C.R.S. 24-33.5-1905

Statutes current through Chapter 52 of the 2024 Regular Session, effective as of April 4, 2024. The 2024 legislative changes are not final until compared and reconciled to the 2024 work product of the Colorado Office of Legislative Services later in 2024.

24-33.5-1905. Research and development.

(1) The university of Colorado at Colorado Springs may partner with a nonprofit organization that supports national, state, and regional cybersecurity initiatives to work to establish a secure environment for research and development, initial operational testing and evaluation, and expedited contracting for production for industrial cyber products and techniques.

(2) In furtherance of subsection (1) of this section, the university of Colorado at Colorado Springs and any nonprofit organization with which the university has a partnership may consider the following:

(a) Creating a business plan to develop a secure facility on the property of the University of Colorado at Colorado Springs that provides physical, electronic, proprietary, and administrative security;

(b) Exploring secure facility development and use at other Colorado universities and facilities that may augment the capacity at the university of Colorado at Colorado Springs and enable collaborative activities;

(c) Establishing relationships with appropriate federally funded research and development corporations under the sponsorship of the United States department of defense and the United States department of homeland security as an administrative partner to:

(I) Establish and certify a top secret and special access-certified facility;

(II) Establish cooperative relations with state and federal law enforcement and intelligence agencies responsible for investigating and collecting information related to cyber-based criminal and national security threats;

(III) Act as a conduit for federal and interstate research and development requirements;

(IV) Establish and monitor nondisclosure agreements to protect proprietary intellectual property; and

(V) Process and hold security clearances for authorized Colorado government personnel;

(d) Consider establishing relationships with the existing MITRE national cybersecurity federally funded research and development center; the aerospace corporation federally funded research and development center; or creating a new parallel organization focused on cybersecurity for national defense and homeland security requirements;

(e) Establishing cooperative relationships with Colorado cyber companies and other businesses, local governments, institutions of higher education, and other Colorado organizations with requirements for cybersecurity participation;

(f) Establishing cooperative relations with civilian industrial producers through entities that encourage the interstate sharing of information for cybersecurity;

(g) Linking to local and national military, homeland security, and intelligence community activities to support research and development, rapid test and evaluation, contracting, and production requirements;

(h) Establishing protocols for coordinating and sharing information with state and federal law enforcement and intelligence agencies responsible for investigating and collecting information related to cyber-based criminal and national security threats;

(i) Supporting state and federal law enforcement agencies with their responsibilities to investigate and prosecute threats to and attacks against critical infrastructure;

(j) Encouraging coordination with the United States department of commerce and the national institute of standards and technologies to develop the capability to act as a Colorado in-state center of excellence on cybersecurity advice and national institute of standards and technologies standards;

(k) Studying efforts to protect privacy of personal identifying information maintained within distributed ledger programs, ensuring that programs make all attempts to follow best practices for privacy, and providing advice to all program stakeholders on the requirement to maintain privacy in accordance with required regulatory bodies and governing standards; and

(l) Encouraging the use of distributed ledger technologies, or blockchains, within their proposed curricula for public sector education.

(3) The university of Colorado at Colorado Springs shall participate in activities in furtherance of this section only upon the approval of the board of regents of the university of Colorado, if required by the laws and policies of the board of regents.

(4)

(a) The department of higher education shall allocate to the governing boards of the institutions of higher education participating in activities related to cybersecurity and distributed ledger technologies, such as blockchains, money appropriated to the department of higher education by the general assembly for fiscal year 2018-19 and for each fiscal year thereafter.

(b) 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.

(c) On or before October 1, 2019, and on or before October 1 each year thereafter, the department of higher education, in consultation with the governing board of each institution of higher education that receives funding pursuant to subsection (4)(a) of this section, shall prepare a report using data submitted by the institutions to the department that demonstrates all progress made toward the goals specified in section 24-33.5-1904 (2)(h), and section 24-33.5-1905 (2)(j), (2)(k), and (2)(l). The report shall be based on baseline estimates provided to the department of higher education in April 2018 by each applicable institution of higher education. The report shall include, at a minimum:

(I) The number of faculty or adjunct faculty hired at each institution of higher education as a result of the funding;

(II) The number of student internships created with the funding at each institution of higher education;

(III) The number of degrees or certificates that have been awarded at each institution of higher education in connection with the funding;

(IV) The number of scholarships awarded at each institution of higher education in connection with the funding;

(V) The number of presentations and seminars given on cybersecurity by each institution of higher education; and

(VI) 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.

(d)

(I) The department of higher education shall submit the report prepared pursuant to subsection (4)(c) of this section to the joint budget committee, to the business affairs and labor committee of the house of representatives, the business, labor, and technology committee of the senate, and the education committees of the house of representatives and the senate, or any successor committees. The department of higher education as well as each institution of higher education that receives money pursuant to subsection (4)(a) of this section shall present the findings from the annual report at the annual “State Measurement for Accountable, Responsive, and Transparent (SMART) Government Act” hearings of the joint business committee.

(II) At the "State Measurement for Accountable, Responsive, and Transparent (SMART) Government Act" hearing of the joint business and joint education committees in 2021 and at such hearing every three years thereafter, the joint business committee shall make a recommendation to the joint budget committee regarding whether the funding received by the institutions of higher education pursuant to subsection (4)(a) of this section shall continue in subsequent fiscal years.

History

Source:L. 2016: Entire part added,(HB 16-1453), ch. 189, p. 670, § 1, effective July 1.**L. 2018:**IP(2), (2)(h), and (2)(i) amended and (2)(j), (2)(k), (2)(l), and (4) added,(SB 18-086), ch. 319, p. 1916, § 4, effective May 30.

End of Document