

113<sup>TH</sup> CONGRESS  
2<sup>D</sup> SESSION

# S. 1353

---

## AN ACT

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

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 Enhancement Act of 2014”.

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.
- Sec. 4. No additional funds authorized.

**TITLE I—PUBLIC-PRIVATE COLLABORATION ON CYBERSECURITY**

Sec. 101. Public-private collaboration on cybersecurity.

**TITLE II—CYBERSECURITY RESEARCH AND DEVELOPMENT**

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

**TITLE III—EDUCATION AND WORKFORCE DEVELOPMENT**

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

**TITLE IV—CYBERSECURITY AWARENESS AND PREPAREDNESS**

Sec. 401. National cybersecurity awareness and education program.

**TITLE V—ADVANCEMENT OF CYBERSECURITY TECHNICAL  
STANDARDS**

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

6 **SEC. 2. DEFINITIONS.**

7 In this Act:

8 (1) **CYBERSECURITY MISSION.**—The term “cy-  
9 bersecurity mission” means activities that encom-  
10 pass the full range of threat reduction, vulnerability  
11 reduction, deterrence, international engagement, in-

1 cident response, resiliency, and recovery policies and  
2 activities, including computer network operations, in-  
3 formation assurance, law enforcement, diplomacy,  
4 military, and intelligence missions as such activities  
5 relate to the security and stability of cyberspace.

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

9 **SEC. 3. NO REGULATORY AUTHORITY.**

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

13 **SEC. 4. NO ADDITIONAL FUNDS AUTHORIZED.**

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

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(c) of the National  
24 Institute of Standards and Technology Act (15 U.S.C.  
25 272(c)) 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, consensus-  
8           based, industry-led set of standards, guidelines, best  
9           practices, methodologies, procedures, and processes  
10          to cost-effectively reduce cyber risks to critical infra-  
11          structure (as defined under subsection (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 (c)(15), the Director—

19                         “(A) shall—

20                                 “(i) coordinate closely and regularly  
21                                 with relevant private sector personnel and  
22                                 entities, critical infrastructure owners and  
23                                 operators, and other relevant industry or-  
24                                 ganizations, including Sector Coordinating  
25                                 Councils and Information Sharing and

1 Analysis Centers, and incorporate industry  
2 expertise;

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

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

16 “(iv) include methodologies—

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

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

23 “(v) incorporate voluntary consensus  
24 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. Nothing in this paragraph shall be construed  
3       to modify any regulatory requirement to report or  
4       submit information to a Federal, State, tribal, or  
5       local department or agency.

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  
12                     term ‘sector-specific agency’ means the Federal  
13                     department or agency responsible for providing  
14                     institutional knowledge and specialized expertise  
15                     as well as leading, facilitating, or supporting  
16                     the security and resilience programs and associ-  
17                     ated activities of its designated critical infra-  
18                     structure sector in the all-hazards environ-  
19                     ment.”.

20       (c) STUDY AND REPORTS.—

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

23                     (A) the progress made by the Director of  
24                     the National Institute of Standards and Tech-  
25                     nology in facilitating the development of stand-

1           ards and procedures to reduce cyber risks to  
2           critical infrastructure in accordance with sec-  
3           tion 2(c)(15) of the National Institute of Stand-  
4           ards and Technology Act, as added by this sec-  
5           tion;

6           (B) the extent to which the Director's fa-  
7           cilitation efforts are consistent with the direc-  
8           tive in such section that the development of  
9           such standards and procedures be voluntary  
10          and led by industry representatives;

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

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



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

4           (2) REPORTS.—Not later than 1 year after the  
5 date of the enactment of this Act, and every 2 years  
6 thereafter for the following 6 years, the Comptroller  
7 General shall submit a report, which summarizes the  
8 findings of the study conducted under paragraph  
9 (1), to the Committee on Commerce, Science, and  
10 Transportation of the Senate and the Committee on  
11 Science, Space, and Technology of the House of  
12 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) FEDERAL CYBERSECURITY RESEARCH AND  
19 DEVELOPMENT STRATEGIC PLAN.—The heads of the  
20 applicable agencies and departments, working  
21 through the National Science and Technology Coun-  
22 cil and the Networking and Information Technology  
23 Research and Development Program, shall develop  
24 and update every 4 years a Federal cybersecurity re-  
25 search and development strategic plan (referred to

1 in this subsection as the “strategic plan”) based on  
2 an assessment of cybersecurity risk to guide the  
3 overall direction of Federal cybersecurity and infor-  
4 mation assurance research and development for in-  
5 formation technology and networking systems. The  
6 heads of the applicable agencies and departments  
7 shall build upon existing programs and plans to de-  
8 velop the strategic plan to meet objectives in cyber-  
9 security, such as—

10 (A) how to design and build complex soft-  
11 ware-intensive systems that are secure and reli-  
12 able when first deployed;

13 (B) how to test and verify that software  
14 and hardware, whether developed locally or ob-  
15 tained from a third party, is free of significant  
16 known security flaws;

17 (C) how to test and verify that software  
18 and hardware obtained from a third party cor-  
19 rectly implements stated functionality, and only  
20 that functionality;

21 (D) how to guarantee the privacy of an in-  
22 dividual, including that individual’s identity, in-  
23 formation, and lawful transactions when stored  
24 in distributed systems or transmitted over net-  
25 works;

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

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

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

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

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

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

16          (K) any additional objectives the heads of  
17 the applicable agencies and departments, in co-  
18 ordination with the head of any relevant Fed-  
19 eral agency and with input from stakeholders,  
20 including appropriate national laboratories, in-  
21 dustry, and academia, determine appropriate.

22       (2) REQUIREMENTS.—

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

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

7 (ii) specify how the near-term objec-  
8 tives described in clause (i) complement re-  
9 search and development areas in which the  
10 private sector is actively engaged;

11 (iii) describe how the heads of the ap-  
12 plicable agencies and departments will  
13 focus on innovative, transformational tech-  
14 nologies with the potential to enhance the  
15 security, reliability, resilience, and trust-  
16 worthiness of the digital infrastructure,  
17 and to protect consumer privacy;

18 (iv) describe how the heads of the ap-  
19 plicable agencies and departments will fos-  
20 ter the rapid transfer of research and de-  
21 velopment results into new cybersecurity  
22 technologies and applications for the timely  
23 benefit of society and the national interest,  
24 including through the dissemination of best  
25 practices and other outreach activities;

1 (v) describe how the heads of the ap-  
2 plicable agencies and departments will es-  
3 tablish and maintain a national research  
4 infrastructure for creating, testing, and  
5 evaluating the next generation of secure  
6 networking and information technology  
7 systems; and

8 (vi) describe how the heads of the ap-  
9 plicable agencies and departments will fa-  
10 cilitate access by academic researchers to  
11 the infrastructure described in clause (v),  
12 as well as to relevant data, including event  
13 data.

14 (B) PRIVATE SECTOR EFFORTS.—In devel-  
15 oping, implementing, and updating the strategic  
16 plan, the heads of the applicable agencies and  
17 departments, working through the National  
18 Science and Technology Council and Net-  
19 working and Information Technology Research  
20 and Development Program, shall work in close  
21 cooperation with industry, academia, and other  
22 interested stakeholders to ensure, to the extent  
23 possible, that Federal cybersecurity research  
24 and development is not duplicative of private  
25 sector efforts.

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

5 (i) the advisory committee established  
6 under section 101(b)(1) of the High-Per-  
7 formance Computing Act of 1991 (15  
8 U.S.C. 5511(b)(1)); and

9 (ii) a wide range of stakeholders, in-  
10 cluding industry, academia, including rep-  
11 resentatives of minority serving institutions  
12 and community colleges, National Labora-  
13 tories, and other relevant organizations  
14 and institutions.

15 (D) IMPLEMENTATION ROADMAP.—The  
16 heads of the applicable agencies and depart-  
17 ments, working through the National Science  
18 and Technology Council and Networking and  
19 Information Technology Research and Develop-  
20 ment Program, shall develop and annually up-  
21 date an implementation roadmap for the stra-  
22 tegic plan. The implementation roadmap  
23 shall—

24 (i) specify the role of each Federal  
25 agency in carrying out or sponsoring re-

1 search and development to meet the re-  
2 search objectives of the strategic plan, in-  
3 cluding a description of how progress to-  
4 ward the research objectives will be evalu-  
5 ated;

6 (ii) specify the funding allocated to  
7 each major research objective of the stra-  
8 tegic plan and the source of funding by  
9 agency for the current fiscal year;

10 (iii) estimate the funding required for  
11 each major research objective of the stra-  
12 tegic plan for the following 3 fiscal years;  
13 and

14 (iv) track ongoing and completed Fed-  
15 eral cybersecurity research and develop-  
16 ment projects.

17 (3) REPORTS TO CONGRESS.—The heads of the  
18 applicable agencies and departments, working  
19 through the National Science and Technology Coun-  
20 cil and Networking and Information Technology Re-  
21 search and Development Program, shall submit to  
22 the 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 (A) the strategic plan not later than 1 year  
2 after the date of enactment of this Act;

3 (B) each quadrennial update to the stra-  
4 tegic plan; and

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

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

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

21 (1) develops, evaluates, disseminates, and inte-  
22 grates new cybersecurity practices and concepts into  
23 the core curriculum of computer science programs  
24 and of other programs where graduates of such pro-  
25 grams have a substantial probability of developing



1 software after graduation, including new practices  
2 and concepts relating to secure coding education and  
3 improvement programs; and

4 (2) develops new models for professional devel-  
5 opment of faculty in cybersecurity education, includ-  
6 ing secure coding development.

7 (c) CYBERSECURITY MODELING AND TEST BEDS.—

8 (1) REVIEW.—Not later than 1 year after the  
9 date of enactment of this Act, the Director of the  
10 National Science Foundation, in coordination with  
11 the Director of the Office of Science and Technology  
12 Policy, shall conduct a review of cybersecurity test  
13 beds in existence on the date of enactment of this  
14 Act to inform the grants under paragraph (2). The  
15 review shall include an assessment of whether a suf-  
16 ficient number of cybersecurity test beds are avail-  
17 able to meet the research needs under the Federal  
18 cybersecurity research and development strategic  
19 plan. Upon completion, the Director shall submit the  
20 review to the Committee on Commerce, Science, and  
21 Transportation of the Senate and the Committee on  
22 Science, Space, and Technology of the House of  
23 Representatives.

24 (2) ADDITIONAL CYBERSECURITY MODELING  
25 AND TEST BEDS.—

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

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

20           (C) ASSESSMENT REQUIRED.—The Direc-  
21 tor of the National Science Foundation, in co-  
22 ordination with the Secretary of Commerce and  
23 the Secretary of Homeland Security, shall  
24 evaluate the effectiveness of any grants award-  
25 ed under this subsection in meeting the objec-

1           tives of the Federal cybersecurity research and  
2           development strategic plan not later than 2  
3           years after the review under paragraph (1) of  
4           this subsection, and periodically thereafter.

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

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

24           (e) NATIONAL SCIENCE FOUNDATION COMPUTER  
25 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 CYBERSECU-  
17   RITY.—The head of each agency and department identi-  
18   fied under section 101(a)(3)(B) of the High-Performance  
19   Computing Act of 1991 (15 U.S.C. 5511(a)(3)(B)),  
20   through existing programs and activities, shall support re-  
21   search that will lead to the development of a scientific  
22   foundation for the field of cybersecurity, including re-  
23   search that increases understanding of the underlying  
24   principles of securing complex networked systems, enables

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) in paragraph (3), by striking “the research  
8 areas” and inserting the following: “improving the  
9 security and resiliency of information technology, re-  
10 ducing cyber vulnerabilities, and anticipating and  
11 mitigating consequences of cyber attacks on critical  
12 infrastructure, by conducting research in the areas”;

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

15 (3) 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;

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

19 “(K) the capability of the applicant to con-  
20 duct research in areas such as systems security,  
21 wireless security, networking and protocols, for-  
22 mal methods and high-performance computing,  
23 nanotechnology, or industrial control systems.”.

1 **SEC. 203. CYBERSECURITY AUTOMATION AND CHECKLISTS**  
2 **FOR GOVERNMENT SYSTEMS.**

3 Section 8(c) of the Cyber Security Research and De-  
4 velopment Act (15 U.S.C. 7406(c)) is amended to read  
5 as follows:

6 “(c) SECURITY AUTOMATION AND CHECKLISTS FOR  
7 GOVERNMENT SYSTEMS.—

8 “(1) IN GENERAL.—The Director of the Na-  
9 tional Institute of Standards and Technology shall,  
10 as necessary, develop and revise security automation  
11 standards, associated reference materials (including  
12 protocols), and checklists providing settings and op-  
13 tion selections that minimize the security risks asso-  
14 ciated with each information technology hardware or  
15 software system and security tool that is, or is likely  
16 to become, widely used within the Federal Govern-  
17 ment, thereby enabling standardized and interoper-  
18 able technologies, architectures, and frameworks for  
19 continuous monitoring of information security within  
20 the Federal Government.

21 “(2) PRIORITIES FOR DEVELOPMENT.—The Di-  
22 rector of the National Institute of Standards and  
23 Technology shall establish priorities for the develop-  
24 ment of standards, reference materials, and check-  
25 lists under this subsection on the basis of—



1           “(A) the security risks associated with the  
2 use of the system;

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

5           “(C) the usefulness of the standards, ref-  
6 erence materials, or checklists to Federal agen-  
7 cies that are users or potential users of the sys-  
8 tem;

9           “(D) the effectiveness of the associated  
10 standard, reference material, or checklist in cre-  
11 ating or enabling continuous monitoring of in-  
12 formation security; or

13           “(E) such other factors as the Director of  
14 the National Institute of Standards and Tech-  
15 nology determines to be appropriate.

16           “(3) EXCLUDED SYSTEMS.—The Director of  
17 the National Institute of Standards and Technology  
18 may exclude from the application of paragraph (1)  
19 any information technology hardware or software  
20 system or security tool for which such Director de-  
21 termines that the development of a standard, ref-  
22 erence material, or checklist is inappropriate because  
23 of the infrequency of use of the system, the obsoles-  
24 cence of the system, or the lack of utility or imprac-

1       ticability of developing a standard, reference mate-  
2       rial, or checklist for the system.

3               “(4) DISSEMINATION OF STANDARDS AND RE-  
4       LATED MATERIALS.—The Director of the National  
5       Institute of Standards and Technology shall ensure  
6       that Federal agencies are informed of the avail-  
7       ability of any standard, reference material, checklist,  
8       or other item developed under this subsection.

9               “(5) AGENCY USE REQUIREMENTS.—The devel-  
10       opment of standards, reference materials, and check-  
11       lists under paragraph (1) for an information tech-  
12       nology hardware or software system or tool does  
13       not—

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

18               “(B) establish conditions or prerequisites  
19       for Federal agency procurement or deployment  
20       of any such system;

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

24               “(D) preclude any Federal agency from  
25       procuring or deploying other information tech-

1           nology hardware or software systems for which  
2           no such standard, reference material, or check-  
3           list has been developed or identified under para-  
4           graph (1).”.

5 **SEC. 204. NATIONAL INSTITUTE OF STANDARDS AND TECH-**  
6                   **NOLOGY CYBERSECURITY RESEARCH AND**  
7                   **DEVELOPMENT.**

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

10           (1) by redesignating subsection (e) as sub-  
11           section (f); and

12           (2) by inserting after subsection (d) the fol-  
13           lowing:

14           “(e) INTRAMURAL SECURITY RESEARCH.—As part of  
15           the research activities conducted in accordance with sub-  
16           section (d)(3), the Institute shall, to the extent practicable  
17           and appropriate—

18           “(1) conduct a research program to develop a  
19           unifying and standardized identity, privilege, and ac-  
20           cess control management framework for the execu-  
21           tion of a wide variety of resource protection policies  
22           and that is amenable to implementation within a  
23           wide variety of existing and emerging computing en-  
24           vironments;

1           “(2) carry out research associated with improv-  
2           ing the security of information systems and net-  
3           works;

4           “(3) carry out research associated with improv-  
5           ing the testing, measurement, usability, and assur-  
6           ance of information systems and networks;

7           “(4) carry out research associated with improv-  
8           ing security of industrial control systems;

9           “(5) carry out research associated with improv-  
10          ing the security and integrity of the information  
11          technology supply chain; and

12          “(6) carry out any additional research the Insti-  
13          tute determines appropriate.”.

## 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, Di-  
19           rector of the National Science Foundation, and Secretary  
20           of Homeland Security, in consultation with the Director  
21           of the Office of Personnel Management, shall—

22           (1) support competitions and challenges under  
23           section 24 of the Stevenson-Wydler Technology In-  
24           novation Act of 1980 (15 U.S.C. 3719) (as amended  
25           by section 105 of the America COMPETES Reau-

1       thorization Act of 2010 (124 Stat. 3989)) or any  
2       other provision of law, as appropriate—

3               (A) to identify, develop, and recruit tal-  
4               ented individuals to perform duties relating to  
5               the security of information technology in Fed-  
6               eral, State, local, and tribal government agen-  
7               cies, and the private sector; or

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

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

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

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

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

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

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

3           (5) veterans; and

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

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

12           (1) Federal agencies;

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

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

16           (4) other private sector organizations.

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

20           (1) ethical hacking;

21           (2) penetration testing;

22           (3) vulnerability assessment;

23           (4) continuity of system operations;

24           (5) security in design;

25           (6) cyber forensics;



1 generation of information technology professionals, indus-  
2 trial control system security professionals, and security  
3 managers to meet the needs of the cybersecurity mission  
4 for Federal, State, local, and tribal governments.

5 (b) PROGRAM DESCRIPTION AND COMPONENTS.—  
6 The Federal Cyber Scholarship-for-Service Program  
7 shall—

8 (1) provide scholarships through qualified insti-  
9 tutions of higher education, including community  
10 colleges, to students who are enrolled in programs of  
11 study at institutions of higher education leading to  
12 degrees or specialized program certifications in the  
13 cybersecurity field;

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

18 (3) prioritize the employment placement of  
19 scholarship recipients in the Federal Government.

20 (c) SCHOLARSHIP AMOUNTS.—Each scholarship  
21 under subsection (b) shall be in an amount that covers  
22 the student's tuition and fees at the institution under sub-  
23 section (b)(1) for not more than 3 years and provides the  
24 student with an additional stipend.



1 (d) POST-AWARD EMPLOYMENT OBLIGATIONS.—

2 Each scholarship recipient, as a condition of receiving a  
3 scholarship under the program, shall enter into an agree-  
4 ment under which the recipient agrees to work in the cy-  
5 bersecurity mission of a Federal, State, local, or tribal  
6 agency for a period equal to the length of the scholarship  
7 following receipt of 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 eligible degree program for which a scholarship  
15 was 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 technology;

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

14          (4) be a full-time student in an eligible degree  
15          program at a qualified institution of higher edu-  
16          cation, as determined by the Director of the Na-  
17          tional Science Foundation; and

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

20          (g) CONDITIONS OF SUPPORT.—

21          (1) IN GENERAL.—As a condition of receiving a  
22          scholarship under this section, a recipient shall agree  
23          to provide the qualified institution of higher edu-  
24          cation with annual verifiable documentation of post-

1 award employment and up-to-date contact informa-  
2 tion.

3 (2) TERMS.—A scholarship recipient under this  
4 section shall be liable to the United States as pro-  
5 vided in subsection (i) if the individual—

6 (A) fails to maintain an acceptable level of  
7 academic standing at the applicable institution  
8 of higher education, as determined by the Di-  
9 rector of the National Science Foundation;

10 (B) is dismissed from the applicable insti-  
11 tution of higher education for disciplinary rea-  
12 sons;

13 (C) withdraws from the eligible degree pro-  
14 gram before completing the program;

15 (D) declares that the individual does not  
16 intend to fulfill the post-award employment ob-  
17 ligation under this section; or

18 (E) fails to fulfill the post-award employ-  
19 ment obligation of the individual under this sec-  
20 tion.

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

24 (1) enter into an agreement with the Director  
25 of the National Science Foundation, to monitor the

1 compliance of scholarship recipients with respect to  
2 their post-award employment obligations; and

3 (2) provide to the Director of the National  
4 Science Foundation, on an annual basis, the post-  
5 award employment documentation required under  
6 subsection (g)(1) for scholarship recipients through  
7 the completion of their post-award employment obli-  
8 gations.

9 (i) AMOUNT OF REPAYMENT.—

10 (1) LESS THAN 1 YEAR OF SERVICE.—If a cir-  
11 cumstance described in subsection (g)(2) occurs be-  
12 fore the completion of 1 year of a post-award em-  
13 ployment obligation under this section, the total  
14 amount of scholarship awards received by the indi-  
15 vidual under this section shall—

16 (A) be repaid; or

17 (B) be treated as a loan to be repaid in ac-  
18 cordance with subsection (j).

19 (2) 1 OR MORE YEARS OF SERVICE.—If a cir-  
20 cumstance described in subparagraph (D) or (E) of  
21 subsection (g)(2) occurs after the completion of 1 or  
22 more years of a post-award employment obligation  
23 under this section, the total amount of scholarship  
24 awards received by the individual under this section,  
25 reduced by the ratio of the number of years of serv-

1       ice completed divided by the number of years of  
2       service required, shall—

3               (A) be repaid; or

4               (B) be treated as a loan to be repaid in ac-  
5       cordance with subsection (j).

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

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

12              (2) be subject to repayment, together with in-  
13      terest thereon accruing from the date of the scholar-  
14      ship award, in accordance with terms and conditions  
15      specified by the Director of the National Science  
16      Foundation (in consultation with the Secretary of  
17      Education) in regulations promulgated to carry out  
18      this subsection.

19      (k) COLLECTION OF REPAYMENT.—

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

24              (A) determine the repayment amounts and  
25      notify the recipient and the Director of the Na-

1            tional Science Foundation of the amounts owed;  
2            and

3            (B) collect the repayment amounts within  
4            a period of time as determined by the Director  
5            of the National Science Foundation, or the re-  
6            payment amounts shall be treated as a loan in  
7            accordance with subsection (j).

8            (2) RETURNED TO TREASURY.—Except as pro-  
9            vided in paragraph (3), any repayment under this  
10           subsection shall be returned to the Treasury of the  
11           United States.

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

19           (1) EXCEPTIONS.—The Director of the National  
20           Science Foundation may provide for the partial or total  
21           waiver or suspension of any service or payment obligation  
22           by an individual under this section whenever compliance  
23           by the individual with the obligation is impossible or would  
24           involve extreme hardship to the individual, or if enforce-

1 ment of such obligation with respect to the individual  
2 would be unconscionable.

3 (m) **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 **TITLE IV—CYBERSECURITY**  
9 **AWARENESS AND PREPARED-**  
10 **NESS**

11 **SEC. 401. NATIONAL CYBERSECURITY AWARENESS AND**  
12 **EDUCATION PROGRAM.**

13 (a) **NATIONAL CYBERSECURITY AWARENESS AND**  
14 **EDUCATION PROGRAM.**—The Director of the National In-  
15 stitute of Standards and Technology (referred to in this  
16 section as the “Director”), in consultation with appro-  
17 priate Federal agencies, industry, educational institutions,  
18 National Laboratories, the Networking and Information  
19 Technology Research and Development program, and  
20 other organizations shall continue to coordinate a national  
21 cybersecurity awareness and education program, that in-  
22 cludes activities such as—

23 (1) the widespread dissemination of cybersecu-  
24 rity technical standards and best practices identified  
25 by the Director;

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

5           (3) increasing public awareness of cybersecu-  
6 rity, cyber safety, and cyber ethics;

7           (4) increasing the understanding of State, local,  
8 and tribal governments, institutions of higher edu-  
9 cation, and private sector entities of—

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

13           (B) the methods to mitigate and remediate  
14 vulnerabilities;

15           (5) supporting formal cybersecurity education  
16 programs at all education levels to prepare and im-  
17 prove a skilled cybersecurity and computer science  
18 workforce for the private sector and Federal, State,  
19 local, and tribal government; and

20           (6) promoting initiatives to evaluate and fore-  
21 cast future cybersecurity workforce needs of the  
22 Federal Government and develop strategies for re-  
23 cruitment, training, and retention.

24           (b) CONSIDERATIONS.—In carrying out the authority  
25 described in subsection (a), the Director, in consultation



1 with appropriate Federal agencies, shall leverage existing  
2 programs designed to inform the public of safety and secu-  
3 rity of products or services, including self-certifications  
4 and independently verified assessments regarding the  
5 quantification and valuation of information security risk.

6 (c) STRATEGIC PLAN.—The Director, in cooperation  
7 with relevant Federal agencies and other stakeholders,  
8 shall build upon programs and plans in effect as of the  
9 date of enactment of this Act to develop and implement  
10 a strategic plan to guide Federal programs and activities  
11 in support of the national cybersecurity awareness and  
12 education program under subsection (a).

13 (d) REPORT.—Not later than 1 year after the date  
14 of enactment of this Act, and every 5 years thereafter,  
15 the Director shall transmit the strategic plan under sub-  
16 section (c) to the Committee on Commerce, Science, and  
17 Transportation of the Senate and the Committee on  
18 Science, Space, and Technology of the House of Rep-  
19 resentatives.

20 **TITLE V—ADVANCEMENT OF CY-**  
21 **BERSECURITY TECHNICAL**  
22 **STANDARDS**

23 **SEC. 501. DEFINITIONS.**

24 In this title:

1           (1) DIRECTOR.—The term “Director” means  
2           the Director of the National Institute of Standards  
3           and Technology.

4           (2) INSTITUTE.—The term “Institute” means  
5           the National Institute of Standards and Technology.

6 **SEC. 502. INTERNATIONAL CYBERSECURITY TECHNICAL**  
7           **STANDARDS.**

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

10           (1) as appropriate, ensure coordination of Fed-  
11           eral agencies engaged in the development of inter-  
12           national technical standards related to information  
13           system security; and

14           (2) not later than 1 year after the date of en-  
15           actment of this Act, develop and transmit to Con-  
16           gress a plan for ensuring such Federal agency co-  
17           ordination.

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

22 **SEC. 503. CLOUD COMPUTING STRATEGY.**

23           (a) IN GENERAL.—The Director, in coordination with  
24           the Office of Management and Budget, in collaboration  
25           with the Federal Chief Information Officers Council, and

1 in consultation with other relevant Federal agencies and  
2 stakeholders from the private sector, shall continue to de-  
3 velop and encourage the implementation of a comprehen-  
4 sive strategy for the use and adoption of cloud computing  
5 services by the Federal Government.

6 (b) ACTIVITIES.—In carrying out the strategy de-  
7 scribed under subsection (a), the Director shall give con-  
8 sideration to activities that—

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

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

16 (3) support, in coordination with the Office of  
17 Management and Budget, and in consultation with  
18 the private sector, the development of appropriate  
19 security frameworks and reference materials, and  
20 the identification of best practices, for use by Fed-  
21 eral agencies to address security and privacy re-  
22 quirements to enable the use and adoption of cloud  
23 computing services, including activities—

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

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

6 (C) to develop security standards as re-  
7 quired under section 20 of the National Insti-  
8 tute of Standards and Technology Act (15  
9 U.S.C. 278g-3); and

10 (D) to support the development of the au-  
11 tomation of continuous monitoring systems.

12 **SEC. 504. IDENTITY MANAGEMENT RESEARCH AND DEVEL-**  
13 **OPMENT.**

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

18 (1) to improve interoperability among identity  
19 management technologies;

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

22 (3) to improve privacy protection in identity  
23 management systems, including health information  
24 technology systems, through authentication and se-  
25 curity protocols; and

1           (4) to improve the usability of identity manage-  
2           ment systems.

Passed the Senate December 11, 2014.

Attest:

*Secretary.*

113<sup>TH</sup> CONGRESS  
2<sup>D</sup> SESSION

---

---

**S. 1353**

**AN ACT**

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