

Date of Hearing: April 25, 2023

ASSEMBLY COMMITTEE ON HIGHER EDUCATION
Mike Fong, Chair
AB 569 (Garcia) – As Amended March 16, 2023

SUBJECT: California State University: Cybersecurity Regional Alliances and Multistakeholder Partnerships Pilot Program

SUMMARY: This bill requires that the Chancellor of the California State University (CSU) report to the Legislature on the Cybersecurity Regional Alliances and Multistakeholder Partnerships Pilot Program with specified program data and recommendations on how to improve the program. Specifically, **this bill:**

- 1) Requires that on or before July 1, 2028, the Office of the Chancellor of the CSU submit a comprehensive report to the legislature on the Cybersecurity Regional Alliances and Multistakeholder Partnerships Pilot Program.
- 2) Specifies that the report must include:
 - a) Recommendations on how to improve the pilot program;
 - b) Data on enrollment in the pilot program;
 - c) Data on how many different groups of people have been served by the pilot program;
 - d) Data on the number of veterans that have participated in the pilot program; and,
 - e) Recommendations on how to recruit more veterans to participate in the pilot program.
- 3) States that the reporting requirement imposed by the bill is rendered inoperative on July 1, 2032, pursuant to Section 10231.5 of the Government Code.

EXISTING LAW:

- 1) Establishes the Cybersecurity Regional Alliances and Multistakeholder Partnerships Pilot Program in order to address the cybersecurity workforce gap by doing all of the following:
 - a) Stimulating cybersecurity education and workforce development by bringing together stakeholders in the cybersecurity ecosystem;
 - b) Aligning the cybersecurity workforce needs of employers with the education and training provided by institutions of higher education;
 - c) Increasing the pipeline of students pursuing cybersecurity careers; and,
 - d) Developing the cybersecurity workforce to meet industry needs within local or regional economies. (Education Code (EDC) Section 89270)

- 2) Requires that on or before March 1, 2023, the office of the Chancellor of the California State University develop an application process, selection process, and criteria for California State University campuses seeking to participate in the pilot program, with preference given to California State University campuses that have or are developing regional pipeline programs in cybersecurity with the California Community Colleges. (EDC Section 89270)
- 3) Requires the office of the Chancellor of the California State University to select any number of campuses to participate in the pilot program. (EDC Section 89270)
- 4) Requires that each selected California State University campus do all of the following:
 - a) Create a pilot program with goals and metrics;
 - b) Develop strategies and tactics for building successful regional alliances and multistakeholder partnerships; and,
 - c) Measure the impact and results of its pilot program and annually share the impact and results with the office of the Chancellor of the California State University. (EDC Section 89270)
- 5) Requires the office of the Chancellor of the California State University to annually report the impact and results from each selected campus's pilot program to the Legislature. (EDC Section 89270)

FISCAL EFFECT: Unknown.

COMMENTS: *Purpose.* According to the author, “cybersecurity and privacy issues are quickly moving to the forefront of homeland security, state priorities, and state-federal policies. State legislatures have taken major action to bolster the cybersecurity of their infrastructure amid new and increasing threats. Some measures have sought to increase cybersecurity investments from the public and private sector, or create or expand state agency authorities to better deal with cyber threats. These investments should also include developing a well-trained workforce to meet the demand for cybersecurity experts. Veterans and transitioning military personnel who served and protected the nation are very well positioned to transition into these open cybersecurity jobs.”

Background. According to the California Cybersecurity Workforce Development and Education Strategy published in September 2020, “global demand for cybersecurity and information security professionals and personnel has been mounting for decades and reaching a critical point. It is imperative in this modern and information-rich era to have a strong cadre of qualified and prepared cybersecurity specialists and specialized workforce (from technicians through managers) flowing into the labor pool. Based on the reliance of technology in today’s digital environment, we need coordinated and linked education, training, and workforce development programs to increase statewide cybersecurity capabilities and enhance cyber-resiliency.”

In September 2016, the National Initiative for Cybersecurity Education, led by the National Institute of Standards and Technology in the U.S. Department of Commerce, awarded funding for five pilot programs for Regional Alliances and Multistakeholder Partnerships to Stimulate Cybersecurity Education and Workforce Development. Through this federal funding

opportunity, it was found that effective multi-stakeholder workforce partnerships focused on organizing multiple employers with skill shortages in specific occupations to focus on developing the skilled workforce to meet industry needs within the local or regional economy. It was also found that bringing together multiple stakeholders in the cybersecurity ecosystem – industry, government, and educational institutions – can help communities address many of the cybersecurity workforce challenges that they face today.

Cybersecurity collaboration. The September 2020 California Cybersecurity Workforce Development and Education Strategy report describes the design, development, and implementation phases of the California Cybersecurity Career Education Pipeline and Pathway Project (CCCEPPP) to transform statewide cyber education and workforce development. The CCCEPPP is an initiative of the California Cybersecurity Task Force (CCTF) Workforce Development and Education Subcommittee (WDE).

The strategy report noted that, “the California Cybersecurity Workforce Development and Education Strategy discusses the alignment and coordination of cybersecurity K-12 and Higher Education model curriculum, academic standards, extra-curricular activities, cyber competitions, professional/career development, apprenticeships, and related areas to build a solid, linked cybersecurity pipeline/pathway to serve the State of California. To be successful, public and private sector key partners/major stakeholders must collaborate and work together earnestly to design education and workforce development programs that assure prospective employers program graduates can demonstrate the necessary knowledge, skills, abilities, and competencies to meet minimum job requirements upon pipeline/pathway completion and graduation.”

Committee comments. The pilot program implemented in the 2022-2023 State Budget, which granted \$4 million one-time, has the potential to align local industry with students pursuing cybersecurity careers, and does including annual reporting requirements. Yet the pilot program does not include a comprehensive report capturing best practices. AB 569 (Garcia) looks to bridge the gap between annual reporting and a true comprehensive report that could better prepare CSU to scale up these programs in the future.

Prior legislation. AB 2695 (Berman, 2022) would have established the Cybersecurity Regional Alliances and Multistakeholder Partnerships pilot program described above. Held in Assembly Appropriations, the bill’s content was included in the budget trailer bill AB 183, which was signed by the Governor.

REGISTERED SUPPORT / OPPOSITION:

Support

California Chamber of Commerce

Opposition

None on file

Analysis Prepared by: Kevin J. Powers / HIGHER ED. / (916) 319-3960