

113TH CONGRESS
1ST 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

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,*

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

4 (a) SHORT TITLE.—This Act may be cited as the
5 “Cybersecurity Act of 2013”.

6 (b) TABLE OF CONTENTS.—The table of contents of
7 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.

1 **SEC. 2. DEFINITIONS.**

2 In this Act:

3 (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.

12 (2) **INFORMATION INFRASTRUCTURE.**—The term “information infrastructure” means the underlying framework that information systems and assets rely on to process, transmit, receive, or store infor-

1 mation electronically, including programmable elec-
2 tronic devices, communications networks, and indus-
3 trial or supervisory control systems and any associ-
4 ated hardware, software, or data.

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

8 **SEC. 3. NO REGULATORY AUTHORITY.**

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

12 **TITLE I—PUBLIC-PRIVATE COL-**
13 **LABORATION ON CYBERSECU-**
14 **RITY**

15 **SEC. 101. PUBLIC-PRIVATE COLLABORATION ON CYBERSE-**
16 **CURITY.**

17 (a) CYBERSECURITY.—Section 2(c) of the National
18 Institute of Standards and Technology Act (15 U.S.C.
19 272(c)) is amended—

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

23 (2) by inserting after paragraph (14) the fol-
24 lowing:

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

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

11 “(e) CYBER RISKS.—

12 “(1) IN GENERAL.—In carrying out the activi-
13 ties under subsection (c)(15), the Director—

14 “(A) shall—

15 “(i) coordinate closely and continu-
16 ously with relevant private sector personnel
17 and entities, critical infrastructure owners
18 and operators, sector coordinating councils,
19 Information Sharing and Analysis Centers,
20 and other relevant industry organizations,
21 and incorporate industry expertise;

22 “(ii) consult with the heads of agen-
23 cies with national security responsibilities,
24 sector-specific agencies, State and local

1 governments, the governments of other na-
2 tions, and international organizations;

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

10 “(iv) include methodologies—

11 “(I) to identify and mitigate im-
12 pacts of the cybersecurity measures or
13 controls on business confidentiality;
14 and

15 “(II) to protect individual privacy
16 and civil liberties;

17 “(v) incorporate voluntary consensus
18 standards and industry best practices;

19 “(vi) align with voluntary inter-
20 national standards to the fullest extent
21 possible;

22 “(vii) prevent duplication of regu-
23 latory processes and prevent conflict with
24 or superseding of regulatory requirements,

1 mandatory standards, and related proc-
2 esses; and

3 “(viii) include such other similar and
4 consistent elements as the Director con-
5 siders necessary; and

6 “(B) shall not prescribe or otherwise re-
7 quire—

8 “(i) the use of specific solutions;

9 “(ii) the use of specific information or
10 communications technology products or
11 services; or

12 “(iii) that information or communica-
13 tions technology products or services be de-
14 signed, developed, or manufactured in a
15 particular manner.

16 “(2) LIMITATION.—Information shared with or
17 provided to the Institute for the purpose of the ac-
18 tivities described under subsection (c)(15) shall not
19 be used by any Federal, State, tribal, or local de-
20 partment or agency to regulate the activity of any
21 entity.

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

23 “(A) CRITICAL INFRASTRUCTURE.—The
24 term ‘critical infrastructure’ has the meaning

1 given the term in section 1016(e) of the USA
 2 PATRIOT Act of 2001 (42 U.S.C. 5195c(e)).

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

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

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

16 (a) FUNDAMENTAL CYBERSECURITY RESEARCH.—

17 (1) IN GENERAL.—The Director of the Office of
 18 Science and Technology Policy, in coordination with
 19 the head of any relevant Federal agency, shall build
 20 upon programs and plans in effect as of the date of
 21 enactment of this Act to develop a Federal cyberse-
 22 curity research and development plan to meet objec-
 23 tives 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
5 and hardware, whether developed locally or ob-
6 tained from a third party, is free of significant
7 known security flaws;

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

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

17 (E) how to build new protocols to enable
18 the Internet to have robust security as one of
19 the key 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
8 of the Office of Science and Technology Policy,
9 in coordination with the head of any relevant
10 Federal agency and with input from stake-
11 holders, including industry and academia, deter-
12 mines 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,

1 the Director of the Office of Science and Tech-
2 nology Policy shall work in close cooperation
3 with industry, academia, and other interested
4 stakeholders to ensure, to the extent possible,
5 that Federal cybersecurity research and devel-
6 opment is not duplicative of private sector ef-
7 forts.

8 (3) TRIENNIAL UPDATES.—

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

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

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

24 (1) develops, evaluates, disseminates, and inte-
25 grates new cybersecurity practices and concepts into

1 the core curriculum of computer science programs
2 and of other programs where graduates of such pro-
3 grams have a substantial probability of developing
4 software after graduation, including new practices
5 and concepts relating to secure coding education and
6 improvement programs; and

7 (2) develops new models for professional devel-
8 opment of faculty in cybersecurity education, includ-
9 ing secure coding development.

10 (c) CYBERSECURITY MODELING AND TEST BEDS.—

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

22 (2) ADDITIONAL CYBERSECURITY MODELING
23 AND TEST BEDS.—

24 (A) IN GENERAL.—If the Director of the
25 National Science Foundation, after the review

1 under paragraph (1), determines that the re-
2 search needs under the Federal cybersecurity
3 research and development plan require the es-
4 tablishment of additional cybersecurity test
5 beds, the Director of the National Science
6 Foundation, in coordination with the Secretary
7 of Commerce and the Secretary of Homeland
8 Security, may award grants to institutions of
9 higher education or research and development
10 non-profit institutions to establish cybersecurity
11 test beds.

12 (B) REQUIREMENT.—The cybersecurity
13 test beds under subparagraph (A) shall be suffi-
14 ciently large in order to model the scale and
15 complexity of real-time cyber attacks and de-
16 fenses on real world networks and environ-
17 ments.

18 (C) ASSESSMENT REQUIRED.—The Direc-
19 tor of the National Science Foundation, in co-
20 ordination with the Secretary of Commerce and
21 the Secretary of Homeland Security, shall
22 evaluate the effectiveness of any grants award-
23 ed under this subsection in meeting the objec-
24 tives of the Federal cybersecurity research and
25 development plan under subsection (a) no later

1 than 2 years after the review under paragraph
2 (1) of this subsection, and periodically there-
3 after.

4 (d) COORDINATION WITH OTHER RESEARCH INITIA-
5 TIVES.—In accordance with the responsibilities under sec-
6 tion 101 of the High-Performance Computing Act of 1991
7 (15 U.S.C. 5511), the Director the Office of Science and
8 Technology Policy shall coordinate, to the extent prac-
9 ticable, Federal research and development activities under
10 this section with other ongoing research and development
11 security-related initiatives, including research being con-
12 ducted by—

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

23 (e) NATIONAL SCIENCE FOUNDATION COMPUTER
24 AND NETWORK SECURITY RESEARCH GRANT AREAS.—

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

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

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

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

8 “(J) secure fundamental protocols that are
9 integral to inter-network communications and
10 data exchange;

11 “(K) secure software engineering and soft-
12 ware assurance, including—

13 “(i) programming languages and sys-
14 tems that include fundamental security
15 features;

16 “(ii) portable or reusable code that re-
17 mains secure when deployed in various en-
18 vironments;

19 “(iii) verification and validation tech-
20 nologies to ensure that requirements and
21 specifications have been implemented; and

22 “(iv) models for comparison and
23 metrics to assure that required standards
24 have been met;

25 “(L) holistic system security that—

1 “(i) addresses the building of secure
2 systems from trusted and untrusted com-
3 ponents;

4 “(ii) proactively reduces
5 vulnerabilities;

6 “(iii) addresses insider threats; and

7 “(iv) supports privacy in conjunction
8 with improved security;

9 “(M) monitoring and detection;

10 “(N) mitigation and rapid recovery meth-
11 ods;

12 “(O) security of wireless networks and mo-
13 bile devices; and

14 “(P) security of cloud infrastructure and
15 services.”.

16 (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
17 Computing Act of 1991 (15 U.S.C. 5511(a)(3)(B)),
18 through existing programs and activities, shall support re-
19 search that will lead to the development of a scientific
20 foundation for the field of cybersecurity, including re-
21 search that increases understanding of the underlying
22 principles of securing complex networked systems, enables
23
24

1 repeatable experimentation, and creates quantifiable secu-
2 rity metrics.

3 **SEC. 202. COMPUTER AND NETWORK SECURITY RESEARCH**
4 **CENTERS.**

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

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

9 (2) in paragraph (5)—

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

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

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

16 “(E) the demonstrated capability of the
17 applicant to conduct high performance com-
18 putation integral to complex computer and net-
19 work security research, through on-site or off-
20 site computing;

21 “(F) the applicant’s affiliation with private
22 sector entities involved with industrial research
23 described in subsection (a)(1);

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

1 “(H) the applicant’s affiliation with exist-
2 ing research programs of the Federal Govern-
3 ment;

4 “(I) the applicant’s experience managing
5 public-private partnerships to transition new
6 technologies into a commercial setting or the
7 government user community; and

8 “(J) the capability of the applicant to con-
9 duct interdisciplinary cybersecurity research,
10 such as in law, economics, or behavioral
11 sciences.”.

12 **TITLE III—EDUCATION AND** 13 **WORKFORCE DEVELOPMENT**

14 **SEC. 301. CYBERSECURITY COMPETITIONS AND CHAL-** 15 **LENGES.**

16 (a) IN GENERAL.—The Secretary of Commerce, Di-
17 rector of the National Science Foundation, and Secretary
18 of Homeland Security shall—

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

23 (A) to identify, develop, and recruit tal-
24 ented individuals to perform duties relating to
25 the security of information infrastructure in

1 Federal, State, and local government agencies,
2 and the private sector; or

3 (B) to stimulate innovation in basic and
4 applied cybersecurity research, technology devel-
5 opment, and prototype demonstration that has
6 the potential for application to the information
7 technology activities of the Federal Govern-
8 ment; and

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

11 (b) PARTICIPATION.—Participants in the competi-
12 tions and challenges under subsection (a)(1) may in-
13 clude—

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

15 (2) students enrolled in a postsecondary pro-
16 gram of study leading to a baccalaureate degree at
17 an institution of higher education;

18 (3) students enrolled in a postbaccalaureate
19 program of study at an institution of higher edu-
20 cation;

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

23 (5) veterans; and

24 (6) other groups or individuals that the Sec-
25 retary of Commerce, Director of the National

1 Science Foundation, and Secretary of Homeland Se-
2 curity determine appropriate.

3 (c) AFFILIATION AND COOPERATIVE AGREE-
4 MENTS.—Competitions and challenges under this section
5 may be carried out through affiliation and cooperative
6 agreements with—

- 7 (1) Federal agencies;
- 8 (2) regional, State, or school programs sup-
9 porting the development of cyber professionals;
- 10 (3) State, local, and tribal governments; or
- 11 (4) other private sector organizations.

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

- 15 (1) ethical hacking;
- 16 (2) penetration testing;
- 17 (3) vulnerability assessment;
- 18 (4) continuity of system operations;
- 19 (5) security in design;
- 20 (6) cyber forensics;
- 21 (7) offensive and defensive cyber operations;
- 22 and
- 23 (8) other areas the Secretary of Commerce, Di-
24 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
14 this 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
25 for Federal, State, local, and tribal governments.

1 (b) PROGRAM DESCRIPTION AND COMPONENTS.—

2 The Federal Cyber Scholarship-for-Service program
3 shall—

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

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

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

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

24 (d) SCHOLARSHIP CONDITIONS.—Each scholarship
25 recipient, as a condition of receiving a scholarship under

1 the program, shall enter into an agreement under which
2 the recipient agrees to work in the cybersecurity mission
3 of a Federal, State, local, or tribal agency for a period
4 equal to the length of the scholarship following receipt of
5 the student's degree.

6 (e) HIRING AUTHORITY.—

7 (1) APPOINTMENT IN EXCEPTED SERVICE.—

8 Notwithstanding any provision of chapter 33 of title
9 5, United States Code, governing appointments in
10 the competitive service, an agency shall appoint in
11 the excepted service an individual who has completed
12 the academic program for which a scholarship was
13 awarded.

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

19 (3) TIMING OF CONVERSION.—An agency may
20 noncompetitively convert a term employee appointed
21 under paragraph (2) to a career-conditional or ca-
22 reer appointment before the term appointment ex-
23 pires.

24 (4) AUTHORITY TO DECLINE CONVERSION.—An
25 agency may decline to make the noncompetitive con-

1 version or appointment under paragraph (2) for
2 cause.

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

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

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

10 (3) have demonstrated a high level of pro-
11 ficiency in mathematics, engineering, or computer
12 sciences.

13 (g) REPAYMENT.—If a scholarship recipient does not
14 meet the terms of the program under this section, the re-
15 cipient shall refund the scholarship payments in accord-
16 ance with rules established by the Director of the National
17 Science Foundation, in coordination with the Director of
18 the Office of Personnel Management and Secretary of
19 Homeland Security.

20 (h) EVALUATION AND REPORT.—The Director of the
21 National Science Foundation shall evaluate and report pe-
22 riodically to Congress on the success of recruiting individ-
23 uals for scholarships under this section and on hiring and
24 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 and the Secretary of Homeland Security shall
7 undertake to enter into appropriate arrangements with the
8 National Academy of Sciences to conduct a comprehensive
9 study of government, academic, and private-sector edu-
10 cation, accreditation, training, and certification programs
11 for the development of professionals in information infra-
12 structure and cybersecurity. The agreement shall require
13 the National Academy of Sciences to consult with sector
14 coordinating councils and relevant governmental agencies,
15 regulatory entities, and nongovernmental organizations in
16 the course of the study.

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

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

23 (2) an assessment of whether existing govern-
24 ment, academic, and private-sector education, ac-
25 creditation, training, and certification programs pro-

1 vide the body of knowledge and various skills de-
2 scribed in 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
15 progress toward improving cybersecurity edu-
16 cation; and

17 (E) the descriptions of the content of cy-
18 bersecurity courses in undergraduate computer
19 science curriculum;

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

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

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

15 (1) findings regarding the state of information
16 infrastructure and cybersecurity education, accredi-
17 tation, training, and certification programs, includ-
18 ing specific areas of deficiency and demonstrable
19 progress; and

20 (2) recommendations for further research and
21 the improvement of information infrastructure and
22 cybersecurity education, accreditation, training, and
23 certification 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
7 PREPAREDNESS CAMPAIGN.—The Director of the Na-
8 tional Institute of Standards and Technology (referred to
9 in this section as the “Director”), in consultation with ap-
10 propriate Federal agencies, shall continue to coordinate a
11 national cybersecurity awareness and preparedness cam-
12 paign, such 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
18 of State and local governments and private sector
19 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
3 cybersecurity and computer science workers for the
4 private sector and Federal, State, and local govern-
5 ment; and

6 (4) initiatives to evaluate and forecast future
7 cybersecurity workforce needs of the Federal govern-
8 ment and develop strategies for recruitment, train-
9 ing, and 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
15 and independently verified assessments regarding the
16 quantification and valuation of information security risk.

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

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

1 the Director shall transmit the strategic plan under sub-
2 section (e) to the Committee on Commerce, Science, and
3 Transportation of the Senate and the Committee on
4 Science, Space, and Technology of the House of Rep-
5 resentatives.

○