

[STAFF WORKING DRAFT]

JULY 10, 2013

1 SECTION 1. TABLE OF CONTENTS.

2 The table of contents of this Act is as follows:

Sec. 1. Table of contents.

Sec. 2. Definitions.

TITLE I—PUBLIC-PRIVATE COLLABORATION ON CYBERSECURITY

Sec. 101. Public-private collaboration on cybersecurity.

TITLE II—CYBERSECURITY RESEARCH AND DEVELOPMENT

Sec. 201. National 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.

3 SEC. 2. DEFINITIONS.

4 In this Act:

5 (1) CYBERSECURITY MISSION.—The term
6 “cybersecurity mission” means activities that encom-
7 pass the full range of threat reduction, vulnerability
8 reduction, deterrence, international engagement, in-
9 cident response, resiliency, and recovery policies and
10 activities, including computer network operations, in-
11 formation 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 **TITLE I—PUBLIC-PRIVATE COL-**
15 **LABORATION ON**
16 **CYBERSECURITY**

17 **SEC. 101. PUBLIC-PRIVATE COLLABORATION ON**
18 **CYBERSECURITY.**

19 (a) CYBERSECURITY.—Section 2(c) of the National
20 Institute of Standards and Technology Act (15 U.S.C.
21 272(c)) is amended—

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

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

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

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

13 “(e) CYBER RISKS.—

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

16 “(A) shall—

17 “(i) coordinate closely and continu-
18 ously with relevant private sector personnel
19 and entities, critical infrastructure owners
20 and operators, sector coordinating councils,
21 Information Sharing and Analysis Centers,
22 and other relevant industry organizations,
23 and incorporate industry expertise to the
24 fullest extent possible;

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

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

13 “(iv) include methodologies—

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

18 “(II) to protect individual privacy
19 and civil liberties;

20 “(v) incorporate voluntary consensus
21 standards and industry best practices, and
22 align with voluntary international stand-
23 ards to the fullest extent possible;

24 “(vi) prevent duplication of existing
25 regulatory processes and prevent conflict

1 with or superseding of existing regulatory
2 requirements and processes; and

3 “(vii) 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
10 technology products or services; or

11 “(iii) that information technology
12 products or services be designed, devel-
13 oped, or manufactured in a particular
14 manner.

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

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

22 “(A) CRITICAL INFRASTRUCTURE.—The
23 term ‘critical infrastructure’ has the meaning
24 given the term in section 1016(e) of the USA
25 PATRIOT Act of 2001 (42 U.S.C. 5195c(e)).

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

10 **TITLE II—CYBERSECURITY**
11 **RESEARCH AND DEVELOPMENT**

12 **SEC. 201. NATIONAL CYBERSECURITY RESEARCH AND DE-**
13 **VELOPMENT.**

14 (a) FUNDAMENTAL CYBERSECURITY RESEARCH.—

15 (1) IN GENERAL.—The Director of the Office of
16 Science and Technology Policy, in coordination with
17 the head of any relevant Federal agency, shall build
18 upon programs and plans in effect as of the date of
19 enactment of this Act to develop a national
20 cybersecurity research and development plan to meet
21 objectives in cybersecurity, including—

22 (A) how to design and build complex soft-
23 ware-intensive systems that are secure and reli-
24 able when first deployed;

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

5 (C) how to test and verify that software
6 obtained from a third party correctly imple-
7 ments stated functionality, and only that
8 functionality;

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

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

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

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

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

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

1 (J) how to protect information stored
2 through cloud computing or transmitted
3 through wireless services; and

4 (K) any additional objectives the Director
5 of the Office of Science and Technology Policy,
6 in coordination with the head of any relevant
7 Federal agency, determines appropriate.

8 (2) REQUIREMENTS.—The national
9 cybersecurity research and development plan shall
10 identify and prioritize near-term, mid-term, and
11 long-term research in computer and information
12 science and engineering to meet the objectives under
13 paragraph (1), including research in the areas de-
14 scribed in section 4(a)(1) of the Cyber Security Re-
15 search and Development Act (15 U.S.C.
16 7403(a)(1)).

17 (3) BIENNIAL UPDATES.—

18 (A) IN GENERAL.—The national
19 cybersecurity research and development plan
20 shall be updated biennially.

21 (B) REPORT TO CONGRESS.—The Director
22 of the Office of Science and Technology Policy
23 shall submit the plan and each updated plan
24 under this section to the Committee on Com-
25 merce, Science, and Transportation of the Sen-

1 ate and the Committee on Science, Space, and
2 Technology of the House of Representatives.

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

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

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

17 (c) CYBERSECURITY MODELING AND TEST BEDS.—

18 (1) REVIEW.—Not later than 1 year after the
19 date of enactment of this Act, the Director the Na-
20 tional Science Foundation shall conduct a review of
21 cybersecurity test beds in existence on the date of
22 enactment of this Act to inform the grants under
23 paragraph (2). The review shall include an assess-
24 ment of whether a sufficient number of cybersecurity
25 test beds are available to meet the research needs

1 under the national cybersecurity research and devel-
2 opment 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 national 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 national 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, research and development activities under this sec-
16 tion with other ongoing research and development secu-
17 rity-related initiatives, including research being conducted
18 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
24 CYBERSECURITY.—The head of each agency and depart-
25 ment identified under section 101(a)(3)(B) of the High-

1 Performance Computing Act of 1991 (15 U.S.C.
2 5511(a)(3)(B)), through existing programs and activities,
3 shall support research that will lead to the development
4 of a scientific foundation for the field of cybersecurity, in-
5 cluding research that increases understanding of the un-
6 derlying principles of securing complex networked sys-
7 tems, enables repeatable experimentation, and creates
8 quantifiable security 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; and

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.”.

15 **TITLE III—EDUCATION AND**
16 **WORKFORCE DEVELOPMENT.**

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

19 (a) IN GENERAL.—The Secretary of Commerce, Di-
20 rector of the National Science Foundation, and Secretary
21 of Homeland Security shall—

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

1 (A) to identify, develop, and recruit tal-
2 ented individuals to perform duties relating to
3 the security of information infrastructure in
4 Federal, State, and local government agencies,
5 and the 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 Govern-
11 ment; and

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

14 (b) PARTICIPATION.—Participants in the competi-
15 tions and challenges under subsection (a)(1) may in-
16 clude—

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

18 (2) students enrolled in a postsecondary pro-
19 gram of study leading to a baccalaureate degree at
20 an institution of higher education;

21 (3) students enrolled in a postbaccalaureate
22 program of study at an institution of higher edu-
23 cation;

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

1 (5) veterans; and

2 (6) other groups or individuals that the Sec-
3 retary of Commerce, Director of the National
4 Science Foundation, and Secretary of Homeland Se-
5 curity determine appropriate.

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

10 (1) Federal agencies;

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

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

14 (4) other private sector organizations.

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

18 (1) ethical hacking;

19 (2) penetration testing;

20 (3) vulnerability assessment;

21 (4) continuity of system operations;

22 (5) cyber forensics;

23 (6) offensive and defensive cyber operations;

24 and

1 (7) other areas the Secretary of Commerce, Di-
2 rector of the National Science Foundation, and Sec-
3 retary of Homeland Security consider necessary to
4 fulfill the cybersecurity mission.

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

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

11 (2) may empanel advisory committees.

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

17 **SEC. 302. FEDERAL CYBER SCHOLARSHIP-FOR-SERVICE**
18 **PROGRAM.**

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

1 managers to meet the needs of the cybersecurity mission
2 for Federal, State, local, and tribal governments.

3 (b) PROGRAM DESCRIPTION AND COMPONENTS.—

4 The Federal Cyber Scholarship-for-Service program
5 shall—

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

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

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

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

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

8 (e) HIRING AUTHORITY.—

9 (1) APPOINTMENT IN EXCEPTED SERVICE.—

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

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

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

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

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

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

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

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

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

22 (h) EVALUATION AND REPORT.—The Director of the
23 National Science Foundation shall evaluate and report pe-
24 riodically to Congress on the success of recruiting individ-

1 uals for scholarships under this section and on hiring and
2 retaining those individuals in the public sector workforce.

3 **SEC. 303. STUDY AND ANALYSIS OF EDUCATION, ACCREDI-**
4 **TATION, TRAINING, AND CERTIFICATION OF**
5 **INFORMATION INFRASTRUCTURE AND**
6 **CYBERSECURITY PROFESSIONALS.**

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

19 (b) SCOPE.—The study shall include—

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

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

6 (3) an evaluation of—

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

10 (B) the extent of professional development
11 opportunities for faculty in cybersecurity prin-
12 ciples and practices;

13 (C) the extent of the partnerships and col-
14 laborative cybersecurity curriculum development
15 activities that leverage industry and government
16 needs, resources, and tools;

17 (D) the proposed metrics to assess
18 progress toward improving cybersecurity edu-
19 cation; and

20 (E) the descriptions of the content of
21 cybersecurity courses in undergraduate com-
22 puter science curriculum;

23 (4) an analysis of any barriers to the Federal
24 Government recruiting and hiring cybersecurity tal-
25 ent, including barriers relating to compensation, the

1 hiring process, job classification, and hiring flexi-
2 bility; and

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

13 (c) REPORT.—Not later than 1 year after the date
14 of enactment of this Act, the National Academies shall
15 submit to the President and Congress a report on the re-
16 sults of the study. The report shall include—

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

22 (2) recommendations for further research and
23 the improvement of information infrastructure and
24 cybersecurity education, accreditation, training, and
25 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.