COLORADO
Department of
Higher Education

REPORT ON THE IMPLEMENTATION OF SB 18-086

1600 Broadway, Suite 2200 • Denver, Colorado 80202 • (303) 862-3001

Overview

C.R.S. 24-33.5-1905 (4) directs the Department of Higher Education (DHE, the Department) to prepare a report detailing progress made towards critical state cyber-security goals at institutions of higher education that received an appropriation through SB 18-086. Specifically, the report must include, at a minimum:

1. The number of faculty or adjunct faculty hired at each institution of higher education as a result of the funding;
2. The number of student internships created with the funding at each institution of higher education;
3. The number of degrees or certificates that have been awarded at each institution of higher education in connection with the funding;
4. The number of scholarships awarded at each institution in connection with the funding;
5. The number of presentations and seminars given on cybersecurity by each institution of higher education; and
6. The amount of all other money that has been raised to match the state investment, which may include tuition, fees, federal funds, and industry donations.

Six governing boards were awarded funding in the 2018-19 fiscal year through the enacting legislation, SB 18-086. The following report summarizes their spending.

Key Findings

Fiscal Year 2018-19 was the first year in which funding was awarded to support cybersecurity and distributed ledger technology activities at institutions. Because this was the first year, and because funding was awarded midway through the academic year, institutions were limited in the amount of time they had to implement activities based on the new funding.

Table 1 summarizes spending on activities related to cybersecurity and distributed ledger technologies, as supported by SB 18-086 funding, including the amount spent on scholarships and whether each governing board provided the required amount of funding earmarked towards scholarships.

	SB 18-086 Appropriation	Total Amount Expended	SB 18-086 Scholarship Requirement	Total Amount Spent on Scholarships
Colorado Mesa University	$300,000	$273,269	$30,000	$29,900
Metropolitan State University of Denver	$300,000	$23,793	$30,000	$9,000
Western State Colorado University	$200,000	$157,909	$20,000	$20,000
Colorado State University System	$1,200,000	$812,024	$180,000	$122,435
University of Colorado System	$2,800,000	$2,800,000	$420,000	$585,475
Colorado Community College System	$300,000	$300,000	$30,000	$30,000

Fiscal Year (FY) 2018-19 was the first year in which institutions received this funding, and several programs required a longer period of implementation. As institutions continue to receive funding to support cybersecurity programs, the amount of programming they are able to offer will likely increase. Institutions that did not expend their full appropriation in the initial year of funding plan to use the remainder of the funding for scholarships, operating expenses, and facilities investments in Fiscal Year 2020.

Table 2 summarizes activities funded by SB 18-086 funding.

	Faculty and Adjuncts Hired	**Internships Created**	**Degrees and Certificates Awarded**	**Scholarships Awarded**	**Presentations and Seminars Given**	**Amount of Other Funding Raised**
Colorado Mesa University	1.6	21	7	23	67	$0
Metropolitan State University of Denver	3	10	0	15	1	$45,703
Western Colorado University	1.4	0	0	5	1	$0
Colorado State University System	2	29	14	76	73	$0
University of Colorado System	6	18	141	488	50	$3,984,642
Colorado Community College System	1	1	16	24	4	$50,000

Institutions used the funds received to support a wide range of activities. Many, such as faculty and staff hiring and direct support for cyber programs, are summarized above. Institutions also participated in a range of public-facing activities with support from SB 18-086 funding, including but not limited to:

- The University of Colorado at Colorado Springs sponsored, and Pikes Peak Community College hosted, a hacker competition training provided by the cybersecurity training company SecureSet. Collaboration between the two institutions and helped facilitate participation in the public event and helped strengthen a strategic cybersecurity partnership with industry and between institutions of higher education.
- In addition to collaborating with Pikes Peak Community college, the University of Colorado at Colorado Springs participated in the following outreach activities:
    - UCCS sponsored the Mountain West Cybersecurity Consortium spring conference, a two-day event attended by twenty-five participants representing ten institutions of higher education from Colorado and New Mexico. This event provided the opportunity to present research, share insights, and build collaboration.
    - The Office of Online and Academic Outreach delivered a one-week training program helping area high school teachers prepare to teach introductory computer programming. The course not only expanded cybersecurity workforce

capacity in Colorado high schools, it also met a critical requirement for K-12 teachers to maintain certifications.
    - UCCS has a Memorandum of Understanding with the National Cybersecurity Center and leverages the state's investment through this partnership.
- At Pikes Peak Community College, cybersecurity students and faculty participated in local, regional, and national events including the following:
    - Students presented to community affiliates on program activities at the PPCC Cyber Security Advisory Board.
    - Faculty served as panelists at the Center for Cybersecurity's Executive Leadership forum.
    - Both students and faculty traveled to present and participate in seminars at the Cyber Maryland national conference and competition, in which PPCC students placed nationally.
- Colorado State University – Pueblo hosted a summer workshop with 25 middle school students in collaboration with the Cyber Institute and participated in cybersecurity competitions with over 60 high school, community college, and CSU Pueblo students.
- Western Colorado University hosted a high school cyber security camp.
- Students at Colorado Mesa University participated in a panel discussion for new businesses, and visited schools ranging from elementary to high school to demonstrate cyber issues. They also held a panel discussion for a Techstars West Slope Session.
- Cybersecurity faculty at Colorado Mesa University presented slides on cybersecurity in aerospace to the Fruita Middle School student body as part of a code.org "hour of code" event and led a discussion on cybersecurity in business for the Palisade Rotary Club.

Several institutions leveraged SB 18-086 funding to raise funds from other sources:

- The National Science Foundation (NSF) announced that UCCS was awarded a five-year, $3.08M grant under the Scholarship for Service (SFS) program. UCCS is the first Colorado institution of higher education to earn this prestigious award. SFS will provide additional scholarships to cybersecurity students, including stipends and travel. Upon graduation, scholarship recipients must accept jobs with the Federal government, and work one year for every year they received their scholarship. The SFS significantly builds on the SB18-086 requirements for cybersecurity scholarships. Additional partnerships through the National Cybersecurity Center have also raised money. A few examples include the Daniels Fund for workforce development ($100,000), the Tusk Montgomery Philanthropies funding to help advance secure voting programs ($200,200), as well as VISA for cybersecurity issues ($375,000).
- Metropolitan State University of Denver raised $45,703 in additional funds to support a teacher certificate training program.
- The Pikes Peak Community College foundation raised $50,000 from the Armed Forces Communications and Electronics Association for Cyber Security education. These monies qualified for matching funds from the Colorado Opportunity Scholarship Initiative (COSI) for a total impact of $100,000.

In addition to the categories outlined in the law, several institutions elected to spend SB 18-086 funding to develop or otherwise support facilities related to cybersecurity. Projects outlined to the Department included:

- The Colorado Community College System invested SB 18-086 funds in infrastructure to support the development of a state-of-the-art Network Operations Center (NOC) on the Pikes Peak Community College Rampart Range campus. This facility is designed to simulate a centralized location where cybersecurity professionals monitor and maintain security for network clients, similar to what graduates would encounter in industry positions. Investments included the purchase of networking servers and installations, which allow the NOC to operate on a secure network outside of the college's existing infrastructure, preventing any malicious code used in training from infecting the college's networks. A multiscreen video wall allowing for multiple visual displays for students engaged in scenario-based cybersecurity training was also purchased.
- At CSU Pueblo, a Systems Cyber Laboratory is being created to facilitate exploring cybersecurity of complex systems and components. The use of digital twins of actual systems allows for testing and resolving cybersecurity issues in complex systems.
- Metropolitan State University of Denver is also in the process of building a cybersecurity lab that is currently in the planning stage with Lockheed Martin and other companies. The university is also seeking additional matching funds to contribute to the development of the lab.
- Colorado Mesa University purchased a server that students set up with a firewall and created virtual machines for use as a "sandbox" for student research projects.

Failure to Meet Financial Aid Requirements

C.R.S. 24-33.5-1905 (4)(b) reads:

The governing board of each institution of higher education participating in activities related to cybersecurity and distributed ledger technologies shall ensure that at least the following percentages of the money allocated to the institution pursuant to subsection (4)(a) of this section is used to provide scholarships to students at the institution who are doing work in connection with cybersecurity and distributed ledger technologies:

> *(I) For an institution of higher education receiving one million dollars or more pursuant to subsection (4)(a) of this section, for the first three years that the institution receives said money, the institution must ensure that at least fifteen percent of the money received is used to provide said scholarships. For the fourth and subsequent years of funding, the institution shall ensure that at least twenty percent of the money received is used to provide said scholarships; except that, for the five percent increase from years three to four, the institution may use private donations to account for the increase.*

> *(II) For an institution receiving less than one million dollars pursuant to subsection (4)(a) of this section, the institution must ensure that at least ten percent of the money received is used to provide said scholarships.*

Three institutions failed to meet the statutory requirements around the percentage of financial aid they were required to award based on the amount of funding received. At both institutions, there was no preexisting cybersecurity program; since the bill passed midway through the academic year they had a limited time frame in which to recruit scholarship candidates. In the next fiscal year, both governing boards fully expect to be able to award the full amount in required scholarship funds. Below are their responses as to why they were unable to offer the required amount of scholarship funding in year one.

Metropolitan State University of Denver received a total appropriation of $300,000, resulting in a scholarship requirement of $30,000. The university provided $9,000 in scholarships in FY 2018-19. Per the department of cybersecurity at the institution, they were unable to award the full scholarship requirement because "it took a semester to create [the] scholarship. It is a first-year program, but it has tripled in size. We had approximately 47 majors the first semester the B.S. was offered, and since the scholarships were offered to [students] other than freshman, not many qualified. We are on track to have 3-4 times (150-200 majors) the number of students in for FY20, so the amount of scholarships will triple as well, along with a Master's program with 17 graduate students starting in FY20. We expect scholarships to exceed the $30,000 minimum requirements."

The Colorado State University System received a total appropriation of $1,200,000, of which $180,000 was required to be devoted to scholarships. The university provided $122,435 in scholarships in FY 2018-19. Per the system office, the scholarship amount was lower than required because "[CSU was] a bit slow getting started, especially in hiring staff and faculty, including one failed faculty search. Students followed those hires, so [CSU was] in start-up mode for scholarships and internships as well." The institution states that they are operating at a close to steady state now and plan to utilize all of the funding and the carry-over in FY 2019-20.

In both cases, the primary reason for failure to meet the scholarship requirement was that both institutions were still in the process of setting their programs up in Academic Year 2018-19 – as the programs were in their early stages there were fewer students enrolled who would be eligible for scholarships.

Additionally, Colorado Mesa University chose to award equal scholarship amounts of $1,300 to 23 eligible students, meaning the institution fell just short of the $30,000 scholarship earmark.

Conclusion

Because FY 2018-19 was the first year of additional funding for cybersecurity and distributed ledger technologies, and because the funds came midway through the academic year, institutions had a limited amount of time to implement programs tied to the funding. As this

funding carries forward, institutions are well-positioned to fully implement the goals of the legislation.

Outside of offering scholarships to students pursuing degrees and credentials related to cybersecurity, and the hiring of faculty and staff, institutions focused funding on improving their cyber facilities and offering outreach events through cyber centers. With ongoing investment in cybersecurity and ledger technology, institutions will be well equipped to continue to invest in these programs and the students enrolled in them.