

(B) PRIVATE SECTOR EFFORTS.—In developing, implementing, and updating the strategic plan, the heads of the applicable agencies and departments, working through the National Science and Technology Council and Networking and Information Technology Research and Development Program, 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.

(C) RECOMMENDATIONS.—In developing and updating the strategic plan the heads of the applicable agencies and departments shall solicit recommendations and advice from—

(i) the advisory committee established under section 101(b)(1) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(b)(1)); and

(ii) a wide range of stakeholders, including industry, academia, including representatives of minority serving institutions and community colleges, National Laboratories, and other relevant organizations and institutions.

(D) IMPLEMENTATION ROADMAP.—The heads of the applicable agencies and departments, working through the National Science and Technology Council and Networking and Information Technology Research and Development Program, shall develop and annually update an implementation roadmap for the strategic plan. The implementation roadmap shall—

(i) specify the role of each Federal agency in carrying out or sponsoring research and development to meet the research objectives of the strategic plan, including a description of how progress toward the research objectives will be evaluated;

(ii) specify the funding allocated to each major research objective of the strategic plan and the source of funding by agency for the current fiscal year;

(iii) estimate the funding required for each major research objective of the strategic plan for the following 3 fiscal years; and

(iv) track ongoing and completed Federal cybersecurity research and development projects.

(3) REPORTS TO CONGRESS.—The heads of the applicable agencies and departments, working through the National Science and Technology Council and Networking and Information Technology Research and Development Program, shall submit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science, Space, and Technology of the House of Representatives—

(A) the strategic plan not later than 1 year after the date of enactment of this Act;

(B) each quadrennial update to the strategic plan; and

(C) the implementation roadmap under subparagraph (D), and its annual updates, which shall be appended to the annual report required under section 101(a)(2)(D) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(2)(D)).

(4) DEFINITION OF APPLICABLE AGENCIES AND DEPARTMENTS.—In this subsection, the term "applicable agencies and departments" means the agencies and departments identified in clauses (i) through (x) of section 101(a)(3)(B) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(3)(B)) or designated under clause (xi) of that section.

(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 of 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 available to meet the research needs under the Federal cybersecurity research and development strategic plan. Upon completion, the Director shall submit the review to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science, Space, and Technology of the House of Representatives.

(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 strategic 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 nonprofit institutions to establish cybersecurity test beds.

(B) REQUIREMENT.—The cybersecurity test beds under subparagraph (A) shall be sufficiently robust 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 coordination 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 strategic plan not 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 of 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) in paragraph (3), by striking "the research areas" and inserting the following: "improving the security and resiliency

of information technology, reducing cyber vulnerabilities, and anticipating and mitigating consequences of cyber attacks on critical infrastructure, by conducting research in the areas";

(2) by striking "the center" in paragraph (4)(D) and inserting "the Center"; and

(3) 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 network 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;

"(J) the capability of the applicant to conduct interdisciplinary cybersecurity research, basic and applied, such as in law, economics, or behavioral sciences; and

"(K) the capability of the applicant to conduct research in areas such as systems security, wireless security, networking and protocols, formal methods and high-performance computing, nanotechnology, or industrial control systems.".

SEC. 203. CYBERSECURITY AUTOMATION AND CHECKLISTS FOR GOVERNMENT SYSTEMS.

Section 8(c) of the Cyber Security Research and Development Act (15 U.S.C. 7406(c)) is amended to read as follows:

"(c) SECURITY AUTOMATION AND CHECKLISTS FOR GOVERNMENT SYSTEMS.—

"(1) IN GENERAL.—The Director of the National Institute of Standards and Technology shall, as necessary, develop and revise security automation standards, associated reference materials (including protocols), and checklists providing settings and option selections that minimize the security risks associated with each information technology hardware or software system and security tool that is, or is likely to become, widely used within the Federal Government, thereby enabling standardized and interoperable technologies, architectures, and frameworks for continuous monitoring of information security within the Federal Government.

"(2) PRIORITIES FOR DEVELOPMENT.—The Director of the National Institute of Standards and Technology shall establish priorities for the development of standards, reference materials, and checklists under this subsection on the basis of—

"(A) the security risks associated with the use of the system;

"(B) the number of agencies that use a particular system or security tool;

"(C) the usefulness of the standards, reference materials, or checklists to Federal agencies that are users or potential users of the system;

"(D) the effectiveness of the associated standard, reference material, or checklist in creating or enabling continuous monitoring of information security; or

"(E) such other factors as the Director of the National Institute of Standards and Technology determines to be appropriate.

"(3) EXCLUDED SYSTEMS.—The Director of the National Institute of Standards and Technology may exclude from the application of paragraph (1) any information technology hardware or software system or security tool for which such Director determines that the development of a standard, reference material, or checklist is inappropriate because of the infrequency of use of the system, the obsolescence of the system, or the lack of utility or impracticability of developing a standard, reference material, or checklist for the system.

"(4) DISSEMINATION OF STANDARDS AND RELATED MATERIALS.—The Director of the National Institute of Standards and Technology shall ensure that Federal agencies are informed of the availability of any standard, reference material, checklist, or other item developed under this subsection.

"(5) AGENCY USE REQUIREMENTS.—The development of standards, reference materials, and checklists under paragraph (1) for an information technology hardware or software system or tool does not—

"(A) require any Federal agency to select the specific settings or options recommended by the standard, reference material, or checklist for the system;

"(B) establish conditions or prerequisites for Federal agency procurement or deployment of any such system;

"(C) imply an endorsement of any such system by the Director of the National Institute of Standards and Technology; or

"(D) preclude any Federal agency from procuring or deploying other information technology hardware or software systems for which no such standard, reference material, or checklist has been developed or identified under paragraph (1).".

SEC. 204. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY CYBERSECURITY RESEARCH AND DEVELOPMENT.

Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) is amended—

(1) by redesignating subsection (e) as subsection (f); and

(2) by inserting after subsection (d) the following:

"(e) INTRAMURAL SECURITY RESEARCH.—As part of the research activities conducted in accordance with subsection (d)(3), the Institute shall, to the extent practicable and appropriate—

"(1) conduct a research program to develop a unifying and standardized identity, privilege, and access control management framework for the execution of a wide variety of resource protection policies and that is amenable to implementation within

a wide variety of existing and emerging computing environments;

"(2) carry out research associated with improving the security of information systems and networks;

"(3) carry out research associated with improving the testing, measurement, usability, and assurance of information systems and networks;

"(4) carry out research associated with improving security of industrial control systems;

"(5) carry out research associated with improving the security and integrity of the information technology supply chain; and

"(6) carry out any additional research the Institute determines appropriate.".

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, in consultation with the Director of the Office of Personnel Management, shall—

(1) support competitions and challenges under section 24 of the Stevenson-Wydler Technology Innovation Act of 1980 (15 U.S.C. 3719) (as amended by 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 technology in Federal, State, local, and tribal 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 through qualified institutions of higher education, including community colleges, 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) prioritize the employment placement of scholarship recipients in the Federal Government.

(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) for not more than 3 years and provides the student with an additional stipend.

(d) POST-AWARD EMPLOYMENT OBLIGATIONS.—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 eligible degree 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 technology;

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

(4) be a full-time student in an eligible degree program at a qualified institution of higher education, as determined by the Director of the National Science Foundation; and

(5) accept the terms of a scholarship under this section.

(g) CONDITIONS OF SUPPORT.—

(1) IN GENERAL.—As a condition of receiving a scholarship under this section, a recipient shall agree to provide the qualified institution of higher education with annual verifiable documentation of post-award employment and up-to-date contact information.

(2) TERMS.—A scholarship recipient under this section shall be liable to the United States as provided in subsection (i) if the individual—

(A) fails to maintain an acceptable level of academic standing at the applicable institution of higher education, as determined by the Director of the National Science Foundation;

(B) is dismissed from the applicable institution of higher education for disciplinary reasons;

(C) withdraws from the eligible degree program before completing the program;

(D) declares that the individual does not intend to fulfill the post-award employment obligation under this section; or

(E) fails to fulfill the post-award employment obligation of the individual under this section.

(h) MONITORING COMPLIANCE.—As a condition of participating in the program, a qualified institution of higher education shall—

(1) enter into an agreement with the Director of the National Science Foundation, to monitor the compliance of scholarship recipients with respect to their post-award employment obligations; and

(2) provide to the Director of the National Science Foundation, on an annual basis, the post-award employment documentation required under subsection (g)(1) for scholarship recipients through the completion of their post-award employment obligations.

(i) AMOUNT OF REPAYMENT.—

(1) LESS THAN 1 YEAR OF SERVICE.—If a circumstance described in subsection (g)(2) occurs before the completion of 1 year of a post-award employment obligation under this section, the total amount of scholarship awards received by the individual under this section shall—

(A) be repaid; or

(B) be treated as a loan to be repaid in accordance with subsection (j).

(2) 1 OR MORE YEARS OF SERVICE.—If a circumstance described in subparagraph (D) or (E) of subsection (g)(2) occurs after the completion of 1 or more years of a post-award employment obligation under this section, the total amount of scholarship awards received by the individual under this section, reduced by the ratio of the number of years of service completed divided by the number of years of service required, shall—

(A) be repaid; or

(B) be treated as a loan to be repaid in accordance with subsection (j).

(j) REPAYMENTS.—A loan described subsection (i) shall—

(1) be treated as a Federal Direct Unsubsidized Stafford Loan under part D of title IV of the Higher Education Act of 1965 (20 U.S.C. 1087a et seq.); and

(2) be subject to repayment, together with interest thereon accruing from the date of the scholarship award, in accordance with terms and conditions specified by the Director of the National Science Foundation (in consultation with the Secretary of Education) in regulations promulgated to carry out this subsection.

(k) COLLECTION OF REPAYMENT.—

(1) IN GENERAL.—In the event that a scholarship recipient is required to repay the scholarship award under this section, the qualified institution of higher education providing the scholarship shall—

(A) determine the repayment amounts and notify the recipient and the Director of the National Science Foundation of the amounts owed; and

(B) collect the repayment amounts within a period of time as determined by the Director of the National Science Foundation, or the repayment amounts shall be treated as a loan in accordance with subsection (j).

(2) RETURNED TO TREASURY.—Except as provided in paragraph (3), any repayment under this subsection shall be returned to the Treasury of the United States.

(3) RETAIN PERCENTAGE.—A qualified institution of higher education may retain a percentage of any repayment the institution collects under this subsection to defray administrative costs associated with the collection. The Director of the National Science Foundation shall establish a single, fixed percentage that will apply to all eligible entities.

(l) EXCEPTIONS.—The Director of the National Science Foundation may provide for the partial or total waiver or suspension of any service or payment obligation by an individual under this section whenever compliance by the individual with the obligation is impossible or would involve extreme hardship to the individual, or if enforcement of such obligation with respect to the individual would be unconscionable.

(m) 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.

TITLE IV—CYBERSECURITY AWARENESS AND PREPAREDNESS

SEC. 401. NATIONAL CYBERSECURITY AWARENESS AND EDUCATION PROGRAM.

(a) NATIONAL CYBERSECURITY AWARENESS AND EDUCATION PROGRAM.—The Director of the National Institute of Standards and Technology (referred to in this section as the "Director"), in consultation with appropriate Federal agencies, industry, educational institutions, National Laboratories, the Networking and Information Technology Research and Development program, and other organizations shall continue to coordinate a national cybersecurity awareness and education program, that includes activities such as—

(1) the widespread dissemination of cybersecurity technical standards and best practices identified by the Director;

(2) efforts to make cybersecurity best practices usable by individuals, small to medium-sized businesses, educational institutions, and State, local, and tribal governments;

(3) increasing public awareness of cybersecurity, cyber safety, and cyber ethics;

(4) increasing the understanding of State, local, and tribal governments, institutions of higher education, and private sector entities of—

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

(B) the methods to mitigate and remediate vulnerabilities;

(5) supporting formal cybersecurity education programs at all education levels to prepare and improve a skilled cybersecurity and computer science workforce for the private sector and Federal, State, local, and tribal government; and

(6) promoting 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 education program 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.

TITLE V—ADVANCEMENT OF CYBERSECURITY TECHNICAL STANDARDS

SEC. 501. DEFINITIONS.

In this title:

(1) DIRECTOR.—The term "Director" means the Director of the National Institute of Standards and Technology.

(2) INSTITUTE.—The term "Institute" means the National Institute of Standards and Technology.

SEC. 502. INTERNATIONAL CYBERSECURITY TECHNICAL STANDARDS.

(a) IN GENERAL.—The Director, in coordination with appropriate Federal authorities, shall—

(1) as appropriate, ensure coordination of Federal agencies engaged in the development of international technical standards related to information system security; and

(2) not later than 1 year after the date of enactment of this Act, develop and transmit to Congress a plan for ensuring such Federal agency coordination.

(b) CONSULTATION WITH THE PRIVATE SECTOR.—In carrying out the activities specified in subsection (a)(1), the Director shall ensure consultation with appropriate private sector stakeholders.

SEC. 503. CLOUD COMPUTING STRATEGY.

(a) IN GENERAL.—The Director, in coordination with the Office of Management and Budget, in collaboration with the Federal Chief Information Officers Council, and in consultation with other relevant Federal agencies and stakeholders from the private sector, shall continue to develop and encourage the implementation of a comprehensive strategy for the use and adoption of cloud computing services by the Federal Government.

(b) ACTIVITIES.—In carrying out the strategy described under subsection (a), the Director shall give consideration to activities that—

(1) accelerate the development, in collaboration with the private sector, of standards that address interoperability and portability of cloud computing services;

(2) advance the development of conformance testing performed by the private sector in support of cloud computing standardization; and

(3) support, in coordination with the Office of Management and Budget, and in consultation with the private sector, the development of appropriate security frameworks and reference materials, and the identification of best practices, for use by Federal agencies to address security and privacy requirements to enable the use and adoption of cloud computing services, including activities—

(A) to ensure the physical security of cloud computing data centers and the data stored in such centers;

(B) to ensure secure access to the data stored in cloud computing data centers;

(C) to develop security standards as required under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3); and

(D) to support the development of the automation of continuous monitoring systems.

SEC. 504. IDENTITY MANAGEMENT RESEARCH AND DEVELOPMENT.

The Director shall continue a program to support the development of voluntary and cost-effective technical standards, metrology, testbeds, and conformance criteria, taking into account appropriate user concerns—

(1) to improve interoperability among identity management technologies;

(2) to strengthen authentication methods of identity management systems;

(3) to improve privacy protection in identity management systems, including health information technology systems, through authentication and security protocols; and

(4) to improve the usability of identity management systems.

Speaker of the House of Representatives.

Vice President of the United States and President of the Senate.