I

117TH CONGRESS
2D SESSION

H. R. 8970

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

SEPTEMBER 22, 2022

Mrs. MCCLAIN (for herself and Ms. CLARKE of New York) introduced the following bill; which was referred to the Committee on Education and Labor, and in addition to the Committees on Science, Space, and Technology, and Appropriations, 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 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.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''National Community College Cybersecurity Challenge Act''.

SEC. 2. DEFINITIONS.

In this Act:

(1) COMMUNITY COLLEGE.—The term ''community college'' means a public institution of higher education at which the highest degree that is predominantly awarded to students is an associate's degree, including a 2-year Tribal College or University (as defined in section 316 of the Higher Education Act of 1965 (20 U.S.C. 1059c)), and public 2-year institutions of higher education.

(2) ELIGIBLE ENTITY.—The term ''eligible entity'' means—

(A) a community college;

(B) a public or private entity with expertise related to cybersecurity education, and professional development; or

(C) a consortium of entities described in subparagraphs (A) and (B), including a consortia of community colleges at the local, State or national level.

(3) IN-DEMAND CYBERSECURITY SKILLS AND CERTIFICATIONS.—The term ''in-demand cybersecurity skills and certifications'' means skills and certifications most sought after by employers of cybersecurity professionals, as identified by the Secretary in consultation with the Secretary of Labor, the Sec-

retary of Commerce, and the Secretary of Homeland Security, and reflected in publicly reported data, including from the National Initiative for Cybersecurity Education (NICE) and other Federal, State, and local sources.

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

(5) RECOGNIZED CYBERSECURITY CREDENTIAL.—The term ''recognized cybersecurity credential'' means an industry-recognized certificate or certification, associate's degree or bachelor's degree in the field of cybersecurity.

(6) SECRETARY.—The term ''Secretary'' means the Secretary of Education.

(7) STATE.—The term ''State'' includes, in addition to the several States of the United States, the Commonwealth of Puerto Rico, the District of Columbia, Guam, American Samoa, the United States Virgin Islands, the Commonwealth of the Northern Mariana Islands, and the Freely Associated States.

(8) UNDERREPRESENTED POPULATIONS.—The term ''underrepresented populations'' means—

(A) a minority group whose number of cybersecurity professionals per 10,000 population of that group is substantially below the comparable figure for cybersecurity professionals who are White and not of Hispanic origin;

(B) populations residing in geographical area in which there is no community college which offers a cybersecurity associate's degree; and

(C) any other group identified by the Secretary, such as veterans and individuals with disabilities, as underrepresented in cybersecurity.

SEC. 3. CYBERSECURITY COMMUNITY COLLEGE CHALLENGE FUND.

(a) GRANTS AUTHORIZED.—From funds appropriated under subsection (i), the Secretary shall award competitive challenge grants to States to carry out the activities described in subsection (c).

(b) APPLICATION.—A State desiring a grant under this section shall submit to the Secretary an application at such time, in such manner, and containing such information as the Secretary determines is required. The application shall include—

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

(A) recruiting and placing cybersecurity professionals from industry to teach in-demand cybersecurity courses, with a demonstrated path to increasing the number professionals with industry experience teaching at community colleges and increasing the number of and quality of cybersecurity course offerings;

(B) enhancing the professional development for permanent and adjunct faculty teaching cybersecurity courses within the community college system related to the most in-demand cybersecurity skills and certifications, including through rotational or shadowing opportunities in private industry, opportunities for participation in communities of practice, exposure to relevant, up-to-date curriculum and providing opportunities for other relevant learning opportunities; and

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

rity, in order to support the professional development of faculty and improve the quality of cybersecurity programs;

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

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

(B) ensure graduation requirements for students pursuing an associate's degree in technology or computer science include completion of fundamental cybersecurity coursework; and

(C) enable more individuals, especially low- and moderate-income students and students from underrepresented populations, to obtain associate's degrees and credentials in cybersecurity, through scholarships, incentives, and support;

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

(A) establishing public-private partnerships that provide work-based experiences for students in order for them to gain in-demand cybersecurity skills and certifications;

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

(C) encourage community colleges to review and update the curriculum and courses within their cybersecurity associate's degree programs to ensure they reflect in-demand cybersecurity skills and certifications and workforce opportunities;

(4) a plan for how the State will annually collect, make publicly available, and report to the Secretary—

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

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

(i) the number of students currently enrolled in a cybersecurity associate's degree program;

(ii) the number of cybersecurity associate's degrees conferred during the most recent year;

(iii) the percentage and number of graduates of programs leading to a cybersecurity associate's degree who are placed into a cybersecurity profession within 6 months; and

(iv) the number and types of cybersecurity courses and non-degree credentials completed; and

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

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

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

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

(e) MATCHING FUNDS.—

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

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

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

(g) CONSULTATION.—In awarding grants under subsection (a) and in developing the application in subsection (b), the Secretary shall consult with—

(1) the Secretary of Labor;

(2) the Secretary of Commerce; and

(3) the Secretary of Homeland Security.

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

SEC. 4. NATIONAL CYBERSECURITY WORKFORCE INNOVATION FUND.

(a) GRANTS AUTHORIZED.—From funds appropriated under subsection (e), the Secretary shall award competitive grants to eligible entities to enable such entities to develop and implement innovative strategies to assist States to accomplish the goals of section 3.

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

(1) include a description of the strategy to be used to maximize the impact of funds toward meeting the goals of section 3;

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

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

and the intended impact and overall goals of the initiative.

(c) PRIORITY.—In awarding grants under this section, the Secretary shall give priority to applications from eligible entities that will assist students from underrepresented populations obtain a cybersecurity associate's degree and provide such students with work-based opportunities related to cybersecurity.

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

(1) public-private partnerships—

(A) to help fill the industry-experienced faculty gap by connecting industry and technology professionals (''Cyber Pros'') to teach cybersecurity courses, including through distance education, at community colleges, with a focus on underserved urban and rural settings; and

(B) through which Cyber Pros would receive professional development to prepare them for the classroom and be matched to community colleges to teach cybersecurity courses; and

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

(e) MATCHING FUNDS.—

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

(2) EXCEPTION.—The Secretary may waive the matching fund requirement under paragraph (1) if the eligible entity demonstrates exceptional circumstances.

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

SEC. 5. FEDERAL CYBER SCHOLARSHIP-FOR-SERVICE PROGRAM.

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

''(B) not more than 10 percent of such recipients are placed as educators in the field of cybersecurity at qualified institutions of higher education; and''.

SEC. 6. RESCISSIONS.

Of the unobligated balances from amounts made available in the Coronavirus Aid, Relief, and Economic Security Act (Public Law 116–136) or the Coronavirus Response and Relief Supplemental Appropriations Act, 2021 (division M of Public Law 116–260)—

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

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

○