

Calendar No. 490

113TH CONGRESS
2D SESSION

S. 1353

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

JULY 24, 2013

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

JULY 24, 2014

Reported by Mr. ROCKEFELLER, with an amendment

[Strike out all after the enacting clause and insert the part printed in *italic*]

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.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

1 **SECTION 1. SHORT TITLE; TABLE OF CONTENTS.**

2 (a) **SHORT TITLE.**—This Act may be cited as the
3 “Cybersecurity Act of 2013”.

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

Sec. 1. Short title; table of contents.

Sec. 2. Definitions.

Sec. 3. No regulatory authority.

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.

TITLE III—EDUCATION AND WORKFORCE DEVELOPMENT

Sec. 301. Cybersecurity competitions and challenges.

Sec. 302. Federal cyber scholarship-for-service program.

Sec. 303. Study and analysis of education, accreditation, training, and certification of information infrastructure and cybersecurity professionals.

TITLE IV—CYBERSECURITY AWARENESS AND PREPAREDNESS

Sec. 401. National cybersecurity awareness and preparedness campaign.

6 **SEC. 2. DEFINITIONS.**

7 In this Act:

8 (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,

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

3 ~~(2)~~ INFORMATION INFRASTRUCTURE.—The
 4 term “information infrastructure” means the under-
 5 lying framework that information systems and assets
 6 rely on to process, transmit, receive, or store infor-
 7 mation electronically, including programmable elec-
 8 tronic devices, communications networks, and indus-
 9 trial or supervisory control systems and any associ-
 10 ated hardware, software, or data.

11 ~~(3)~~ INFORMATION SYSTEM.—The term “infor-
 12 mation system” has the meaning given that term in
 13 section 3502 of title 44, United States Code.

14 **SEC. 3. NO REGULATORY AUTHORITY.**

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

18 **TITLE I—PUBLIC-PRIVATE COL-**
 19 **LABORATION ON CYBERSECU-**
 20 **RITY**

21 **SEC. 101. PUBLIC-PRIVATE COLLABORATION ON CYBERSE-**
 22 **CURITY.**

23 ~~(a)~~ CYBERSECURITY.—Section 2(e) of the National
 24 Institute of Standards and Technology Act (15 U.S.C.
 25 272(e)) is amended—

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

4 (2) by inserting after paragraph (14) the fol-
5 lowing:

6 “(15) on an ongoing basis, facilitate and sup-
7 port the development of a voluntary, industry-led set
8 of standards, guidelines, best practices, methodolo-
9 gies, procedures, and processes to reduce cyber risks
10 to critical infrastructure (as defined under sub-
11 section (e));”.

12 (b) SCOPE AND LIMITATIONS.—Section 2 of the Na-
13 tional Institute of Standards and Technology Act (15
14 U.S.C. 272) is amended by adding at the end the fol-
15 lowing:

16 “(e) CYBER RISKS.—

17 “(1) IN GENERAL.—In carrying out the activi-
18 ties under subsection (e)(15), the Director—

19 “(A) shall—

20 “(i) coordinate closely and continu-
21 ously with relevant private sector personnel
22 and entities, critical infrastructure owners
23 and operators, sector coordinating councils,
24 Information Sharing and Analysis Centers,

1 and other relevant industry organizations,
2 and incorporate industry expertise;

3 “(ii) consult with the heads of agen-
4 cies with national security responsibilities,
5 sector-specific agencies, State and local
6 governments, the governments of other na-
7 tions, and international organizations;

8 “(iii) identify a prioritized, flexible, re-
9 peatable, performance-based, and cost-ef-
10 fective approach, including information se-
11 curity measures and controls, that may be
12 voluntarily adopted by owners and opera-
13 tors of critical infrastructure to help them
14 identify, assess, and manage cyber risks;

15 “(iv) include methodologies—

16 “(I) to identify and mitigate im-
17 pacts of the cybersecurity measures or
18 controls on business confidentiality;
19 and

20 “(II) to protect individual privacy
21 and civil liberties;

22 “(v) incorporate voluntary consensus
23 standards and industry best practices;

1 “(vi) align with voluntary inter-
2 national standards to the fullest extent
3 possible;

4 “(vii) prevent duplication of regu-
5 latory processes and prevent conflict with
6 or superseding of regulatory requirements,
7 mandatory standards, and related proc-
8 esses; and

9 “(viii) include such other similar and
10 consistent elements as the Director con-
11 siders necessary; and

12 “(B) shall not prescribe or otherwise re-
13 quire—

14 “(i) the use of specific solutions;

15 “(ii) the use of specific information or
16 communications technology products or
17 services; or

18 “(iii) that information or communica-
19 tions technology products or services be de-
20 signed, developed, or manufactured in a
21 particular manner.

22 “(2) LIMITATION.—Information shared with or
23 provided to the Institute for the purpose of the ac-
24 tivities described under subsection (c)(15) shall not
25 be used by any Federal, State, tribal, or local de-

1 partment or agency to regulate the activity of any
2 entity.

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

4 “(A) CRITICAL INFRASTRUCTURE.—The
5 term ‘critical infrastructure’ has the meaning
6 given the term in section 1016(e) of the USA
7 PATRIOT Act of 2001 (42 U.S.C. 5195e(e)).

8 “(B) SECTOR-SPECIFIC AGENCY.—The
9 term ‘sector-specific agency’ means the Federal
10 department or agency responsible for providing
11 institutional knowledge and specialized expertise
12 as well as leading, facilitating, or supporting
13 the security and resilience programs and associ-
14 ated activities of its designated critical infra-
15 structure sector in the all-hazards environ-
16 ment.”.

17 **TITLE II—CYBERSECURITY**
18 **RESEARCH AND DEVELOPMENT**

19 **SEC. 201. FEDERAL CYBERSECURITY RESEARCH AND DE-**
20 **VELOPMENT.**

21 (a) FUNDAMENTAL CYBERSECURITY RESEARCH.—

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

1 enactment of this Act to develop a Federal cyberse-
2 curity research and development plan to meet objec-
3 tives in cybersecurity, such as—

4 (A) how to design and build complex soft-
5 ware-intensive systems that are secure and reli-
6 able when first deployed;

7 (B) how to test and verify that software
8 and hardware, whether developed locally or ob-
9 tained from a third party, is free of significant
10 known security flaws;

11 (C) how to test and verify that software
12 and hardware obtained from a third party cor-
13 rectly implements stated functionality, and only
14 that functionality;

15 (D) how to guarantee the privacy of an in-
16 dividual, including that individual's identity, in-
17 formation, and lawful transactions when stored
18 in distributed systems or transmitted over net-
19 works;

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

23 (F) how to determine the origin of a mes-
24 sage transmitted over the Internet;

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

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

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

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

11 (K) any additional objectives the Director
12 of the Office of Science and Technology Policy,
13 in coordination with the head of any relevant
14 Federal agency and with input from stake-
15 holders, including industry and academia, deter-
16 mines appropriate.

17 (2) REQUIREMENTS.—

18 (A) IN GENERAL.—The Federal cybersecu-
19 rity research and development plan shall iden-
20 tify and prioritize near-term, mid-term, and
21 long-term research in computer and information
22 science and engineering to meet the objectives
23 under paragraph (1), including research in the
24 areas described in section 4(a)(1) of the Cyber

1 Security Research and Development Act (15
2 U.S.C. 7403(a)(1)).

3 (B) PRIVATE SECTOR EFFORTS.—In devel-
4 oping, implementing, and updating the Federal
5 cybersecurity research and development plan,
6 the Director of the Office of Science and Tech-
7 nology Policy shall work in close cooperation
8 with industry, academia, and other interested
9 stakeholders to ensure, to the extent possible,
10 that Federal cybersecurity research and devel-
11 opment is not duplicative of private sector ef-
12 forts.

13 (3) TRIENNIAL UPDATES.—

14 (A) IN GENERAL.—The Federal cybersecu-
15 rity research and development plan shall be up-
16 dated triennially.

17 (B) REPORT TO CONGRESS.—The Director
18 of the Office of Science and Technology Policy
19 shall submit the plan, not later than 1 year
20 after the date of enactment of this Act, and
21 each updated plan under this section to the
22 Committee on Commerce, Science, and Trans-
23 portation of the Senate and the Committee on
24 Science, Space, and Technology of the House of
25 Representatives.

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

4 (1) develops, evaluates, disseminates, and inte-
5 grates new cybersecurity practices and concepts into
6 the core curriculum of computer science programs
7 and of other programs where graduates of such pro-
8 grams have a substantial probability of developing
9 software after graduation, including new practices
10 and concepts relating to secure coding education and
11 improvement programs; and

12 (2) develops new models for professional devel-
13 opment of faculty in cybersecurity education, includ-
14 ing secure coding development.

15 (c) **CYBERSECURITY MODELING AND TEST BEDS.**—

16 (1) **REVIEW.**—Not later than 1 year after the
17 date of enactment of this Act, the Director the Na-
18 tional Science Foundation, in coordination with the
19 Director of the Office of Science and Technology
20 Policy, shall conduct a review of cybersecurity test
21 beds in existence on the date of enactment of this
22 Act to inform the grants under paragraph (2). The
23 review shall include an assessment of whether a suf-
24 ficient number of cybersecurity test beds are avail-

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

3 ~~(2)~~ ~~ADDITIONAL CYBERSECURITY MODELING~~
4 ~~AND TEST BEDS.—~~

5 (A) ~~IN GENERAL.—~~If the Director of the
6 National Science Foundation, after the review
7 under paragraph (1), determines that the re-
8 search needs under the Federal cybersecurity
9 research and development plan require the es-
10 tablishment of additional cybersecurity test
11 beds, the Director of the National Science
12 Foundation, in coordination with the Secretary
13 of Commerce and the Secretary of Homeland
14 Security, may award grants to institutions of
15 higher education or research and development
16 non-profit institutions to establish cybersecurity
17 test beds.

18 (B) ~~REQUIREMENT.—~~The cybersecurity
19 test beds under subparagraph (A) shall be suffi-
20 ciently large in order to model the scale and
21 complexity of real-time cyber attacks and de-
22 fenses on real world networks and environ-
23 ments.

24 (C) ~~ASSESSMENT REQUIRED.—~~The Direc-
25 tor of the National Science Foundation, in co-

1 ordination with the Secretary of Commerce and
2 the Secretary of Homeland Security, shall
3 evaluate the effectiveness of any grants award-
4 ed under this subsection in meeting the objec-
5 tives of the Federal cybersecurity research and
6 development plan under subsection (a) no later
7 than 2 years after the review under paragraph
8 (1) of this subsection, and periodically there-
9 after.

10 (d) **COORDINATION WITH OTHER RESEARCH INITIA-**
11 **TIVES.**—In accordance with the responsibilities under sec-
12 tion 101 of the High-Performance Computing Act of 1991
13 (15 U.S.C. 5511), the Director the Office of Science and
14 Technology Policy shall coordinate, to the extent prac-
15 ticable, Federal research and development activities under
16 this section with other ongoing research and development
17 security-related initiatives, including research being con-
18 ducted by—

19 (1) the National Science Foundation;

20 (2) the National Institute of Standards and
21 Technology;

22 (3) the Department of Homeland Security;

23 (4) other Federal agencies;

24 (5) other Federal and private research labora-
25 tories, research entities, and universities;

- 1 (6) institutions of higher education;
2 (7) relevant nonprofit organizations; and
3 (8) international partners of the United States.

4 (e) NATIONAL SCIENCE FOUNDATION COMPUTER
5 AND NETWORK SECURITY RESEARCH GRANT AREAS.—

6 Section 4(a)(1) of the Cyber Security Research and Devel-
7 opment Act (15 U.S.C. 7403(a)(1)) is amended—

8 (1) in subparagraph (H), by striking “and” at
9 the end;

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

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

13 “(J) secure fundamental protocols that are
14 integral to inter-network communications and
15 data exchange;

16 “(K) secure software engineering and soft-
17 ware assurance, including—

18 “(i) programming languages and sys-
19 tems that include fundamental security
20 features;

21 “(ii) portable or reusable code that re-
22 mains secure when deployed in various en-
23 vironments;

1 “(iii) verification and validation tech-
2 nologies to ensure that requirements and
3 specifications have been implemented; and

4 “(iv) models for comparison and
5 metrics to assure that required standards
6 have been met;

7 “(L) holistic system security that—

8 “(i) addresses the building of secure
9 systems from trusted and untrusted com-
10 ponents;

11 “(ii) proactively reduces
12 vulnerabilities;

13 “(iii) addresses insider threats; and

14 “(iv) supports privacy in conjunction
15 with improved security;

16 “(M) monitoring and detection;

17 “(N) mitigation and rapid recovery meth-
18 ods;

19 “(O) security of wireless networks and mo-
20 bile devices; and

21 “(P) security of cloud infrastructure and
22 services.”.

23 (f) RESEARCH ON THE SCIENCE OF CYBERSECU-
24 RITY.—The head of each agency and department identi-
25 fied under section 101(a)(3)(B) of the High-Performance

1 Computing Act of 1991 (15 U.S.C. 5511(a)(3)(B)),
 2 through existing programs and activities, shall support re-
 3 search that will lead to the development of a scientific
 4 foundation for the field of cybersecurity, including re-
 5 search that increases understanding of the underlying
 6 principles of securing complex networked systems, enables
 7 repeatable experimentation, and creates quantifiable secu-
 8 rity metrics.

9 **SEC. 202. COMPUTER AND NETWORK SECURITY RESEARCH**
 10 **CENTERS.**

11 Section 4(b) of the Cyber Security Research and De-
 12 velopment Act (15 U.S.C. 7403(b)) is amended—

13 (1) by striking “the center” in paragraph
 14 (4)(D) and inserting “the Center”; and

15 (2) in paragraph (5)—

16 (A) by striking “and” at the end of sub-
 17 paragraph (C);

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

21 (C) by adding at the end the following:

22 “(E) the demonstrated capability of the
 23 applicant to conduct high performance com-
 24 putation integral to complex computer and net-

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

3 “(F) the applicant’s affiliation with private
4 sector entities involved with industrial research
5 described in subsection (a)(1);

6 “(G) the capability of the applicant to con-
7 duct research in a secure environment;

8 “(H) the applicant’s affiliation with exist-
9 ing research programs of the Federal Govern-
10 ment;

11 “(I) the applicant’s experience managing
12 public-private partnerships to transition new
13 technologies into a commercial setting or the
14 government user community; and

15 “(J) the capability of the applicant to con-
16 duct interdisciplinary cybersecurity research,
17 such as in law, economics, or behavioral
18 sciences.”.

19 **TITLE III—EDUCATION AND**
20 **WORKFORCE DEVELOPMENT**

21 **SEC. 301. CYBERSECURITY COMPETITIONS AND CHAL-**
22 **LENGES.**

23 (a) IN GENERAL.—The Secretary of Commerce, Di-
24 rector of the National Science Foundation, and Secretary
25 of Homeland Security shall—

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

5 (A) to identify, develop, and recruit tal-
6 ented individuals to perform duties relating to
7 the security of information infrastructure in
8 Federal, State, and local government agencies,
9 and the private sector; or

10 (B) to stimulate innovation in basic and
11 applied cybersecurity research, technology devel-
12 opment, and prototype demonstration that has
13 the potential for application to the information
14 technology activities of the Federal Govern-
15 ment; and

16 (2) ensure the effective operation of the com-
17 petitions and challenges under this section.

18 (b) PARTICIPATION.—Participants in the competi-
19 tions and challenges under subsection (a)(1) may in-
20 clude—

21 (1) students enrolled in grades 9 through 12;

22 (2) students enrolled in a postsecondary pro-
23 gram of study leading to a baccalaureate degree at
24 an institution of higher education;

1 (3) students enrolled in a postbaccalaureate
2 program of study at an institution of higher edu-
3 cation;

4 (4) institutions of higher education and re-
5 search institutions;

6 (5) veterans; and

7 (6) other groups or individuals that the Sec-
8 retary of Commerce, Director of the National
9 Science Foundation, and Secretary of Homeland Se-
10 curity determine appropriate.

11 (e) AFFILIATION AND COOPERATIVE AGREE-
12 MENTS.—Competitions and challenges under this section
13 may be carried out through affiliation and cooperative
14 agreements with—

15 (1) Federal agencies;

16 (2) regional, State, or school programs sup-
17 porting the development of cyber professionals;

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

19 (4) other private sector organizations.

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

23 (1) ethical hacking;

24 (2) penetration testing;

25 (3) vulnerability assessment;

- 1 (4) continuity of system operations;
 2 (5) security in design;
 3 (6) cyber forensics;
 4 (7) offensive and defensive cyber operations;
 5 and
 6 (8) other areas the Secretary of Commerce, Di-
 7 rector of the National Science Foundation, and Sec-
 8 retary of Homeland Security consider necessary to
 9 fulfill the cybersecurity mission.

10 (e) TOPICS.—In selecting topics for competitions and
 11 challenges under subsection (a)(1), the Secretary of Com-
 12 merce, Director of the National Science Foundation, and
 13 Secretary of Homeland Security—

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

16 (2) may empanel advisory committees.

17 (f) INTERNSHIPS.—The Director of the Office of Per-
 18 sonnel Management may support, as appropriate, intern-
 19 ships or other work experience in the Federal Government
 20 to the winners of the competitions and challenges under
 21 this section.

22 **SEC. 302. FEDERAL CYBER SCHOLARSHIP-FOR-SERVICE**
 23 **PROGRAM.**

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

1 the Office of Personnel Management and Secretary of
2 Homeland Security, shall continue a Federal Cyber Schol-
3 arship-for-Service program to recruit and train the next
4 generation of information technology professionals, indus-
5 trial control system security professionals, and security
6 managers to meet the needs of the cybersecurity mission
7 for Federal, State, local, and tribal governments.

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

11 (1) provide scholarships to students who are en-
12 rolled in programs of study at institutions of higher
13 education leading to degrees or specialized program
14 certifications in the cybersecurity field;

15 (2) provide the scholarship recipients with sum-
16 mer internship opportunities or other meaningful
17 temporary appointments in the Federal information
18 technology workforce; and

19 (3) provide a procedure by which the National
20 Science Foundation or a Federal agency, consistent
21 with regulations of the Office of Personnel Manage-
22 ment, may request and fund security clearances for
23 scholarship recipients, including providing for clear-
24 ances during internships or other temporary ap-
25 pointments and after receipt of their degrees.

1 (c) SCHOLARSHIP AMOUNTS.—Each scholarship
2 under subsection (b) shall be in an amount that covers
3 the student’s tuition and fees at the institution under sub-
4 section (b)(1) and provides the student with an additional
5 stipend.

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

13 (e) HIRING AUTHORITY.—

14 (1) APPOINTMENT IN EXCEPTED SERVICE.—
15 Notwithstanding any provision of chapter 33 of title
16 5, United States Code, governing appointments in
17 the competitive service, an agency shall appoint in
18 the excepted service an individual who has completed
19 the academic program for which a scholarship was
20 awarded.

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

1 (3) ~~TIMING OF CONVERSION.~~—An agency may
 2 noncompetitively convert a term employee appointed
 3 under paragraph (2) to a career-conditional or ca-
 4 reer appointment before the term appointment ex-
 5 pires.

6 (4) ~~AUTHORITY TO DECLINE CONVERSION.~~—An
 7 agency may decline to make the noncompetitive con-
 8 version or appointment under paragraph (2) for
 9 cause.

10 (f) ~~ELIGIBILITY.~~—To be eligible to receive a scholar-
 11 ship under this section, an individual shall—

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

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

17 (3) have demonstrated a high level of pro-
 18 ficiency in mathematics, engineering, or computer
 19 sciences.

20 (g) ~~REPAYMENT.~~—If a scholarship recipient does not
 21 meet the terms of the program under this section, the re-
 22 cipient shall refund the scholarship payments in accord-
 23 ance with rules established by the Director of the National
 24 Science Foundation, in coordination with the Director of

1 the Office of Personnel Management and Secretary of
2 Homeland Security.

3 (h) **EVALUATION AND REPORT.**—The Director of the
4 National Science Foundation shall evaluate and report pe-
5 riodically to Congress on the success of recruiting individ-
6 uals for scholarships under this section and on hiring and
7 retaining those individuals in the public sector workforce.

8 **SEC. 303. STUDY AND ANALYSIS OF EDUCATION, ACCREDI-**
9 **TATION, TRAINING, AND CERTIFICATION OF**
10 **INFORMATION INFRASTRUCTURE AND CY-**
11 **BERSECURITY PROFESSIONALS.**

12 (a) **STUDY.**—The Director of the National Science
13 Foundation and the Secretary of Homeland Security shall
14 undertake to enter into appropriate arrangements with the
15 National Academy of Sciences to conduct a comprehensive
16 study of government, academic, and private-sector edu-
17 cation, accreditation, training, and certification programs
18 for the development of professionals in information infra-
19 structure and cybersecurity. The agreement shall require
20 the National Academy of Sciences to consult with sector
21 coordinating councils and relevant governmental agencies,
22 regulatory entities, and nongovernmental organizations in
23 the course of the study.

24 (b) **SCOPE.**—The study shall include—

1 (1) an evaluation of the body of knowledge and
2 various skills that specific categories of professionals
3 in information infrastructure and cybersecurity
4 should possess in order to secure information sys-
5 tems;

6 (2) an assessment of whether existing govern-
7 ment, academic, and private-sector education, ac-
8 creditation, training, and certification programs pro-
9 vide the body of knowledge and various skills de-
10 scribed in paragraph (1);

11 (3) an evaluation of—

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

15 (B) the extent of professional development
16 opportunities for faculty in cybersecurity prin-
17 ciples and practices;

18 (C) the extent of the partnerships and col-
19 laborative cybersecurity curriculum development
20 activities that leverage industry and government
21 needs, resources, and tools;

22 (D) the proposed metrics to assess
23 progress toward improving cybersecurity edu-
24 cation; and

1 (~~E~~) the descriptions of the content of cy-
2 bersecurity courses in undergraduate computer
3 science curriculum;

4 (4) an analysis of any barriers to the Federal
5 Government recruiting and hiring cybersecurity tal-
6 ent, including barriers relating to compensation, the
7 hiring process, job classification, and hiring flexi-
8 bility; and

9 (5) an analysis of the sources and availability of
10 cybersecurity talent, a comparison of the skills and
11 expertise sought by the Federal Government and the
12 private sector, an examination of the current and fu-
13 ture capacity of United States institutions of higher
14 education, including community colleges, to provide
15 current and future cybersecurity professionals,
16 through education and training activities, with those
17 skills sought by the Federal Government, State and
18 local entities, and the private sector.

19 (~~e~~) REPORT.—Not later than 1 year after the date
20 of enactment of this Act, the National Academy of
21 Sciences shall submit to the President and Congress a re-
22 port on the results of the study. The report shall include—

23 (1) findings regarding the state of information
24 infrastructure and cybersecurity education, accredi-
25 tation, training, and certification programs, includ-

1 ing specific areas of deficiency and demonstrable
2 progress; and

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

7 **TITLE IV—CYBERSECURITY**
8 **AWARENESS AND PREPARED-**
9 **NESS**

10 **SEC. 401. NATIONAL CYBERSECURITY AWARENESS AND**
11 **PREPAREDNESS CAMPAIGN.**

12 (a) NATIONAL CYBERSECURITY AWARENESS AND
13 PREPAREDNESS CAMPAIGN.—The Director of the Na-
14 tional Institute of Standards and Technology (referred to
15 in this section as the “Director”), in consultation with ap-
16 propriate Federal agencies, shall continue to coordinate a
17 national cybersecurity awareness and preparedness cam-
18 paign, such as—

19 (1) a campaign to increase public awareness of
20 cybersecurity, cyber safety, and cyber ethics, includ-
21 ing the use of the Internet, social media, entertain-
22 ment, and other media to reach the public;

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

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

4 (B) the methods to mitigate and remediate
5 vulnerabilities;

6 (3) support for formal cybersecurity education
7 programs at all education levels to prepare skilled
8 cybersecurity and computer science workers for the
9 private sector and Federal, State, and local govern-
10 ment; and

11 (4) initiatives to evaluate and forecast future
12 cybersecurity workforce needs of the Federal govern-
13 ment and develop strategies for recruitment, train-
14 ing, and retention.

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

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

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

4 (d) REPORT.—Not later than 1 year after the date
 5 of enactment of this Act, and every 5 years thereafter,
 6 the Director shall transmit the strategic plan under sub-
 7 section (c) to the Committee on Commerce, Science, and
 8 Transportation of the Senate and the Committee on
 9 Science, Space, and Technology of the House of Rep-
 10 resentatives.

11 **SECTION 1. SHORT TITLE; TABLE OF CONTENTS.**

12 (a) SHORT TITLE.—*This Act may be cited as the “Cy-*
 13 *bersecurity Act of 2013”.*

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

Sec. 1. Short title; table of contents.

Sec. 2. Definitions.

Sec. 3. No regulatory authority.

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.

TITLE III—EDUCATION AND WORKFORCE DEVELOPMENT

Sec. 301. Cybersecurity competitions and challenges.

Sec. 302. Federal cyber scholarship-for-service program.

*Sec. 303. Study and analysis of education, accreditation, training, and certifi-
 cation of information infrastructure and cybersecurity profes-
 sionals.*

TITLE IV—CYBERSECURITY AWARENESS AND PREPAREDNESS

Sec. 401. National cybersecurity awareness and preparedness campaign.

1 **SEC. 2. DEFINITIONS.**

2 *In this Act:*

3 (1) *CYBERSECURITY MISSION.*—*The term “cyber-*
4 *security mission” means activities that encompass the*
5 *full range of threat reduction, vulnerability reduction,*
6 *deterrence, international engagement, incident re-*
7 *sponse, resiliency, and recovery policies and activi-*
8 *ties, including computer network operations, informa-*
9 *tion assurance, law enforcement, diplomacy, military,*
10 *and intelligence missions as such activities relate to*
11 *the security and stability of cyberspace.*

12 (2) *INFORMATION INFRASTRUCTURE.*—*The term*
13 *“information infrastructure” means the underlying*
14 *framework that information systems and assets rely*
15 *on to process, transmit, receive, or store information*
16 *electronically, including programmable electronic de-*
17 *vices, communications networks, and industrial or su-*
18 *pervisory control systems and any associated hard-*
19 *ware, software, or data.*

20 (3) *INFORMATION SYSTEM.*—*The term “informa-*
21 *tion system” has the meaning given that term in sec-*
22 *tion 3502 of title 44, United States Code.*

23 **SEC. 3. NO REGULATORY AUTHORITY.**

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

1 **TITLE I—PUBLIC-PRIVATE COL-**
 2 **LABORATION ON CYBERSECU-**
 3 **RITY**

4 **SEC. 101. PUBLIC-PRIVATE COLLABORATION ON CYBERSE-**
 5 **CURITY.**

6 (a) *CYBERSECURITY.*—Section 2(c) of the National In-
 7 stitute of Standards and Technology Act (15 U.S.C. 272(c))
 8 is amended—

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

12 (2) *by inserting after paragraph (14) the fol-*
 13 *lowing:*

14 “(15) *on an ongoing basis, facilitate and support*
 15 *the development of a voluntary, industry-led set of*
 16 *standards, guidelines, best practices, methodologies,*
 17 *procedures, and processes to reduce cyber risks to crit-*
 18 *ical infrastructure (as defined under subsection (e));”.*

19 (b) *SCOPE AND LIMITATIONS.*—Section 2 of the Na-
 20 tional Institute of Standards and Technology Act (15
 21 U.S.C. 272) is amended by adding at the end the following:

22 “(e) *CYBER RISKS.*—

23 “(1) *IN GENERAL.*—*In carrying out the activities*
 24 *under subsection (c)(15), the Director—*

25 “(A) *shall—*

1 “(i) coordinate closely and continu-
2 ously with relevant private sector personnel
3 and entities, critical infrastructure owners
4 and operators, sector coordinating councils,
5 Information Sharing and Analysis Centers,
6 and other relevant industry organizations,
7 and incorporate industry expertise;

8 “(ii) consult with the heads of agencies
9 with national security responsibilities, sec-
10 tor-specific agencies, State and local govern-
11 ments, the governments of other nations,
12 and international organizations;

13 “(iii) identify a prioritized, flexible,
14 repeatable, performance-based, and cost-ef-
15 fective approach, including information se-
16 curity measures and controls, that may be
17 voluntarily adopted by owners and opera-
18 tors of critical infrastructure to help them
19 identify, assess, and manage cyber risks;

20 “(iv) include methodologies—

21 “(I) to identify and mitigate im-
22 pacts of the cybersecurity measures or
23 controls on business confidentiality;
24 and

1 “(II) to protect individual pri-
2 vacy and civil liberties;

3 “(v) incorporate voluntary consensus
4 standards and industry best practices;

5 “(vi) align with voluntary inter-
6 national standards to the fullest extent pos-
7 sible;

8 “(vii) prevent duplication of regulatory
9 processes and prevent conflict with or super-
10 seding of regulatory requirements, manda-
11 tory standards, and related processes; and

12 “(viii) include such other similar and
13 consistent elements as the Director considers
14 necessary; and

15 “(B) shall not prescribe or otherwise re-
16 quire—

17 “(i) the use of specific solutions;

18 “(ii) the use of specific information or
19 communications technology products or
20 services; or

21 “(iii) that information or communica-
22 tions technology products or services be de-
23 signed, developed, or manufactured in a
24 particular manner.

1 “(2) *LIMITATION.*—*Information shared with or*
2 *provided to the Institute for the purpose of the activi-*
3 *ties described under subsection (c)(15) shall not be*
4 *used by any Federal, State, tribal, or local depart-*
5 *ment or agency to regulate the activity of any entity.*

6 “(3) *DEFINITIONS.*—*In this subsection:*

7 “(A) *CRITICAL INFRASTRUCTURE.*—*The*
8 *term ‘critical infrastructure’ has the meaning*
9 *given the term in section 1016(e) of the USA*
10 *PATRIOT Act of 2001 (42 U.S.C. 5195c(e)).*

11 “(B) *SECTOR-SPECIFIC AGENCY.*—*The term*
12 *‘sector-specific agency’ means the Federal depart-*
13 *ment or agency responsible for providing institu-*
14 *tional knowledge and specialized expertise as*
15 *well as leading, facilitating, or supporting the*
16 *security and resilience programs and associated*
17 *activities of its designated critical infrastructure*
18 *sector in the all-hazards environment.”.*

19 “(c) *STUDY AND REPORT.*—

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

22 “(A) *the progress made by the Director of the*
23 *National Institute of Standards and Technology*
24 *in facilitating the development of standards and*
25 *procedures to reduce cyber risks to critical infra-*

1 *structure in accordance with section 2(c)(15) of*
2 *the National Institute of Standards and Tech-*
3 *nology Act, as added by this section;*

4 *(B) the extent to which the Director's facili-*
5 *tation efforts are consistent with the directive in*
6 *such section that the development of such stand-*
7 *ards and procedures be voluntary and led by in-*
8 *dustry representatives;*

9 *(C) the extent to which sectors of critical in-*
10 *frastructure (as defined in section 1016(e) of the*
11 *USA PATRIOT Act of 2001 (42 U.S.C.*
12 *5195c(e))) have adopted a voluntary, industry-*
13 *led set of standards, guidelines, best practices,*
14 *methodologies, procedures, and processes to re-*
15 *duce cyber risks to critical infrastructure in ac-*
16 *cordance with such section 2(c)(15);*

17 *(D) the reasons behind the decisions of sec-*
18 *tors of critical infrastructure (as defined in sub-*
19 *paragraph (C)) to adopt or to not adopt the vol-*
20 *untary standards described in subparagraph (C);*
21 *and*

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

1 (2) *REPORTS.*—Not later than 1 year after the
 2 date of the enactment of this Act, and every 2 years
 3 thereafter for the following 6 years, the Comptroller
 4 General shall submit a report, which summarizes the
 5 findings of the study conducted under paragraph (1),
 6 to—

7 (A) the Committee on Commerce, Science,
 8 and Transportation of the Senate;

9 (B) the Committee on Energy and Com-
 10 merce of the House of Representatives; and

11 (C) the Committee on Science, Space, and
 12 Technology of the House of Representatives.

13 **TITLE II—CYBERSECURITY**
 14 **RESEARCH AND DEVELOPMENT**

15 **SEC. 201. FEDERAL CYBERSECURITY RESEARCH AND DE-**
 16 **VELOPMENT.**

17 (a) *FUNDAMENTAL CYBERSECURITY RESEARCH.*—

18 (1) *IN GENERAL.*—The Director of the Office of
 19 Science and Technology Policy, in coordination with
 20 the head of any relevant Federal agency, shall build
 21 upon programs and plans in effect as of the date of
 22 enactment of this Act to develop a Federal cybersecu-
 23 rity research and development plan to meet objectives
 24 in cybersecurity, such as—

1 (A) *how to design and build complex soft-*
2 *ware-intensive systems that are secure and reli-*
3 *able when first deployed;*

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

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

12 (D) *how to guarantee the privacy of an in-*
13 *dividual, including that individual's identity,*
14 *information, and lawful transactions when*
15 *stored in distributed systems or transmitted over*
16 *networks;*

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

20 (F) *how to determine the origin of a mes-*
21 *sage transmitted over the Internet;*

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

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

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

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

7 (K) *any additional objectives the Director of*
8 *the Office of Science and Technology Policy, in*
9 *coordination with the head of any relevant Fed-*
10 *eral agency and with input from stakeholders,*
11 *including appropriate national laboratories, in-*
12 *dustry, and academia, determines appropriate.*

13 (2) *REQUIREMENTS.—*

14 (A) *IN GENERAL.—The Federal cybersecu-*
15 *rity research and development plan shall iden-*
16 *tify and prioritize near-term, mid-term, and*
17 *long-term research in computer and information*
18 *science and engineering to meet the objectives*
19 *under paragraph (1), including research in the*
20 *areas described in section 4(a)(1) of the Cyber*
21 *Security Research and Development Act (15*
22 *U.S.C. 7403(a)(1)).*

23 (B) *PRIVATE SECTOR EFFORTS.—In devel-*
24 *oping, implementing, and updating the Federal*
25 *cybersecurity research and development plan, the*

1 *Director of the Office of Science and Technology*
2 *Policy shall work in close cooperation with in-*
3 *dustry, academia, and other interested stake-*
4 *holders to ensure, to the extent possible, that Fed-*
5 *eral cybersecurity research and development is*
6 *not duplicative of private sector efforts.*

7 (3) *TRIENNIAL UPDATES.*—

8 (A) *IN GENERAL.*—*The Federal cybersecu-*
9 *rity research and development plan shall be up-*
10 *dated triennially.*

11 (B) *REPORT TO CONGRESS.*—*The Director*
12 *of the Office of Science and Technology Policy*
13 *shall submit the plan, not later than 1 year after*
14 *the date of enactment of this Act, and each up-*
15 *dated plan under this section to the Committee*
16 *on Commerce, Science, and Transportation of*
17 *the Senate and the Committee on Science, Space,*
18 *and Technology of the House of Representatives.*

19 (b) *CYBERSECURITY PRACTICES RESEARCH.*—*The Di-*
20 *rector of the National Science Foundation shall support re-*
21 *search that—*

22 (1) *develops, evaluates, disseminates, and inte-*
23 *grates new cybersecurity practices and concepts into*
24 *the core curriculum of computer science programs and*
25 *of other programs where graduates of such programs*

1 *have a substantial probability of developing software*
2 *after graduation, including new practices and con-*
3 *cepts relating to secure coding education and im-*
4 *provement programs; and*

5 *(2) develops new models for professional develop-*
6 *ment of faculty in cybersecurity education, including*
7 *secure coding development.*

8 *(c) CYBERSECURITY MODELING AND TEST BEDS.—*

9 *(1) REVIEW.—Not later than 1 year after the*
10 *date of enactment of this Act, the Director the Na-*
11 *tional Science Foundation, in coordination with the*
12 *Director of the Office of Science and Technology Pol-*
13 *icy, shall conduct a review of cybersecurity test beds*
14 *in existence on the date of enactment of this Act to*
15 *inform the grants under paragraph (2). The review*
16 *shall include an assessment of whether a sufficient*
17 *number of cybersecurity test beds are available to*
18 *meet the research needs under the Federal cybersecu-*
19 *rity research and development plan.*

20 *(2) ADDITIONAL CYBERSECURITY MODELING AND*
21 *TEST BEDS.—*

22 *(A) IN GENERAL.—If the Director of the*
23 *National Science Foundation, after the review*
24 *under paragraph (1), determines that the re-*
25 *search needs under the Federal cybersecurity re-*

1 search and development plan require the estab-
2 lishment of additional cybersecurity test beds, the
3 Director of the National Science Foundation, in
4 coordination with the Secretary of Commerce
5 and the Secretary of Homeland Security, may
6 award grants to institutions of higher education
7 or research and development non-profit institu-
8 tions to establish cybersecurity test beds.

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

14 (C) ASSESSMENT REQUIRED.—The Director
15 of the National Science Foundation, in coordina-
16 tion with the Secretary of Commerce and the
17 Secretary of Homeland Security, shall evaluate
18 the effectiveness of any grants awarded under
19 this subsection in meeting the objectives of the
20 Federal cybersecurity research and development
21 plan under subsection (a) no later than 2 years
22 after the review under paragraph (1) of this sub-
23 section, and periodically thereafter.

24 (d) COORDINATION WITH OTHER RESEARCH INITIA-
25 TIVES.—In accordance with the responsibilities under sec-

1 *tion 101 of the High-Performance Computing Act of 1991*
 2 *(15 U.S.C. 5511), the Director the Office of Science and*
 3 *Technology Policy shall coordinate, to the extent prac-*
 4 *ticable, Federal research and development activities under*
 5 *this section with other ongoing research and development*
 6 *security-related initiatives, including research being con-*
 7 *ducted by—*

- 8 (1) *the National Science Foundation;*
 9 (2) *the National Institute of Standards and*
 10 *Technology;*
 11 (3) *the Department of Homeland Security;*
 12 (4) *other Federal agencies;*
 13 (5) *other Federal and private research labora-*
 14 *tories, research entities, and universities;*
 15 (6) *institutions of higher education;*
 16 (7) *relevant nonprofit organizations; and*
 17 (8) *international partners of the United States.*

18 (e) *NATIONAL SCIENCE FOUNDATION COMPUTER AND*
 19 *NETWORK SECURITY RESEARCH GRANT AREAS.—Section*
 20 *4(a)(1) of the Cyber Security Research and Development*
 21 *Act (15 U.S.C. 7403(a)(1)) is amended—*

- 22 (1) *in subparagraph (H), by striking “and” at*
 23 *the end;*
 24 (2) *in subparagraph (I), by striking the period*
 25 *at the end and inserting a semicolon; and*

1 (3) *by adding at the end the following:*

2 “(J) *secure fundamental protocols that are*
3 *integral to inter-network communications and*
4 *data exchange;*

5 “(K) *secure software engineering and soft-*
6 *ware assurance, including—*

7 “(i) *programming languages and sys-*
8 *tems that include fundamental security fea-*
9 *tures;*

10 “(ii) *portable or reusable code that re-*
11 *mains secure when deployed in various en-*
12 *vironments;*

13 “(iii) *verification and validation tech-*
14 *nologies to ensure that requirements and*
15 *specifications have been implemented; and*

16 “(iv) *models for comparison and*
17 *metrics to assure that required standards*
18 *have been met;*

19 “(L) *holistic system security that—*

20 “(i) *addresses the building of secure*
21 *systems from trusted and untrusted compo-*
22 *nents;*

23 “(ii) *proactively reduces*
24 *vulnerabilities;*

25 “(iii) *addresses insider threats; and*

1 “(iv) supports privacy in conjunction
2 with improved security;

3 “(M) monitoring and detection;

4 “(N) mitigation and rapid recovery meth-
5 ods;

6 “(O) security of wireless networks and mo-
7 bile devices; and

8 “(P) security of cloud infrastructure and
9 services.”.

10 (f) *RESEARCH ON THE SCIENCE OF CYBERSECURITY.*—*The head of each agency and department identified*
11 *under section 101(a)(3)(B) of the High-Performance Com-*
12 *puting Act of 1991 (15 U.S.C. 5511(a)(3)(B)), through ex-*
13 *isting programs and activities, shall support research that*
14 *will lead to the development of a scientific foundation for*
15 *the field of cybersecurity, including research that increases*
16 *understanding of the underlying principles of securing com-*
17 *plex networked systems, enables repeatable experimentation,*
18 *and creates quantifiable security metrics.*

20 **SEC. 202. COMPUTER AND NETWORK SECURITY RESEARCH**
21 **CENTERS.**

22 Section 4(b) of the Cyber Security Research and Devel-
23 opment Act (15 U.S.C. 7403(b)) is amended—

24 (1) in paragraph (3), by striking “the research
25 areas” and inserting the following: “improving the se-

1 *curity and resiliency of information infrastructure,*
2 *reducing cyber vulnerabilities, and anticipating and*
3 *mitigating consequences of cyber attacks on critical*
4 *infrastructure, by conducting research in the areas”;*

5 *(2) by striking “the center” in paragraph (4)(D)*
6 *and inserting “the Center”; and*

7 *(3) in paragraph (5)—*

8 *(A) by striking “and” at the end of sub-*
9 *paragraph (C);*

10 *(B) by striking the period at the end of sub-*
11 *paragraph (D) and inserting a semicolon; and*

12 *(C) by adding at the end the following:*

13 *“(E) the demonstrated capability of the ap-*
14 *plicant to conduct high performance computa-*
15 *tion integral to complex computer and network*
16 *security research, through on-site or off-site com-*
17 *puting;*

18 *“(F) the applicant’s affiliation with private*
19 *sector entities involved with industrial research*
20 *described in subsection (a)(1);*

21 *“(G) the capability of the applicant to con-*
22 *duct research in a secure environment;*

23 *“(H) the applicant’s affiliation with exist-*
24 *ing research programs of the Federal Govern-*
25 *ment;*

1 “(I) the applicant’s experience managing
2 public-private partnerships to transition new
3 technologies into a commercial setting or the gov-
4 ernment user community;

5 “(J) the capability of the applicant to con-
6 duct interdisciplinary cybersecurity research,
7 basic and applied, such as in law, economics, or
8 behavioral sciences; and

9 “(K) the capability of the applicant to con-
10 duct research in areas such as systems security,
11 wireless security, networking and protocols, for-
12 mal methods and high-performance computing,
13 nanotechnology, or industrial control systems.”.

14 **TITLE III—EDUCATION AND**
15 **WORKFORCE DEVELOPMENT**

16 **SEC. 301. CYBERSECURITY COMPETITIONS AND CHAL-**
17 **LENGES.**

18 (a) *IN GENERAL.*—The Secretary of Commerce, Direc-
19 tor of the National Science Foundation, and Secretary of
20 Homeland Security, in consultation with the Director of
21 the Office of Personnel Management, shall—

22 (1) support competitions and challenges under
23 section 105 of the America COMPETES Reauthoriza-
24 tion Act of 2010 (124 Stat. 3989) or any other provi-
25 sion of law, as appropriate—

1 (A) to identify, develop, and recruit talented
2 individuals to perform duties relating to the se-
3 curity of information infrastructure in Federal,
4 State, and local government agencies, and the
5 private sector; or

6 (B) to stimulate innovation in basic and
7 applied cybersecurity research, technology devel-
8 opment, and prototype demonstration that has
9 the potential for application to the information
10 technology activities of the Federal Government;
11 and

12 (2) ensure the effective operation of the competi-
13 tions and challenges under this section.

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

16 (1) students enrolled in grades 9 through 12;

17 (2) students enrolled in a postsecondary program
18 of study leading to a baccalaureate degree at an insti-
19 tution of higher education;

20 (3) students enrolled in a postbaccalaureate pro-
21 gram of study at an institution of higher education;

22 (4) institutions of higher education and research
23 institutions;

24 (5) veterans; and

1 (6) *other groups or individuals that the Sec-*
2 *retary of Commerce, Director of the National Science*
3 *Foundation, and Secretary of Homeland Security de-*
4 *termine appropriate.*

5 (c) *AFFILIATION AND COOPERATIVE AGREEMENTS.—*
6 *Competitions and challenges under this section may be car-*
7 *ried out through affiliation and cooperative agreements*
8 *with—*

9 (1) *Federal agencies;*

10 (2) *regional, State, or school programs sup-*
11 *porting the development of cyber professionals;*

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

13 (4) *other private sector organizations.*

14 (d) *AREAS OF SKILL.—Competitions and challenges*
15 *under subsection (a)(1)(A) shall be designed to identify, de-*
16 *velop, and recruit exceptional talent relating to—*

17 (1) *ethical hacking;*

18 (2) *penetration testing;*

19 (3) *vulnerability assessment;*

20 (4) *continuity of system operations;*

21 (5) *security in design;*

22 (6) *cyber forensics;*

23 (7) *offensive and defensive cyber operations; and*

24 (8) *other areas the Secretary of Commerce, Di-*
25 *rector of the National Science Foundation, and Sec-*

1 *retary of Homeland Security consider necessary to*
2 *fulfill the cybersecurity mission.*

3 *(e) TOPICS.—In selecting topics for competitions and*
4 *challenges under subsection (a)(1), the Secretary of Com-*
5 *merce, Director of the National Science Foundation, and*
6 *Secretary of Homeland Security—*

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

9 *(2) may empanel advisory committees.*

10 *(f) INTERNSHIPS.—The Director of the Office of Per-*
11 *sonnel Management may support, as appropriate, intern-*
12 *ships or other work experience in the Federal Government*
13 *to the winners of the competitions and challenges under this*
14 *section.*

15 **SEC. 302. FEDERAL CYBER SCHOLARSHIP-FOR-SERVICE**
16 **PROGRAM.**

17 *(a) IN GENERAL.—The Director of the National*
18 *Science Foundation, in coordination with the Director of*
19 *the Office of Personnel Management and Secretary of*
20 *Homeland Security, shall continue a Federal Cyber Schol-*
21 *arship-for-Service program to recruit and train the next*
22 *generation of information technology professionals, indus-*
23 *trial control system security professionals, and security*
24 *managers to meet the needs of the cybersecurity mission for*
25 *Federal, State, local, and tribal governments.*

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

3 (1) *provide scholarships to students who are en-*
4 *rolled in programs of study at institutions of higher*
5 *education leading to degrees or specialized program*
6 *certifications in the cybersecurity field;*

7 (2) *provide the scholarship recipients with sum-*
8 *mer internship opportunities or other meaningful*
9 *temporary appointments in the Federal information*
10 *technology workforce; and*

11 (3) *provide a procedure by which the National*
12 *Science Foundation or a Federal agency, consistent*
13 *with regulations of the Office of Personnel Manage-*
14 *ment, may request and fund security clearances for*
15 *scholarship recipients, including providing for clear-*
16 *ances during internships or other temporary appoint-*
17 *ments and after receipt of their degrees.*

18 **(c) SCHOLARSHIP AMOUNTS.**—*Each scholarship under*
19 *subsection (b) shall be in an amount that covers the stu-*
20 *dent’s tuition and fees at the institution under subsection*
21 *(b)(1) and provides the student with an additional stipend.*

22 **(d) SCHOLARSHIP CONDITIONS.**—*Each scholarship re-*
23 *cipient, as a condition of receiving a scholarship under the*
24 *program, shall enter into an agreement under which the*
25 *recipient agrees to work in the cybersecurity mission of a*

1 *Federal, State, local, or tribal agency for a period equal*
2 *to the length of the scholarship following receipt of the stu-*
3 *dent's degree.*

4 *(e) HIRING AUTHORITY.—*

5 *(1) APPOINTMENT IN EXCEPTED SERVICE.—Not-*
6 *withstanding any provision of chapter 33 of title 5,*
7 *United States Code, governing appointments in the*
8 *competitive service, an agency shall appoint in the*
9 *excepted service an individual who has completed the*
10 *academic program for which a scholarship was*
11 *awarded.*

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

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

21 *(4) AUTHORITY TO DECLINE CONVERSION.—An*
22 *agency may decline to make the noncompetitive con-*
23 *version or appointment under paragraph (2) for*
24 *cause.*

1 (f) *ELIGIBILITY.*—*To be eligible to receive a scholar-*
2 *ship under this section, an individual shall—*

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

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

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

10 (g) *REPAYMENT.*—*If a scholarship recipient does not*
11 *meet the terms of the program under this section, the recipi-*
12 *ent shall refund the scholarship payments in accordance*
13 *with rules established by the Director of the National*
14 *Science Foundation, in coordination with the Director of*
15 *the Office of Personnel Management and Secretary of*
16 *Homeland Security.*

17 (h) *EVALUATION AND REPORT.*—*The Director of the*
18 *National Science Foundation shall evaluate and report pe-*
19 *riodically to Congress on the success of recruiting individ-*
20 *uals for scholarships under this section and on hiring and*
21 *retaining those individuals in the public sector workforce.*

1 **SEC. 303. STUDY AND ANALYSIS OF EDUCATION, ACCREDI-**
2 **TATION, TRAINING, AND CERTIFICATION OF**
3 **INFORMATION INFRASTRUCTURE AND CY-**
4 **BERSECURITY PROFESSIONALS.**

5 (a) *STUDY.*—*The Director of the National Science*
6 *Foundation, the Director of the Office of Personnel Manage-*
7 *ment, and the Secretary of Homeland Security shall under-*
8 *take to enter into appropriate arrangements with the Na-*
9 *tional Academy of Sciences to conduct a comprehensive*
10 *study of government, academic, and private-sector edu-*
11 *cation, accreditation, training, and certification programs*
12 *for the development of professionals in information infra-*
13 *structure and cybersecurity. The agreement shall require the*
14 *National Academy of Sciences to consult with sector coordi-*
15 *nating councils and relevant governmental agencies, regu-*
16 *latory entities, and nongovernmental organizations in the*
17 *course of the study.*

18 (b) *SCOPE.*—*The study shall include—*

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

23 (2) *an assessment of whether existing govern-*
24 *ment, academic, and private-sector education, accred-*
25 *itation, training, and certification programs provide*

1 *the body of knowledge and various skills described in*
2 *paragraph (1);*

3 *(3) an evaluation of—*

4 *(A) the state of cybersecurity education at*
5 *institutions of higher education in the United*
6 *States;*

7 *(B) the extent of professional development*
8 *opportunities for faculty in cybersecurity prin-*
9 *ciples and practices;*

10 *(C) the extent of the partnerships and col-*
11 *laborative cybersecurity curriculum development*
12 *activities that leverage industry and government*
13 *needs, resources, and tools;*

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

16 *(E) the descriptions of the content of cyber-*
17 *security courses in undergraduate computer*
18 *science curriculum;*

19 *(4) an analysis of any barriers to the Federal*
20 *Government recruiting and hiring cybersecurity tal-*
21 *ent, including barriers relating to compensation, the*
22 *hiring process, job classification, and hiring flexi-*
23 *bility; and*

24 *(5) an analysis of the sources and availability of*
25 *cybersecurity talent, a comparison of the skills and*

1 *expertise sought by the Federal Government and the*
2 *private sector, an examination of the current and fu-*
3 *ture capacity of United States institutions of higher*
4 *education, including community colleges, to provide*
5 *current and future cybersecurity professionals,*
6 *through education and training activities, with those*
7 *skills sought by the Federal Government, State and*
8 *local entities, and the private sector.*

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

13 *(1) findings regarding the state of information*
14 *infrastructure and cybersecurity education, accredita-*
15 *tion, training, and certification programs, including*
16 *specific areas of deficiency and demonstrable progress;*
17 *and*

18 *(2) recommendations for further research and the*
19 *improvement of information infrastructure and cyber-*
20 *security education, accreditation, training, and cer-*
21 *tification programs.*

1 **TITLE** **IV—CYBERSECURITY**
2 **AWARENESS AND PREPARED-**
3 **NESS**

4 **SEC. 401. NATIONAL CYBERSECURITY AWARENESS AND**
5 **PREPAREDNESS CAMPAIGN.**

6 (a) *NATIONAL CYBERSECURITY AWARENESS AND PRE-*
7 *PREPAREDNESS CAMPAIGN.—The Director of the National In-*
8 *stitute of Standards and Technology (referred to in this sec-*
9 *tion as the “Director”), in consultation with appropriate*
10 *Federal agencies, shall continue to coordinate a national*
11 *cybersecurity awareness and preparedness campaign, such*
12 *as—*

13 (1) *a campaign to increase public awareness of*
14 *cybersecurity, cyber safety, and cyber ethics, includ-*
15 *ing the use of the Internet, social media, entertain-*
16 *ment, and other media to reach the public;*

17 (2) *a campaign to increase the understanding of*
18 *State and local governments, institutions of higher*
19 *education, and private sector entities of—*

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

23 (B) *the methods to mitigate and remediate*
24 *vulnerabilities;*

1 (3) support for formal cybersecurity education
2 programs at all education levels to prepare skilled cy-
3 bersecurity and computer science workers for the pri-
4 vate sector and Federal, State, and local government;
5 and

6 (4) initiatives to evaluate and forecast future cy-
7 bersecurity workforce needs of the Federal government
8 and develop strategies for recruitment, training, and
9 retention.

10 (b) *CONSIDERATIONS.*—In carrying out the authority
11 described in subsection (a), the Director, in consultation
12 with appropriate Federal agencies, shall leverage existing
13 programs designed to inform the public of safety and secu-
14 rity of products or services, including self-certifications and
15 independently verified assessments regarding the quan-
16 tification and valuation of information security risk.

17 (c) *STRATEGIC PLAN.*—The Director, in cooperation
18 with relevant Federal agencies and other stakeholders, shall
19 build upon programs and plans in effect as of the date of
20 enactment of this Act to develop and implement a strategic
21 plan to guide Federal programs and activities in support
22 of the national cybersecurity awareness and preparedness
23 campaign under subsection (a).

24 (d) *REPORT.*—Not later than 1 year after the date of
25 enactment of this Act, and every 5 years thereafter, the Di-

1 *rector shall transmit the strategic plan under subsection (c)*
2 *to the Committee on Commerce, Science, and Transpor-*
3 *tation of the Senate and the Committee on Science, Space,*
4 *and Technology of the House of Representatives.*

Calendar No. 490

113TH CONGRESS
2^D SESSION

S. 1353

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.

JULY 24, 2014

Reported with an amendment