

116TH CONGRESS
2D SESSION

H. R. 8634

To improve United States cybersecurity through STEM scholarships, prize competitions, and other STEM activities, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

OCTOBER 20, 2020

Ms. KENDRA S. HORN of Oklahoma introduced the following bill; which was referred to the Committee on Science, Space, and Technology, and in addition to the Committee on Education and Labor, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

A BILL

To improve United States cybersecurity through STEM scholarships, prize competitions, and other STEM activities, 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.**

4 This Act may be cited as the “HACKED Act”.

1 **SEC. 2. IMPROVING NATIONAL INITIATIVE FOR CYBERSE-**
2 **CURITY EDUCATION.**

3 (a) PROGRAM IMPROVEMENTS GENERALLY.—Sub-
4 section (a) of section 401 of the Cybersecurity Enhance-
5 ment Act of 2014 (15 U.S.C. 7451(a)) is amended—

6 (1) in paragraph (5), by striking “; and” and
7 inserting a semicolon;

8 (2) by redesignating paragraph (6) as para-
9 graph (10); and

10 (3) by inserting after paragraph (5) the fol-
11 lowing:

12 “(6) supporting efforts to identify cybersecurity
13 workforce skill gaps in public and private sectors;

14 “(7) facilitating efforts for Federal programs to
15 advance cybersecurity education, training, and work-
16 force development;

17 “(8) in coordination with the Department of
18 Homeland Security and other appropriate agencies,
19 considering any specific needs of the cybersecurity
20 workforce of critical infrastructure, to include cyber
21 physical systems and control systems;

22 “(9) advising the Director of the Office of Man-
23 agement and Budget, as needed, in developing
24 metrics to measure the effectiveness and effect of
25 programs and initiatives to advance the cybersecu-
26 rity workforce; and”.

1 (b) STRATEGIC PLAN.—Subsection (c) of such sec-
2 tion is amended—

3 (1) by striking “The Director” and inserting
4 the following:

5 “(1) IN GENERAL.—The Director”; and

6 (2) by adding at the end the following:

7 “(2) REQUIREMENT.—The strategic plan devel-
8 oped and implemented under paragraph (1) shall in-
9 clude an indication of how the Director will carry
10 out this subsection.”.

11 (c) CYBERSECURITY CAREER PATHWAYS.—

12 (1) IDENTIFICATION OF MULTIPLE CYBERSECU-
13 RITY CAREER PATHWAYS.—In carrying out sub-
14 section (a) of such section and not later than 540
15 days after the date of the enactment of this Act, the
16 Director of the National Institute of Standards and
17 Technology shall, in coordination with the Secretary
18 of Homeland Security, the Director of the Office of
19 Personnel Management, and other appropriate agen-
20 cies, use a consultative process with other Federal
21 agencies, academia, and industry to make public a
22 report identifying multiple career pathways for cy-
23 bersecurity work roles that can be used in the pri-
24 vate and public sectors.

1 (2) REQUIREMENTS.—The Director of the Na-
2 tional Institute of Standards and Technology shall
3 ensure that the multiple cybersecurity career path-
4 ways identified under paragraph (1) indicate the
5 knowledge, skills, and abilities, including relevant
6 education, training, internships, apprenticeships, cer-
7 tifications, and other experiences, that—

8 (A) align with employers’ cybersecurity
9 skill needs, including proficiency level require-
10 ments, for its workforce; and

11 (B) prepare an individual to be successful
12 in entering or advancing in a cybersecurity ca-
13 reer.

14 (3) EXCHANGE PROGRAM.—Consistent with re-
15 quirements under chapter 37 of title 5, United
16 States Code, the Director of the National Institute
17 of Standards and Technology, in coordination with
18 the Director of the Office of Personnel Management,
19 may establish a voluntary program for the exchange
20 of employees engaged in one of the cybersecurity
21 work roles identified in the National Initiative for
22 Cybersecurity Education (NICE) Cybersecurity
23 Workforce Framework (NIST Special Publication
24 800–181), or successor framework, between the Na-
25 tional Institute of Standards and Technology and

1 private sector institutions, including nonpublic or
2 commercial businesses, research institutions, or in-
3 stitutions of higher education, as the Director of the
4 National Institute of Standards and Technology con-
5 siderers feasible.

6 (d) PROFICIENCY TO PERFORM CYBERSECURITY
7 TASKS.—In carrying out subsection (a) of such section,
8 the Director of the National Institute of Standards and
9 Technology shall, in coordination with the Secretary of
10 Homeland Security, and other appropriate agencies—

11 (1) assess the scope and sufficiency of efforts to
12 measure an individual’s capability to perform spe-
13 cific tasks found in the National Initiative for Cyber-
14 security Education (NICE) Cybersecurity Workforce
15 Framework (NIST Special Publication 800–181) at
16 all proficiency levels; and

17 (2) not later than 540 days after the date of
18 the enactment of this Act, submit to Congress a re-
19 port—

20 (A) on the findings of the Director with re-
21 spect to the assessment carried out under para-
22 graph (1); and

23 (B) with recommendations for effective
24 methods for measuring the cybersecurity pro-
25 ficiency of learners.

1 (e) CYBERSECURITY METRICS.—Such section is fur-
2 ther amended by adding at the end the following:

3 “(e) CYBERSECURITY METRICS.—In carrying out
4 subsection (a), the Director of the Office of Management
5 and Budget may seek input from the Director of the Na-
6 tional Institute of Standards and Technology, in coordina-
7 tion with the Department of Homeland Security, the Of-
8 fice of Personnel Management, and such agencies as the
9 Director of the National Institute of Standards and Tech-
10 nology considers relevant, to develop quantifiable metrics
11 for evaluating federally funded cybersecurity workforce
12 programs and initiatives based on the outcomes of such
13 programs and initiatives.”.

14 (f) REGIONAL ALLIANCES AND MULTISTAKEHOLDER
15 PARTNERSHIPS.—Such section is further amended by
16 adding at the end the following:

17 “(f) REGIONAL ALLIANCES AND MULTISTAKE-
18 HOLDER PARTNERSHIPS.—

19 “(1) IN GENERAL.—Pursuant to section 2(b)(4)
20 of the National Institute of Standards and Tech-
21 nology Act, the Director shall establish cooperative
22 agreements between the National Initiative for Cy-
23 bersecurity Education (NICE) of the Institute and
24 regional alliances or partnerships for cybersecurity
25 education and workforce.

1 “(2) AGREEMENTS.—The cooperative agree-
2 ments established under paragraph (1) shall advance
3 the goals of the National Initiative for Cybersecurity
4 Education Cybersecurity Workforce Framework
5 (NIST Special Publication 800–181), or successor
6 framework, by facilitating local and regional partner-
7 ships—

8 “(A) to identify the workforce needs of the
9 local economy and classify such workforce in ac-
10 cordance with such framework;

11 “(B) to identify the education, training,
12 apprenticeship, and other opportunities avail-
13 able in the local economy; and

14 “(C) to support opportunities to meet the
15 needs of the local economy.

16 “(3) FINANCIAL ASSISTANCE.—

17 “(A) FINANCIAL ASSISTANCE AUTHOR-
18 IZED.—The Director may award financial as-
19 sistance to a regional alliance or partnership
20 with whom the Director enters into a coopera-
21 tive agreement under paragraph (1) in order to
22 assist the regional alliance or partnership in
23 carrying out the term of the cooperative agree-
24 ment.

1 “(B) AMOUNT OF ASSISTANCE.—The ag-
2 gregate amount of financial assistance awarded
3 under subparagraph (A) per cooperative agree-
4 ment shall not exceed \$200,000.

5 “(C) MATCHING REQUIREMENT.—The Di-
6 rector may not award financial assistance to a
7 regional alliance or partnership under subpara-
8 graph (A) unless the regional alliance or part-
9 nership agrees that, with respect to the costs to
10 be incurred by the regional alliance or partner-
11 ship in carrying out the cooperative agreement
12 for which the assistance was awarded, the re-
13 gional alliance or partnership will make avail-
14 able (directly or through donations from public
15 or private entities) non-Federal contributions,
16 including in-kind contributions, in an amount
17 equal to 50 percent of Federal funds provided
18 under the award.

19 “(4) APPLICATION.—

20 “(A) IN GENERAL.—A regional alliance or
21 partnership seeking to enter into a cooperative
22 agreement under paragraph (1) and receive fi-
23 nancial assistance under paragraph (3) shall
24 submit to the Director an application therefore

1 at such time, in such manner, and containing
2 such information as the Director may require.

3 “(B) REQUIREMENTS.—Each application
4 submitted under subparagraph (A) shall include
5 the following:

6 “(i)(I) An identification of, or a plan
7 to establish, a multistakeholder workforce
8 partnership that includes—

9 “(aa) at least one institution of
10 higher education or nonprofit training
11 organization; and

12 “(bb) at least one local employer
13 or owner or operator of critical infra-
14 structure.

15 “(II) Participation from academic in-
16 stitutions in the Federal Cyber Scholar-
17 ships for Service, National Centers of Aca-
18 demic Excellence in Cybersecurity program
19 or advanced technological education pro-
20 grams, as well as elementary and sec-
21 ondary schools, training and certification
22 providers, State and local governments,
23 economic development organizations, or
24 other community organizations is encour-
25 aged.

1 “(ii) A description of how the work-
2 force partnership would identify the work-
3 force needs of the local economy.

4 “(iii) A description of how the multi-
5 stakeholder workforce partnership would
6 leverage the programs and objectives of the
7 National Initiative for Cybersecurity Edu-
8 cation, such as the Cybersecurity Work-
9 force Framework and the strategic plan of
10 such initiative.

11 “(iv) A description of how employers
12 in the community will be recruited to sup-
13 port internships, externships, apprentice-
14 ships, or cooperative education programs
15 in conjunction with providers of education
16 and training. Inclusion of programs that
17 seek to include veterans and underrep-
18 resented groups, including women, minori-
19 ties, persons from rural and underserved
20 areas, and persons with disabilities, is en-
21 couraged.

22 “(v) A definition of the metrics to be
23 used in determining the success of the ef-
24 forts of the regional alliance or partnership
25 under the agreement.

1 “(C) PRIORITY CONSIDERATION.—In
2 awarding financial assistance under paragraph
3 (3), the Director shall give priority consider-
4 ation to a regional alliance or partnership that
5 includes an institution of higher education that
6 is designated as a National Center of Academic
7 Excellence in Cybersecurity or which received
8 an award under the Federal Cyber Scholarship
9 for Service program located in the State or re-
10 gion of the regional alliance or partnership.

11 “(5) AUDITS.—Each cooperative agreement for
12 which financial assistance is awarded under para-
13 graph (3) shall be subject to audit requirements
14 under part 200 of title 2, Code of Federal Regula-
15 tions (relating to uniform administrative require-
16 ments, cost principles, and audit requirements for
17 Federal awards), or successor regulation.

18 “(6) REPORTS.—

19 “(A) IN GENERAL.—Upon completion of a
20 cooperative agreement under paragraph (1), the
21 regional alliance or partnership that partici-
22 pated in the agreement shall submit to the Di-
23 rector a report on the activities of the regional
24 alliance or partnership under the agreement,

1 which may include training and education out-
 2 comes.

3 “(B) CONTENTS.—Each report submitted
 4 under subparagraph (A) by a regional alliance
 5 or partnership shall include the following:

6 “(i) An assessment of efforts made by
 7 the regional alliance or partnership to
 8 carry out paragraph (2).

9 “(ii) The metrics used by the regional
 10 alliance or partnership to measure the suc-
 11 cess of the efforts of the regional alliance
 12 or partnership under the cooperative agree-
 13 ment.”.

14 (g) TRANSFER OF SECTION.—

15 (1) TRANSFER.—Such section is transferred to
 16 the end of title III of such Act and redesignated as
 17 section 303.

18 (2) REPEAL.—Title IV of such Act is repealed.

19 (3) CLERICAL.—The table of contents in sec-
 20 tion 1(b) of such Act is amended—

21 (A) by striking the items relating to title
 22 IV and section 401; and

23 (B) by inserting after the item relating to
 24 section 302 the following:

“Sec. 303. National cybersecurity awareness and education program.”.

25 (4) CONFORMING AMENDMENTS.—

1 (A) Section 302(3) of the Federal Cyberse-
2 curity Workforce Assessment Act of 2015 (5
3 U.S.C. 301 note) is amended by striking
4 “under section 401 of the Cybersecurity En-
5 hancement Act of 2014 (15 U.S.C. 7451)” and
6 inserting “under section 303 of the Cybersecu-
7 rity Enhancement Act of 2014”.

8 (B) Section 2(c)(3) of the NIST Small
9 Business Cybersecurity Act (15 U.S.C. 272
10 note) is amended by striking “under section
11 401 of the Cybersecurity Enhancement Act of
12 2014 (15 U.S.C. 7451)” and inserting “under
13 section 303 of the Cybersecurity Enhancement
14 Act of 2014”.

15 (C) Section 302(f) of the Cybersecurity
16 Enhancement Act of 2014 (15 U.S.C. 7442(f))
17 is amended by striking “under section 401”
18 and inserting “under section 303”.

19 **SEC. 3. DEVELOPMENT OF STANDARDS AND GUIDELINES**
20 **FOR IMPROVING CYBERSECURITY WORK-**
21 **FORCE OF FEDERAL AGENCIES.**

22 (a) IN GENERAL.—Section 20(a) of the National In-
23 stitute of Standards and Technology Act (15 U.S.C.
24 278g–3(a)) is amended—

1 (1) in paragraph (3), by striking “; and” and
2 inserting a semicolon;

3 (2) in paragraph (4), by striking the period at
4 the end and inserting “; and”; and

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

6 “(5) identify and develop standards and guide-
7 lines for improving the cybersecurity workforce for
8 an agency as part of the National Initiative for Cy-
9 bersecurity Education (NICE) Cybersecurity Work-
10 force Framework (NIST Special Publication 800–
11 181), or successor framework.”.

12 (b) PUBLICATION OF STANDARDS AND GUIDELINES
13 ON CYBERSECURITY AWARENESS.—Not later than 3 years
14 after the date of the enactment of this Act and pursuant
15 to section 20 of the National Institute of Standards and
16 Technology Act (15 U.S.C. 278g–3), the Director of the
17 National Institute of Standards and Technology shall pub-
18 lish standards and guidelines for improving cybersecurity
19 awareness of employees and contractors of Federal agen-
20 cies.

21 **SEC. 4. MODIFICATIONS TO FEDERAL CYBER SCHOLAR-**
22 **SHIP-FOR-SERVICE PROGRAM.**

23 Section 302 of the Cybersecurity Enhancement Act
24 of 2014 (15 U.S.C. 7442) is amended—

25 (1) in subsection (b)—

1 (A) in paragraph (2), by striking “infor-
2 mation technology” and inserting “information
3 technology and cybersecurity”;

4 (B) by amending paragraph (3) to read as
5 follows:

6 “(3) prioritize the placement of scholarship re-
7 cipients fulfilling the post-award employment obliga-
8 tion under this section to ensure that—

9 “(A) not less than 70 percent of such re-
10 cipients are placed in an executive agency (as
11 defined in section 105 of title 5, United States
12 Code);

13 “(B) not more than 10 percent of such re-
14 cipients are placed as educators in the field of
15 cybersecurity at qualified institutions of higher
16 education that provide scholarships under this
17 section; and

18 “(C) not more than 20 percent of such re-
19 cipients are placed in positions described in
20 paragraphs (2) through (5) of subsection (d);
21 and”; and

22 (C) in paragraph (4), in the matter pre-
23 ceding subparagraph (A), by inserting “, includ-
24 ing by seeking to provide awards in coordina-
25 tion with other relevant agencies for summer

1 cybersecurity camp or other experiences, includ-
2 ing teacher training, in each of the 50 States,”
3 after “cybersecurity education”;

4 (2) in subsection (d)—

5 (A) in paragraph (4), by striking “or” at
6 the end;

7 (B) in paragraph (5), by striking the pe-
8 riod at the end and inserting “; or”; and

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

10 “(6) as provided by subsection (b)(3)(B), a
11 qualified institution of higher education.”;

12 (3) in subsection (f)—

13 (A) in paragraph (4), by striking “; and”
14 and inserting a semicolon; and

15 (B) by striking paragraph (5) and insert-
16 ing the following:

17 “(5) enter into an agreement accepting and ac-
18 knowledging the post award employment obligations,
19 pursuant to section (d);

20 “(6) accept and acknowledge the conditions of
21 support under section (g); and

22 “(7) accept all terms and conditions of a schol-
23 arship under this section.”;

24 (4) in subsection (g)—

1 (A) in paragraph (1), by inserting “the Of-
2 fice of Personnel Management, in coordination
3 with the National Science Foundation, and” be-
4 fore “the qualified institution”; and

5 (B) in paragraph (2)—

6 (i) in subparagraph (D), by striking
7 “; or” and inserting a semicolon; and

8 (ii) by striking subparagraph (E) and
9 inserting the following:

10 “(E) fails to maintain or fulfill any of the
11 post-graduation or post-award obligations or re-
12 quirements of the individual; or

13 “(F) fails to fulfill the requirements of
14 paragraph (1).”;

15 (5) in subsection (h)(2), by inserting “and the
16 Director of the Office of Personnel Management”
17 after “Foundation”;

18 (6) in subsection (k)(1)(A), by striking “and
19 the Director” and all that follows and inserting “,
20 the Director of the National Science Foundation,
21 and the Director of the Office of Personnel Manage-
22 ment of the amounts owed; and”; and

23 (7) in subsection (m)—

1 (A) in paragraph (1), in the matter pre-
 2 ceding subparagraph (A), by striking “cyber”
 3 and inserting “cybersecurity”; and

4 (B) in paragraph (2), by striking “once
 5 every 3 years” and all that follows and insert-
 6 ing “once every 2 years, to the Committee on
 7 Commerce, Science, and Transportation and the
 8 Committee on Homeland Security and Govern-
 9 mental Affairs of the Senate and the Committee
 10 on Science, Space, and Technology and the
 11 Committee on Oversight and Reform of the
 12 House of Representatives a report, including—

13 “(A) the results of the evaluation under
 14 paragraph (1);

15 “(B) the disparity in any reporting be-
 16 tween scholarship recipients and their respective
 17 institutions of higher education; and

18 “(C) any recent statistics regarding the
 19 size, composition, and educational requirements
 20 of the Federal cybersecurity workforce.”.

21 **SEC. 5. CYBERSECURITY IN PROGRAMS OF THE NATIONAL**
 22 **SCIENCE FOUNDATION.**

23 (a) COMPUTER SCIENCE AND CYBERSECURITY EDU-
 24 CATION RESEARCH.—Section 310 of the American Inno-

1 vation and Competitiveness Act (42 U.S.C. 1862s–7) is
2 amended—

3 (1) in subsection (b)—

4 (A) in paragraph (1), by inserting “and cy-
5 bersecurity” after “computer science”; and

6 (B) in paragraph (2)—

7 (i) in subparagraph (C), by striking “;
8 and” and inserting a semicolon;

9 (ii) in subparagraph (D), by striking
10 the period at the end and inserting “;
11 and”; and

12 (iii) by adding at the end the fol-
13 lowing:

14 “(E) tools and models for the integration
15 of cybersecurity and other interdisciplinary ef-
16 forts into computer science education and com-
17 putational thinking at secondary and postsec-
18 ondary levels of education.”; and

19 (2) in subsection (c), by inserting “, cybersecu-
20 rity,” after “computing”.

21 (b) SCIENTIFIC AND TECHNICAL EDUCATION.—Sec-
22 tion 3(j)(9) of the Scientific and Advanced-Technology Act
23 of 1992 (42 U.S.C. 1862i(j)(9)) is amended by inserting
24 “and cybersecurity” after “computer science”.

1 (c) LOW-INCOME SCHOLARSHIP PROGRAM.—Section
2 414(d) of the American Competitiveness and Workforce
3 Improvement Act of 1998 (42 U.S.C. 1869c) is amend-
4 ed—

5 (1) in paragraph (1), by striking “or computer
6 science” and inserting “computer science, or cyber-
7 security”; and

8 (2) in paragraph (2)(A)(iii), by inserting “cy-
9 bersecurity,” after “computer science,”.

10 (d) PRESIDENTIAL AWARDS FOR TEACHING EXCEL-
11 LENCE.—The Director of the National Science Founda-
12 tion shall ensure that educators and mentors in fields re-
13 lating to cybersecurity can be considered for—

14 (1) Presidential Awards for Excellence in Math-
15 ematics and Science Teaching made under section
16 117 of the National Science Foundation Authoriza-
17 tion Act of 1988 (42 U.S.C. 1881b); and

18 (2) Presidential Awards for Excellence in
19 STEM Mentoring administered under section 307 of
20 the American Innovation and Competitiveness Act
21 (42 U.S.C. 1862s–6).

1 **SEC. 6. CYBERSECURITY IN STEM PROGRAMS OF THE NA-**
2 **TIONAL AERONAUTICS AND SPACE ADMINIS-**
3 **TRATION.**

4 In carrying out any STEM education program of the
5 National Aeronautics and Space Administration (referred
6 to in this section as “NASA”), including a program of
7 the Office of STEM Engagement, the Administrator of
8 NASA shall, to the maximum extent practicable, encour-
9 age the inclusion of cybersecurity education opportunities
10 in such program.

11 **SEC. 7. CYBERSECURITY WORKFORCE DEVELOPMENT AT**
12 **THE DEPARTMENT OF ENERGY.**

13 (a) IN GENERAL.—The Secretary of Energy shall
14 support the development of a cybersecurity workforce
15 through a program that—

16 (1) facilitates collaboration between under-grad-
17 uate and graduate students, researchers at the Na-
18 tional Laboratories (as defined in section 2 of the
19 Energy Policy Act of 2005), and the private sector;

20 (2) prioritizes science and technology in areas
21 relevant to the mission of the Department of Energy
22 through the design and application of cybersecurity
23 technologies;

24 (3) develops, or facilitates private sector devel-
25 opment of, voluntary cybersecurity training and re-
26 training standards, lessons, and recommendations

1 for the energy sector that minimize duplication of
 2 cybersecurity compliance training programs; and

3 (4) maintains a public database of cybersecurity
 4 education, training, and certification programs.

5 (b) COLLABORATION.—In carrying out the program
 6 authorized in subsection (a), the Secretary of Energy shall
 7 leverage programs and activities carried out across the De-
 8 partment of Energy, other relevant Federal agencies, in-
 9 stitutions of higher education, and other appropriate enti-
 10 ties best suited to provide national leadership on cyberse-
 11 curity related issues.

12 **SEC. 8. NATIONAL CYBERSECURITY CHALLENGES.**

13 (a) IN GENERAL.—Title II of the Cybersecurity En-
 14 hancement Act of 2014 (15 U.S.C. 7431 et seq.) is amend-
 15 ed by adding at the end the following:

16 **“SEC. 205. NATIONAL CYBERSECURITY CHALLENGES.**

17 **“(a) ESTABLISHMENT OF NATIONAL CYBERSECU-**
 18 **RITY CHALLENGES.—**

19 **“(1) IN GENERAL.—**To achieve high-priority
 20 breakthroughs in cybersecurity by 2028, the Direc-
 21 tor of the National Institutes of Standards and
 22 Technology shall establish the following national cy-
 23 bersecurity challenges:

24 **“(A) ECONOMICS OF A CYBER ATTACK.—**

25 Building more resilient systems that measur-

ably and exponentially raise adversary costs of carrying out common cyber attacks.

“(B) CYBER TRAINING.—

“(i) Empowering the people of the United States with an appropriate and measurably sufficient level of digital literacy to make safe and secure decisions online.

“(ii) Developing a cybersecurity workforce with measurable skills to protect and maintain information systems.

“(C) EMERGING TECHNOLOGY.—Advancing cybersecurity efforts in response to emerging technology, such as artificial intelligence, quantum science, and next generation communications technologies.

“(D) REIMAGINING DIGITAL IDENTITY.—Maintaining a high sense of usability while improving the privacy, security and safety of online activity of individuals in the United States.

“(E) FEDERAL AGENCY RESILIENCE.—Reducing cybersecurity risks to Federal networks and systems, and improving the response of Federal agencies to cybersecurity incidents on such networks and systems.

1 “(2) COORDINATION.—In establishing the chal-
2 lenges under paragraph (1), the Director of the Na-
3 tional Institutes of Standards and Technology shall
4 coordinate with the Secretary of Homeland Security
5 on the challenges under subparagraphs (B) and (E)
6 of such paragraph.

7 “(b) PURSUIT OF NATIONAL CYBERSECURITY CHAL-
8 LENGES.—

9 “(1) IN GENERAL.—Not later than 180 days
10 after the date of the enactment of this section, the
11 Director of the National Institutes of Standards and
12 Technology, shall commence efforts to pursue the
13 national cybersecurity challenges established under
14 subsection (a).

15 “(2) COMPETITIONS.—The efforts required by
16 paragraph (1) shall include carrying out programs to
17 award prizes, including cash and noncash prizes,
18 competitively pursuant to the authorities and proc-
19 esses established under section 24 of the Stevenson-
20 Wylder Technology Innovation Act of 1980 (15
21 U.S.C. 3719) or any other applicable provision of
22 law.

23 “(3) ADDITIONAL AUTHORITIES.—In carrying
24 out paragraph (1), the Director of the National In-
25 stitutes of Standards and Technology may enter into

1 and perform such other transactions as the Director
2 considers necessary and on such terms as the Direc-
3 tor considers appropriate.

4 “(4) COORDINATION.—In pursuing national cy-
5 bersecurity challenges under paragraph (1), the Di-
6 rector of the National Institutes of Standards and
7 Technology shall coordinate with the following:

8 “(A) The Director of the National Science
9 Foundation.

10 “(B) The Secretary of Homeland Security.

11 “(C) The Director of the Defense Ad-
12 vanced Research Projects Agency.

13 “(D) The Director of the Office of Science
14 and Technology Policy.

15 “(E) The Director of the Office of Man-
16 agement and Budget.

17 “(F) The heads of such other Federal
18 agencies as the Secretary of Commerce con-
19 siders appropriate for purposes of this section.

20 “(5) SOLICITATION OF ACCEPTANCE OF
21 FUNDS.—

22 “(A) IN GENERAL.—Pursuant to section
23 24 of the Stevenson-Wydler Technology Innova-
24 tion Act of 1980 (15 U.S.C. 3719), the Direc-
25 tor of the National Institutes of Standards and

1 Technology shall request and accept funds from
2 other Federal agencies, State, United States
3 territory, local, or tribal government agencies,
4 private sector for-profit entities, and nonprofit
5 entities to support efforts to pursue a national
6 cybersecurity challenge under this section.

7 “(B) RULE OF CONSTRUCTION.—Nothing
8 in subparagraph (A) shall be construed to re-
9 quire any person or entity to provide funds or
10 otherwise participate in an effort or competition
11 under this section.

12 “(c) RECOMMENDATIONS.—

13 “(1) IN GENERAL.—In carrying out this sec-
14 tion, the Director of the National Institutes of
15 Standards and Technology shall designate an advi-
16 sory council to seek recommendations.

17 “(2) ELEMENTS.—The recommendations re-
18 quired by paragraph (1) shall include the following:

19 “(A) A scope for efforts carried out under
20 subsection (b).

21 “(B) Metrics to assess submissions for
22 prizes under competitions carried out under
23 subsection (b) as the submissions pertain to the
24 national cybersecurity challenges established
25 under subsection (a).

1 “(3) NO ADDITIONAL COMPENSATION.—The
2 Director of the National Institutes of Standards and
3 Technology may not provide any additional com-
4 pensation, except for travel expenses, to a member
5 of the advisory council designated under paragraph
6 (1) for participation in the advisory council.”.

7 (b) CONFORMING AMENDMENTS.—Section 201(a)(1)
8 of such Act is amended—

9 (1) in subparagraph (J), by striking “; and”
10 and inserting a semicolon;

11 (2) by redesignating subparagraph (K) as sub-
12 paragraph (L); and

13 (3) by inserting after subparagraph (J) the fol-
14 lowing:

15 “(K) implementation of section 205
16 through research and development on the topics
17 identified under subsection (a) of such section;
18 and”.

19 (c) CLERICAL AMENDMENT.—The table of contents
20 in section 1(b) of such Act is amended by inserting after
21 the item relating to section 204 the following:

“Sec. 205. National cybersecurity challenges.”.

○