

.....
(Original Signature of Member)

117TH CONGRESS
2D SESSION

H. R.

To provide funding to strengthen cybersecurity defenses and capabilities by expanding community colleges programs leading to the award of cybersecurity credentials that are in demand in government, critical infrastructure, nonprofit, and private sectors, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Mrs. McCLAIN (for herself and Ms. CLARKE of New York) introduced the following bill; which was referred to the Committee on

A BILL

To provide funding to strengthen cybersecurity defenses and capabilities by expanding community colleges programs leading to the award of cybersecurity credentials that are in demand in government, critical infrastructure, nonprofit, and private sectors, 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 “National Community
5 College Cybersecurity Challenge Act”.

1 **SEC. 2. DEFINITIONS.**

2 In this Act:

3 (1) **COMMUNITY COLLEGE.**—The term “commu-
4 nity college” means a public institution of higher
5 education at which the highest degree that is pre-
6 dominantly awarded to students is an associate’s de-
7 gree, including a 2-year Tribal College or University
8 (as defined in section 316 of the Higher Education
9 Act of 1965 (20 U.S.C. 1059e)), and public 2-year
10 institutions of higher education.

11 (2) **ELIGIBLE ENTITY.**—The term “eligible enti-
12 ty” means—

13 (A) a community college;

14 (B) a public or private entity with exper-
15 tise related to cybersecurity education, and pro-
16 fessional development; or

17 (C) a consortium of entities described in
18 subparagraphs (A) and (B), including a con-
19 sortia of community colleges at the local, State
20 or national level.

21 (3) **IN-DEMAND CYBERSECURITY SKILLS AND**
22 **CERTIFICATIONS.**—The term “in-demand cybersecu-
23 rity skills and certifications” means skills and cer-
24 tifications most sought after by employers of cyber-
25 security professionals, as identified by the Secretary
26 in consultation with the Secretary of Labor, the Sec-

1 retary of Commerce, and the Secretary of Homeland
2 Security, and reflected in publicly reported data, in-
3 cluding from the National Initiative for Cybersecu-
4 rity Education (NICE) and other Federal, State and
5 local sources.

6 (4) INSTITUTION OF HIGHER EDUCATION.—The
7 term “institution of higher education” has the
8 meaning given such term in section 101(a) of the
9 Higher Education Act of 1965 (20 U.S.C. 1001(a)).

10 (5) RECOGNIZED CYBERSECURITY CREDEN-
11 TIAL.—The term “recognized cybersecurity creden-
12 tial” means an industry-recognized certificate or cer-
13 tification, associate’s degree or bachelor’s degree in
14 the field of cybersecurity.

15 (6) SECRETARY.—The term “Secretary” means
16 the Secretary of Education.

17 (7) STATE.—The term “State” includes, in ad-
18 dition to the several States of the United States, the
19 Commonwealth of Puerto Rico, the District of Co-
20 lumbia, Guam, American Samoa, the United States
21 Virgin Islands, the Commonwealth of the Northern
22 Mariana Islands, and the Freely Associated States.

23 (8) UNDERREPRESENTED POPULATIONS.—The
24 term “underrepresented populations” means—

1 (A) a minority group whose number of cy-
2 bersecurity professionals per 10,000 population
3 of that group is substantially below the com-
4 parable figure for cybersecurity professionals
5 who are white and not of Hispanic origin;

6 (B) Populations residing in geographical
7 area in which there is no community college
8 which offers a cybersecurity associate's degree;
9 and

10 (C) Any other group identified by the Sec-
11 retary, such as veterans and individuals with
12 disabilities, as underrepresented in cybersecu-
13 rity.

14 **SEC. 3. CYBERSECURITY COMMUNITY COLLEGE CHAL-**
15 **LENGE FUND.**

16 (a) GRANTS AUTHORIZED.—From funds appro-
17 priated under subsection (i), the Secretary shall award
18 competitive challenge grants to States to carry out the ac-
19 tivities described in subsection (e).

20 (b) APPLICATION.—A State desiring a grant under
21 this section shall submit to the Secretary an application
22 at such time, in such manner, and containing such infor-
23 mation as the Secretary determines is required. The appli-
24 cation shall include—

1 (1) a plan for how the State will increase the
2 number of skilled cybersecurity faculty at community
3 colleges within the State, by supporting efforts
4 which at a minimum shall include—

5 (A) recruiting and placing cybersecurity
6 professionals from industry to teach in-demand
7 cybersecurity courses, with a demonstrated path
8 to increasing the number professionals with in-
9 dustry experience teaching at community col-
10 leges and increasing the number of and quality
11 of cybersecurity course offerings;

12 (B) enhancing the professional develop-
13 ment for permanent and adjunct faculty teach-
14 ing cybersecurity courses within the community
15 college system related to the most in-demand
16 cybersecurity skills and certifications, including
17 through rotational or shadowing opportunities
18 in private industry, opportunities for participa-
19 tion in communities of practice, exposure to rel-
20 evant, up-to-date curriculum and providing op-
21 portunities for other relevant learning opportu-
22 nities; and

23 (C) increasing the number of community
24 colleges in the State designated as a National
25 Center of Academic Excellence in Cybersecu-

1 rity, in order to support the professional devel-
2 opment of faculty and improve the quality of
3 cybersecurity programs;

4 (2) a plan for how the State will increase the
5 number of individuals within the State obtaining a
6 cybersecurity associate's degree and in-demand cy-
7 bersecurity skills and certifications, including how
8 the State will—

9 (A) ensure students at every community
10 college within the State are able to enroll in a
11 cybersecurity degree program at the college
12 they attend or through distance education in
13 partnership with another community college.
14 Such programs may also be offered through
15 dual enrollment;

16 (B) ensure graduation requirements for
17 students pursuing an associate's degree in tech-
18 nology or computer science include completion
19 of fundamental cybersecurity coursework; and

20 (C) enable more individuals, especially low-
21 and moderate-income students and students
22 from underrepresented populations, to obtain
23 associate's degrees and credentials in cybersecu-
24 rity, through scholarships, incentives, and sup-
25 port;

1 (3) a plan for how the State will support the ef-
2 forts of community colleges to build connections to
3 real-world cybersecurity work-based experiences and
4 job opportunities for students, including by—

5 (A) establishing public-private partnerships
6 that provide work-based experiences for stu-
7 dents in order for them to gain in-demand cy-
8 bersecurity skills and certifications;

9 (B) connecting students to work-based
10 learning experiences, as well as pathways to
11 continue further education, including bachelors'
12 degrees and pathways to employment; and

13 (C) encourage community colleges to re-
14 view and update the curriculum and courses
15 within their cybersecurity associate's degree
16 programs to ensure they reflect in-demand cy-
17 bersecurity skills and certifications and work-
18 force opportunities;

19 (4) a plan for how the State will annually col-
20 lect, make publicly available, and report to the Sec-
21 retary—

22 (A) the extent to which the State has made
23 progress in implementing the plans, and is
24 meeting the goals, described in paragraphs (1)
25 through (3); and

1 (B) data on cybersecurity skills attainment
2 across the State's community colleges,
3 disaggregated by race, ethnicity and sex, and
4 other relevant factors including—

5 (i) the number of students currently
6 enrolled in a cybersecurity associate's de-
7 gree program;

8 (ii) the number of cybersecurity asso-
9 ciate's degrees conferred during the most
10 recent year;

11 (iii) the percentage and number of
12 graduates of programs leading to a cyber-
13 security associate's degree who are placed
14 into a cybersecurity profession within 6
15 months; and

16 (iv) the number and types of cyberse-
17 curity courses and non-degree credentials
18 completed; and

19 (5) an identification of the amounts the State
20 plans to expend to achieve the goals described in
21 paragraphs (1) through (3).

22 (c) USE OF FUNDS.—A State receiving a grant under
23 this section shall use grant funds for carrying out the ac-
24 tivities described in the State's approved plan under sub-

1 section (b), which may include the awarding of subgrants
2 to eligible entities.

3 (d) AMOUNT OF GRANT.—The amount of a grant
4 awarded to a State under subsection (a) shall be deter-
5 mined by the Secretary, taking into account the population
6 of the eligible State and the amount of funds identified
7 by the State under subsection (b)(5).

8 (e) MATCHING FUNDS.—

9 (1) IN GENERAL.—Except as provided under
10 paragraph (2), to receive a grant under this section
11 a State shall, through cash or in-kind contributions,
12 provide matching funds from non-Federal sources in
13 an amount equal to not less than 50 percent of the
14 funds provided under such grant.

15 (2) EXCEPTION.—The Secretary may waive the
16 matching fund requirement under subparagraph (1)
17 if the State demonstrates exceptional circumstances.

18 (f) LIMITATION.—The Secretary may not award more
19 than one grant under this section to any State.

20 (g) CONSULTATION.—In awarding grants under sub-
21 section (a) and in developing the application in subsection
22 (b), the Secretary shall consult with—

- 23 (1) the Secretary of Labor;
- 24 (2) the Secretary of Commerce; and
- 25 (3) the Secretary of Homeland Security.

1 (i) AUTHORIZATION OF APPROPRIATIONS.—There
2 are appropriated to carry out this section, to the extent
3 funds are made available pursuant to section 6,
4 \$250,000,000 million for each of fiscal years 2023
5 through 2027.

6 **SEC. 4. NATIONAL CYBERSECURITY WORKFORCE INNOVA-**
7 **TION FUND.**

8 (a) GRANTS AUTHORIZED.—From funds appro-
9 priated under subsection (e), the Secretary shall award
10 competitive grants to eligible entities to enable such enti-
11 ties to develop and implement innovative strategies to as-
12 sist States to accomplish the goals of section 3.

13 (b) APPLICATION.—An eligible entity desiring a grant
14 under this section shall submit to the Secretary, an appli-
15 cation at such time, in such manner, and containing such
16 information as the Secretary determine is required. The
17 application shall—

18 (1) include a description of the strategy to be
19 used to maximize the impact of funds toward meet-
20 ing the goals of section 3;

21 (2) include a description of how the strategy
22 will be sustained after the grant period; and

23 (3) provide information detailing the number of
24 students who would be served under the initiative

1 and the intended impact and overall goals of the ini-
2 tiative.

3 (c) PRIORITY.—In awarding grants under this sec-
4 tion, the Secretary shall give priority to applications from
5 eligible entities that will assist students from underrep-
6 resented populations obtain a cybersecurity associate’s de-
7 gree and provide such students with work-based opportu-
8 nities related to cybersecurity.

9 (d) USE OF FUNDS.—An eligible entity that is
10 awarded a grant under this section shall use the grant
11 funds to create, develop, implement, replicate, or take to
12 scale evidence-based innovations to accomplish the goals
13 of section 3 through activities such as—

14 (1) public-private partnerships—

15 (A) to help fill the industry-experienced
16 faculty gap by connecting industry and tech-
17 nology professionals (“Cyber Pros”) to teach
18 cybersecurity courses, including through dis-
19 tance education, at community colleges, with a
20 focus on underserved urban and rural settings;
21 and

22 (B) through which Cyber Pros would re-
23 ceive professional development to prepare them
24 for the classroom and be matched to community
25 colleges to teach cybersecurity courses; and

1 (2) establishing work-based initiatives through
2 regional public-private partnerships which are able
3 to develop, at scale, opportunities for individuals to
4 access work-based learning and move into cybersecu-
5 rity jobs.

6 (e) MATCHING FUNDS.—

7 (1) IN GENERAL.—Except as provided under
8 paragraph (2), to receive a grant under this section
9 an eligible entity shall, through cash or in-kind con-
10 tributions, provide matching funds from non-Federal
11 sources in an amount equal to not less than 50 per-
12 cent of the funds provided under such grant.

13 (2) EXCEPTION.—The Secretary may waive the
14 matching fund requirement under subparagraph (1)
15 if the eligible entity demonstrates exceptional cir-
16 cumstances.

17 (f) AUTHORIZATION OF APPROPRIATIONS.—There
18 are appropriated to carry out this section, to the extent
19 funds are made available pursuant to section 6,
20 \$150,000,000 million for fiscal year 2023, to remain avail-
21 able through the last day of fiscal year 2027.

1 **SEC. 5. FEDERAL CYBER SCHOLARSHIP-FOR-SERVICE PRO-**
2 **GRAM.**

3 Section 302(b)(3) of the Cybersecurity Enhancement
4 Act of 2014 (15 U.S.C. 7442(b)(3)) is amended by strik-
5 ing subparagraph (B) and inserting the following:

6 “(B) not more than 10 percent of such re-
7 cipients are placed as educators in the field of
8 cybersecurity at qualified institutions of higher
9 education; and”.

10 **SEC. 6. RESCISSIONS.**

11 Of the unobligated balances from amounts made
12 available in the Coronavirus Aid, Relief, and Economic Se-
13 curity Act (Public Law 116-136) or the Coronavirus Re-
14 sponse and Relief Supplemental Appropriations Act, 2021
15 (division M of Public Law 116-260)—

16 (1) for fiscal year 2023, \$400,000,000 is hereby
17 permanently rescinded; and

18 (2) for each of fiscal years 2024 through 2027,
19 \$250,000,000 is hereby permanently rescinded.