

Second Regular Session  
Seventy-first General Assembly  
STATE OF COLORADO

REVISED

*This Version Includes All Amendments Adopted  
on Second Reading in the Second House*

LLS NO. 18-0326.01 Nicole Myers x4326

SENATE BILL 18-086

SENATE SPONSORSHIP

Lambert and Williams A.,

HOUSE SPONSORSHIP

Ginal and Rankin,

Senate Committees

Business, Labor, & Technology  
Appropriations

House Committees

Business Affairs and Labor  
Appropriations

A BILL FOR AN ACT

101 CONCERNING THE USE OF CYBER CODING CRYPTOLOGY FOR STATE  
102 RECORDS, AND, IN CONNECTION THEREWITH, MAKING AN  
103 APPROPRIATION.

Bill Summary

*(Note: This summary applies to this bill as introduced and does not reflect any amendments that may be subsequently adopted. If this bill passes third reading in the house of introduction, a bill summary that applies to the reengrossed version of this bill will be available at <http://leg.colorado.gov>.)*

The chief information security officer in the governor's office of information technology (OIT), the director of OIT, the department of state, and the executive director of the department of regulatory agencies are required to take certain actions to protect state records containing trusted sensitive and confidential information from criminal,

Shading denotes HOUSE amendment. Double underlining denotes SENATE amendment.  
Capital letters or bold & italic numbers indicate new material to be added to existing statute.  
Dashes through the words indicate deletions from existing statute.

HOUSE  
Amended 2nd Reading  
May 2, 2018

SENATE  
3rd Reading Unamended  
April 6, 2018

SENATE  
Amended 2nd Reading  
April 5, 2018

unauthorized, or inadvertent manipulation or theft.

The chief information security officer is required to:

- ! Identify, assess, and mitigate cyber threats to state government;
- ! Annually collect information from all public agencies to assess the nature of threats to data systems and the potential risks and civil liabilities from the theft or inadvertent release of such information;
- ! In coordination and partnership with specified agencies, boards, and councils, annually assess the data systems of each public agency for the benefits and costs of adopting and applying distributed ledger technologies such as blockchains;
- ! Develop and maintain a series of metrics to identify, assess, and monitor each public agency data system for its platform descriptions, vulnerabilities, risks, liabilities, appropriate employee access control, and the benefits and costs of adopting encryption and distributed ledger technologies.

The director of OIT is required to consider the annual metrics from the office of the chief information security officer to recommend programs, contracts, and upgrades of data systems that have good cost-benefit potential or return on investment. In addition, OIT and the office of the chief information security officer are required to consider developing public-private partnerships and contracts to allow capitalization of encryption technologies while protecting intellectual property rights.

The department of state is required to consider research, development, and implementation for encryption and data integrity techniques, including distributed ledger technologies such as blockchains. The department of state is required to consider using distributed ledger technologies when accepting business licensing records and when distributing department of state data to other departments and agencies.

The executive director of the department of regulatory agencies or the director's designee is required to consider secure encryption methods, including distributed ledger technologies, to protect against falsification, create visibility to identify external hacking threats, and to improve internal data security.

In addition, the bill specifies that institutions of higher education may include distributed ledger technologies within their curricula and research and development activities.

The bill also specifies that the university of Colorado at Colorado Springs and any nonprofit organization with which the university has a partnership may consider:

- ! 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;

- ! 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
- ! Encouraging the use of distributed ledger technologies, such as blockchains, within their proposed curricula for public sector education.

---

1 *Be it enacted by the General Assembly of the State of Colorado:*

2           **SECTION 1.** In Colorado Revised Statutes, **add** 24-37.5-407 as  
3 follows:

4           **24-37.5-407. Cyber coding cryptology for the transmission and**  
5 **storage of state records - legislative declaration - intent.** (1) (a) THE

6 GENERAL ASSEMBLY HEREBY FINDS, DETERMINES, AND DECLARES THAT:

7           (I) AN IMPORTANT FUNCTION OF STATE GOVERNMENT IS TO  
8 PROTECT STATE RECORDS CONTAINING TRUSTED INFORMATION ABOUT  
9 INDIVIDUALS, ORGANIZATIONS, ASSETS, AND ACTIVITIES FROM CRIMINAL,  
10 UNAUTHORIZED, OR INADVERTENT MANIPULATION OR THEFT;

11           (II) IN 2017, THE CYBER THREAT TO THE COLORADO GOVERNMENT  
12 INCLUDED SIX TO EIGHT MILLION ATTEMPTED ATTACKS PER DAY;

13           (III) UNSECURED PUBLIC RECORDS ARE VALUABLE TARGETS FOR  
14 IDENTITY THIEVES AND HACKERS WITH THE INTENT TO STEAL OR  
15 PENETRATE CORPORATE RECORDS. IN ADDITION, THERE ARE INCREASING  
16 THREATS TO THE THEFT OF PERSONAL PRIVACY INFORMATION WITHIN  
17 GOVERNMENT DATA AND A GROWING NUMBER OF THREATS TO NETWORKS,

1 CRITICAL INFRASTRUCTURE, AND PRIVATE DATA AND DEVICES.

2 (IV) IT IS CRUCIAL TO DESIGN A FRAMEWORK TO IDENTIFY  
3 SOLUTIONS TO PREVENT UNAUTHORIZED EXTERNAL DISCLOSURES,  
4 PROTECT PRIVACY AND CONFIDENTIALITY, AND PREVENT INADVERTENT  
5 RELEASES OF INFORMATION;

6 (V) THE EXPANDED USE OF DISTRIBUTED LEDGER TECHNOLOGIES,  
7 SUCH AS BLOCKCHAINS, MAY OFFER TRANSFORMATIVE IMPROVEMENTS TO  
8 DATA SECURITY, ACCOUNTABILITY, TRANSPARENCY, AND SAFETY ACROSS  
9 DISPERSED STATE DEPARTMENTS AND JURISDICTIONS;

10 (VI) LOCAL, REGIONAL, AND NATIONAL AGENCIES ARE CHARGED  
11 WITH MAINTAINING RECORDS THAT INCLUDE BIRTH AND DEATH DATES,  
12 INFORMATION ABOUT MARITAL STATUS, BUSINESS LICENSING, PROPERTY  
13 TRANSFERS, OR CRIMINAL ACTIVITY. MANAGING AND USING THESE DATA  
14 CAN BE COMPLICATED, EVEN FOR ADVANCED GOVERNMENTS. SOME  
15 RECORDS EXIST ONLY IN PAPER FORM, AND IF CHANGES NEED TO BE MADE  
16 IN OFFICIAL REGISTRIES, CITIZENS OFTEN MUST APPEAR IN PERSON TO DO  
17 SO. INDIVIDUAL AGENCIES TEND TO BUILD THEIR OWN ISOLATED  
18 REPOSITORIES OF DATA AND INFORMATION-MANAGEMENT PROTOCOLS,  
19 WHICH PRECLUDE OTHER PARTS OF THE GOVERNMENT FROM USING THEM.

20 (VII) DISTRIBUTED LEDGER AND BLOCKCHAIN TECHNOLOGIES ARE  
21 RAPIDLY EVOLVING FOR EVERY SECTOR OF THE MARKETPLACE AS IT  
22 OFFERS UNIQUE SOLUTIONS TO SUPPORT CONNECTION OF SOCIETY,  
23 TECHNOLOGY, AND FINANCES BY SUPPORTING THE MAPPING OF HUMAN  
24 ACTION TO TRANSACTIONS PERFORMED ON THE INTERNET;

25 (VIII) DISTRIBUTED LEDGERS PROVIDE THE CAPABILITY OF OPENLY  
26 TRACEABLE TRANSACTIONS WHILE MAINTAINING THE PRIVACY OF EACH  
27 PERSON PERFORMING THE TRANSACTIONS;

1 (IX) GOVERNMENT PROGRAMS USING DISTRIBUTED LEDGER  
2 TECHNOLOGIES, SUCH AS BLOCKCHAINS, CAN OFFER THE ABILITY TO  
3 CONTROL FUNCTIONALITY, TRACK TRANSACTIONS, VERIFY IDENTITIES,  
4 SUPPORT UNIFORMITY, RESIST TAMPERING, ENABLE LOGISTICAL CONTROL  
5 FOR LARGE NUMBERS OF PARTICIPANTS, PROTECT PRIVACY, AND SUPPORT  
6 ACCOUNTABILITY AND AUDITING;

7 (X) DISTRIBUTED LEDGER TECHNOLOGIES CAN PROVIDE OR  
8 INCREASE THE FOLLOWING BENEFITS:

9 (A) ENABLE THE STATE TO REDUCE FRAUD AND MALICIOUS  
10 INFILTRATION OF STATE-CONTROLLED PROGRAMS BY CREATING AN  
11 AUDITABLE VISIBILITY FOR ALL TRANSACTIONS AND THE PEOPLE WHO  
12 PERFORM THEM;

13 (B) REDUCE FALSE COMMUNICATIONS FROM COMPUTING DEVICES,  
14 WHICH CAN PROVIDE DATA TO PURSUE APPROPRIATE ENFORCEMENT  
15 ACTIONS. DATA WITH PROOF OF ORIGIN WOULD BE ABLE TO BE USED TO  
16 TRACK FORENSIC CHAIN OF CUSTODY FOR USE IN COURTS OF LAW.

17 (C) SUPPORT VERIFICATION OF AUTHORIZED USERS,  
18 ORGANIZATIONS, DISTRIBUTED COMPUTING DEVICES, AND  
19 NONREPUDIATION OF THE ACTIONS OF PARTIES PARTICIPATING IN VIRTUAL  
20 TRANSACTIONS;

21 (D) REDUCE SPOOFING OF DEVICES, FALSIFICATION OF DATA  
22 RECEIVED FROM REGULATED OR CONTROL DEVICES, AND DRASTICALLY  
23 REDUCE OR ELIMINATE THE THREAT OF MALWARE INSTALLED ON DEVICES  
24 USED STATEWIDE;

25 (E) BETTER PROTECT PERSONAL PRIVACY INFORMATION;

26 (F) CREATE GLOBAL VISIBILITY WHILE MAINTAINING THE  
27 CONFIDENTIALITY AND PRIVACY OF INDIVIDUAL ORGANIZATIONS AND

1       USERS;

2               (G) REDUCE STATE GOVERNMENT EXPENDITURES AND COSTS AS  
3       A RESULT OF THE VISIBILITY OF TRANSACTIONS GAINED FROM THE OPEN  
4       NATURE OF BLOCKCHAIN-ENABLED PROGRAMS;

5               (H) THE ABILITY TO ADOPT DISTRIBUTED LEDGER-ENABLED  
6       PLATFORMS FOR COMPUTER-CONTROLLED PROGRAMS, DATA TRANSFER  
7       AND STORAGE, OR REGULATION PROGRAMS THAT WOULD BE NEEDED OR  
8       USED BY THE STATE. THESE WOULD ALSO ENABLE TRANSACTION-BASED  
9       REVENUE GENERATION AND RETURN ON INVESTMENT FOR STATE  
10       PROGRAMS.

11              (I) PROVIDE QUANTIFIABLE RISK AND QUALITY RATING CAPABILITY  
12       FOR ALL ORGANIZATIONS, AGENCIES, AND INSURANCE PROVIDERS, GIVING  
13       THE ABILITY TO SET PREMIUMS AND REWARD OR ENFORCE PUNITIVE  
14       CONTROLS ON ORGANIZATIONS BASED ON THEIR QUALITY PERFORMANCE  
15       OVER TIME. POSITIVE ACTION TO MITIGATE RISK SHOULD LOWER STATE  
16       CIVIL LIABILITIES, LOWER INSURANCE COSTS, AND LOWER STATE  
17       VULNERABILITY TO ADVERSE LITIGATION.

18              (J) WHEN AUTHORIZED, PROVIDE A REVENUE GENERATION STREAM  
19       FOR THE STATE BY THE SALE OF TRANSACTIONS, FEES, AND MEMBERSHIPS  
20       TO PRIVATE ORGANIZATIONS FOR USE OF STATE-OWNED OPERATIONAL  
21       BLOCKCHAIN OR DISTRIBUTED LEDGER PLATFORMS. A DISTRIBUTED  
22       LEDGER-ENABLED PLATFORM MAY ALLOW THE SALE OF TRUSTED  
23       COMPONENTS AND CONTINUED TRANSACTION-BASED RETURNS ON  
24       INVESTMENT ON AN ONGOING BASIS.

25              (K) ENFORCE COLORADO GOVERNANCE REQUIREMENTS AND  
26       LAWS, THEREBY PROTECTING LEGAL AND LEGITIMATE DISTRIBUTION OF  
27       CONTROLLED SUBSTANCES TO PROTECT STATE REVENUE STREAMS

1 RECEIVED BY TAXATION OF CONTROLLED SUBSTANCES.

2 (b) THE GENERAL ASSEMBLY FURTHER FINDS, DETERMINES, AND  
3 DECLARES THAT THE INTENT OF THIS SECTION IS TO ALLOW AND  
4 ENCOURAGE THE OFFICE OF INFORMATION TECHNOLOGY, THE OFFICE OF  
5 THE CHIEF INFORMATION SECURITY OFFICER, DEPARTMENTS, AND  
6 AGENCIES TO IDENTIFY AND IMPLEMENT DISTRIBUTED LEDGER  
7 TECHNOLOGIES, SUCH AS BLOCKCHAINS, WHENEVER APPROPRIATE,  
8 RATHER THAN TO MANDATE SPECIFIC SOLUTIONS. IN ADDITION, THE  
9 INTENT OF THIS SECTION IS TO ENCOURAGE THE OFFICE OF THE CHIEF  
10 INFORMATION SECURITY OFFICER TO COORDINATE CROSS-JURISDICTIONAL  
11 STANDARDS AND PROCEDURES, ESPECIALLY AMONG STATE DEPARTMENTS  
12 AND AGENCIES AND AMONG COUNTIES AND MUNICIPALITIES WHEN  
13 APPROPRIATE.

14 (2) THE OFFICE OF THE CHIEF INFORMATION SECURITY OFFICER  
15 SHALL IDENTIFY, ASSESS, AND MITIGATE CYBER THREATS TO STATE  
16 GOVERNMENT. IN FURTHERANCE OF THIS RESPONSIBILITY, THE CHIEF  
17 INFORMATION SECURITY OFFICER SHALL, ON AN ANNUAL BASIS AND  
18 THROUGH ANNUAL PUBLIC AGENCY ENTERPRISE CYBERSECURITY PLANS,  
19 COLLECT INFORMATION FROM ALL PUBLIC AGENCIES AS DEFINED IN  
20 SECTION 24-37.5-402 (9) TO ASSESS THE NATURE OF THREATS TO DATA  
21 SYSTEMS AND THE POTENTIAL RISKS AND CIVIL LIABILITIES FROM THE  
22 THEFT OR INADVERTENT RELEASE OF SUCH INFORMATION. INSTITUTIONS  
23 OF HIGHER EDUCATION AND THE GENERAL ASSEMBLY MAY PROVIDE THE  
24 INFORMATION SPECIFIED IN THIS SUBSECTION (2) TO THE CHIEF  
25 INFORMATION SECURITY OFFICER.

26 (3) IN COORDINATION WITH THE COLORADO CYBERSECURITY  
27 COUNCIL CREATED IN SECTION 24-33.5-1902, AND IN PARTNERSHIP WITH

1 THE OFFICE AND THE GOVERNMENT DATA ADVISORY BOARD CREATED IN  
2 SECTION 24-37.5-703, THE OFFICE OF THE CHIEF INFORMATION SECURITY  
3 OFFICER IS ENCOURAGED TO ASSESS THE DATA SYSTEMS OF EACH PUBLIC  
4 AGENCY FOR THE BENEFITS AND COSTS OF ADOPTING AND APPLYING  
5 DISTRIBUTED LEDGER TECHNOLOGIES SUCH AS BLOCKCHAINS. THE OFFICE  
6 OF THE CHIEF INFORMATION SECURITY OFFICER IS ENCOURAGED TO  
7 CONSIDER PROGRAM LOSSES DUE TO POTENTIAL MALICIOUS ATTACK,  
8 TRANSACTIONAL ERRORS, OR FRAUD AS POSSIBLE SAVINGS ACHIEVABLE  
9 FROM VISIBILITY GAINED THROUGH DISTRIBUTED LEDGER PLATFORMS. THE  
10 OFFICE OF THE CHIEF INFORMATION SECURITY OFFICER IS ENCOURAGED TO  
11 DEVELOP AND MAINTAIN A SERIES OF METRICS TO IDENTIFY, ASSESS, AND  
12 MONITOR EACH PUBLIC AGENCY DATA SYSTEM ON AN ONGOING BASIS FOR  
13 THEIR PLATFORM DESCRIPTIONS, VULNERABILITIES, RISKS, LIABILITIES,  
14 APPROPRIATE EMPLOYEE ACCESS CONTROL, AND THE BENEFITS AND COSTS  
15 OF ADOPTING ENCRYPTION AND DISTRIBUTED LEDGER TECHNOLOGIES. THE  
16 OFFICE OF THE CHIEF INFORMATION SECURITY OFFICER IS ALSO  
17 ENCOURAGED TO CONSIDER THE COST-AVOIDANCE BENEFITS AND THE  
18 POSITIVE BENEFITS OF REDUCING LITIGATION RISKS OR THE COSTS OF  
19 STATE INSURANCE AGAINST STATE LEGAL LIABILITIES.

20 (4) THE OFFICE AND THE OFFICE OF THE CHIEF INFORMATION  
21 SECURITY OFFICER SHALL CONSIDER DEVELOPING PUBLIC-PRIVATE  
22 PARTNERSHIPS AND CONTRACTS TO ALLOW CAPITALIZATION OF  
23 ENCRYPTION TECHNOLOGIES, WHILE PROTECTING INTELLECTUAL  
24 PROPERTY RIGHTS.

25 (5) IN COMMUNICATION BETWEEN MULTIPLE PARTIES, THE OFFICE  
26 AND THE OFFICE OF THE CHIEF INFORMATION SECURITY OFFICER ARE  
27 ENCOURAGED TO ENSURE THAT PLATFORMS INCORPORATE THE

1 NONREPUDIATION OF PARTICIPATING ENTITIES IN VIRTUAL TRANSACTIONS.  
2 DUE TO THE INHERENT LACK OF POSITIVE IDENTIFICATION BETWEEN  
3 PARTIES COMMUNICATING OVER THE INTERNET, SECURE COMMUNICATION  
4 SYSTEMS SHOULD BE DESIGNED TO ASSURE THAT EACH SENDER OF DATA  
5 IS PROVIDED WITH PROOF OF DELIVERY AND THAT THE RECIPIENT OF DATA  
6 IS PROVIDED WITH PROOF OF THE SENDER'S IDENTITY TO ENSURE THAT THE  
7 INTEGRITY OF THE COMMUNICATIONS CAN BE TRUSTED, THAT EACH  
8 COMMUNICATION IS ACCOUNTABLE AND AUDITABLE, AND THE  
9 COMMUNICATORS CANNOT DENY THAT THEIR COMMUNICATIONS TOOK  
10 PLACE. THIS IS TECHNICALLY CALLED NONREPUDIATION, IN COMPLIANCE  
11 WITH FEDERAL GUIDELINES AND INDUSTRY BEST PRACTICES.

12 (6) A COUNTY OR MUNICIPAL GOVERNMENT SHALL NOT:

13 (a) IMPOSE A TAX OR FEE ON THE USE OF DISTRIBUTED LEDGER  
14 TECHNOLOGIES BY ANY PRIVATE PERSON OR ENTITY; OR

15 (b) REQUIRE ANY PRIVATE PERSON OR ENTITY TO OBTAIN FROM  
16 ANY PUBLIC AGENCY ANY CERTIFICATE, LICENSE, OR PERMIT TO USE  
17 DISTRIBUTED LEDGER TECHNOLOGIES.

18 **SECTION 2.** In Colorado Revised Statutes, **add** 24-21-117 as  
19 follows:

20 **24-21-117. Encryption and data integrity techniques -**  
21 **research and development.** IN CONJUNCTION WITH THE EFFORTS OF THE  
22 OFFICE OF INFORMATION TECHNOLOGY REGARDING CYBER CODING  
23 CRYPTOLOGY FOR STATE RECORDS PURSUANT TO SECTION 24-37.5-407,  
24 THE DEPARTMENT OF STATE, IN CONJUNCTION WITH UPGRADES TO THE  
25 DEPARTMENT OF STATE'S BUSINESS SUITE, SHALL CONSIDER RESEARCH,  
26 DEVELOPMENT, AND IMPLEMENTATION FOR APPROPRIATE ENCRYPTION  
27 AND DATA INTEGRITY TECHNIQUES, INCLUDING DISTRIBUTED LEDGER

1 TECHNOLOGIES SUCH AS BLOCKCHAINS. AFTER ACCEPTING BUSINESS  
2 LICENSING RECORDS, THE DEPARTMENT OF STATE SHALL CONSIDER  
3 ENSURING THE INTEGRITY OF THOSE TRANSACTIONS BY SECURE METHODS,  
4 INCLUDING DISTRIBUTED LEDGER TECHNOLOGIES, TO PROTECT AGAINST  
5 FALSIFICATION, CREATE VISIBILITY TO IDENTIFY EXTERNAL HACKING  
6 THREATS, AND TO IMPROVE INTERNAL DATA SECURITY. WHEN  
7 DISTRIBUTING DEPARTMENT OF STATE DATA TO OTHER DEPARTMENTS AND  
8 AGENCIES, THE DEPARTMENT OF STATE SHALL CONSIDER USING  
9 DISTRIBUTED LEDGER TECHNOLOGIES, INCLUDING BLOCKCHAINS, AS A  
10 MEANS OF PROTECTING DATA ACROSS JURISDICTIONS.

11 **SECTION 3.** In Colorado Revised Statutes, 24-33.5-1904,  
12 **amend** (2) introductory portion, (2)(f), and (2)(g); and **add** (2)(h) as  
13 follows:

14 **24-33.5-1904. Education - training - workforce development.**

15 (2) In furtherance of ~~the provisions of~~ subsection (1) of this section, the  
16 university of Colorado at Colorado Springs, in conjunction with other  
17 institutions of higher education and a nonprofit organization, may:

18 (f) Establish protocols for coordinating and sharing information  
19 with state and federal law enforcement and intelligence agencies  
20 responsible for investigating and collecting information related to  
21 cyber-based criminal and national security threats; ~~and~~

22 (g) Support state and federal law enforcement agencies with their  
23 responsibilities to investigate and prosecute threats to and attacks against  
24 critical infrastructure; AND

25 (h) INCLUDE DISTRIBUTED LEDGER TECHNOLOGIES WITHIN ITS  
26 CURRICULA AND RESEARCH AND DEVELOPMENT ACTIVITIES.

27 **SECTION 4.** In Colorado Revised Statutes, 24-33.5-1905,

1 **amend** (2) introductory portion, (2)(h), and (2)(i); and **add** (2)(j), (2)(k),  
2 (2)(l), and (4) as follows:

3 **24-33.5-1905. Research and development.** (2) In furtherance of  
4 ~~the provisions of~~ subsection (1) of this section, the university of Colorado  
5 at Colorado Springs and any nonprofit organization with which the  
6 university has a partnership may consider the following:

7 (h) ~~Establish~~ ESTABLISHING protocols for coordinating and  
8 sharing information with state and federal law enforcement and  
9 intelligence agencies responsible for investigating and collecting  
10 information related to cyber-based criminal and national security threats;  
11 **and**

12 (i) ~~Support~~ SUPPORTING state and federal law enforcement  
13 agencies with their responsibilities to investigate and prosecute threats to  
14 and attacks against critical infrastructure;

15 (j) ENCOURAGING COORDINATION WITH THE UNITED STATES  
16 DEPARTMENT OF COMMERCE AND THE NATIONAL INSTITUTE OF  
17 STANDARDS AND TECHNOLOGIES TO DEVELOP THE CAPABILITY TO ACT AS  
18 A COLORADO IN-STATE CENTER OF EXCELLENCE ON CYBERSECURITY  
19 ADVICE AND NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGIES  
20 STANDARDS;

21 (k) STUDYING EFFORTS TO PROTECT PRIVACY OF PERSONAL  
22 IDENTIFYING INFORMATION MAINTAINED WITHIN DISTRIBUTED LEDGER  
23 PROGRAMS, ENSURING THAT PROGRAMS MAKE ALL ATTEMPTS TO FOLLOW  
24 BEST PRACTICES FOR PRIVACY, AND PROVIDING ADVICE TO ALL PROGRAM  
25 STAKEHOLDERS ON THE REQUIREMENT TO MAINTAIN PRIVACY IN  
26 ACCORDANCE WITH REQUIRED REGULATORY BODIES AND GOVERNING  
27 STANDARDS; AND

1 (1) ENCOURAGING THE USE OF DISTRIBUTED LEDGER  
2 TECHNOLOGIES, OR BLOCKCHAINS, WITHIN THEIR PROPOSED CURRICULA  
3 FOR PUBLIC SECTOR EDUCATION.

4 (4) (a) THE DEPARTMENT OF HIGHER EDUCATION SHALL ALLOCATE  
5 TO THE GOVERNING BOARDS OF THE INSTITUTIONS OF HIGHER EDUCATION  
6 PARTICIPATING IN ACTIVITIES RELATED TO CYBERSECURITY AND  
7 DISTRIBUTED LEDGER TECHNOLOGIES, SUCH AS BLOCKCHAINS, MONEY  
8 APPROPRIATED TO THE DEPARTMENT OF HIGHER EDUCATION BY THE  
9 GENERAL ASSEMBLY FOR FISCAL YEAR 2018-19 AND FOR EACH FISCAL  
10 YEAR THEREAFTER. THE GOVERNING BOARD OF EACH INSTITUTION OF  
11 HIGHER EDUCATION PARTICIPATING IN ACTIVITIES RELATED TO  
12 CYBERSECURITY AND DISTRIBUTED LEDGER TECHNOLOGIES SHALL ENSURE  
13 THAT AT LEAST THE FOLLOWING PERCENTAGES OF THE MONEY ALLOCATED  
14 TO THE INSTITUTION PURSUANT TO THIS SUBSECTION (4) IS USED TO  
15 PROVIDE SCHOLARSHIPS TO STUDENTS AT THE INSTITUTION WHO ARE  
16 DOING WORK IN CONNECTION WITH CYBERSECURITY AND DISTRIBUTED  
17 LEDGER TECHNOLOGIES.

18 (b) (1) FOR AN INSTITUTION OF HIGHER EDUCATION RECEIVING  
19 ONE MILLION DOLLARS OR MORE FOR SCHOLARSHIPS PURSUANT TO  
20 SUBSECTION (4)(a) OF THIS SECTION, FOR THE FIRST THREE YEARS THAT  
21 THE INSTITUTION RECEIVES SAID MONEY, THE INSTITUTION MUST ENSURE  
22 THAT AT LEAST FIFTEEN PERCENT OF THE MONEY RECEIVED IS USED TO  
23 PROVIDE SAID SCHOLARSHIPS. FOR THE FOURTH AND SUBSEQUENT YEARS  
24 OF FUNDING, THE INSTITUTION SHALL ENSURE THAT AT LEAST TWENTY  
25 PERCENT OF THE MONEY RECEIVED IS USED TO PROVIDE SAID  
26 SCHOLARSHIPS; EXCEPT THAT, FOR THE FIVE PERCENT INCREASE FROM  
27 YEARS THREE TO FOUR, THE INSTITUTION MAY USE PRIVATE DONATIONS TO

1 ACCOUNT FOR THE INCREASE.

2 (II) FOR AN INSTITUTION RECEIVING LESS THAN ONE MILLION  
3 DOLLARS FOR SCHOLARSHIPS PURSUANT TO SUBSECTION (4)(a) OF THIS  
4 SECTION, THE INSTITUTION MUST ENSURE THAT AT LEAST TEN PERCENT OF  
5 THE MONEY RECEIVED IS USED TO PROVIDE SAID SCHOLARSHIPS.

6 (c) ON OR BEFORE OCTOBER 1, 2019, AND ON OR BEFORE OCTOBER  
7 1 EACH YEAR THEREAFTER, THE DEPARTMENT OF HIGHER EDUCATION, IN  
8 CONSULTATION WITH THE GOVERNING BOARD OF EACH INSTITUTION OF  
9 HIGHER EDUCATION THAT RECEIVES FUNDING PURSUANT TO SUBSECTION  
10 (4)(a) OF THIS SECTION, SHALL PREPARE A REPORT USING DATA SUBMITTED  
11 BY THE INSTITUTIONS TO THE DEPARTMENT THAT DEMONSTRATES ALL  
12 PROGRESS MADE TOWARD THE GOALS SPECIFIED IN SECTION 24-33-5-1904  
13 (2)(h), AND SECTION 24-33.5-1905 (2)(j), (2)(k), AND (2)(l). THE REPORT  
14 SHALL BE BASED ON BASELINE ESTIMATES PROVIDED TO THE DEPARTMENT  
15 OF HIGHER EDUCATION IN APRIL 2018 BY EACH APPLICABLE INSTITUTION  
16 OF HIGHER EDUCATION. THE REPORT SHALL INCLUDE, AT A MINIMUM:

17 (I) THE NUMBER OF FACULTY OR ADJUNCT FACULTY HIRED AT  
18 EACH INSTITUTION OF HIGHER EDUCATION AS A RESULT OF THE FUNDING;

19 (II) THE NUMBER OF STUDENT INTERNSHIPS CREATED WITH THE  
20 FUNDING AT EACH INSTITUTION OF HIGHER EDUCATION;

21 (III) THE NUMBER OF DEGREES OR CERTIFICATES THAT HAVE BEEN  
22 AWARDED AT EACH INSTITUTION OF HIGHER EDUCATION IN CONNECTION  
23 WITH THE FUNDING;

24 (IV) THE NUMBER OF SCHOLARSHIPS AWARDED AT EACH  
25 INSTITUTION OF HIGHER EDUCATION IN CONNECTION WITH THE FUNDING;

26 (V) THE NUMBER OF PRESENTATIONS AND SEMINARS GIVEN ON  
27 CYBERSECURITY BY EACH INSTITUTION OF HIGHER EDUCATION; AND

1 (VI) THE AMOUNT OF ALL OTHER MONEY THAT HAS BEEN RAISED  
2 TO MATCH THE STATE INVESTMENT, WHICH MAY INCLUDE TUITION, FEES,  
3 FEDERAL FUNDS, AND INDUSTRY DONATIONS.

4 (d) (I) THE DEPARTMENT OF HIGHER EDUCATION SHALL SUBMIT  
5 THE REPORT PREPARED PURSUANT TO SUBSECTION (4)(b) OF THIS SECTION  
6 TO THE JOINT BUDGET COMMITTEE, TO THE BUSINESS AFFAIRS AND LABOR  
7 COMMITTEE OF THE HOUSE OF REPRESENTATIVES, THE BUSINESS, LABOR,  
8 AND TECHNOLOGY COMMITTEE OF THE SENATE, AND THE EDUCATION  
9 COMMITTEES OF THE HOUSE OF REPRESENTATIVES AND THE SENATE, OR  
10 ANY SUCCESSOR COMMITTEES. THE DEPARTMENT OF HIGHER EDUCATION  
11 AS WELL AS EACH INSTITUTION OF HIGHER EDUCATION THAT RECEIVES  
12 MONEY PURSUANT TO SUBSECTION (4)(a) OF THIS SECTION SHALL PRESENT  
13 THE FINDINGS FROM THE ANNUAL REPORT AT THE ANNUAL "STATE  
14 MEASUREMENT FOR ACCOUNTABLE, RESPONSIVE, AND TRANSPARENT  
15 (SMART) GOVERNMENT ACT" HEARINGS OF THE JOINT BUSINESS  
16 COMMITTEE.

17 (II) AT THE "STATE MEASUREMENT FOR ACCOUNTABLE,  
18 RESPONSIVE, AND TRANSPARENT (SMART) GOVERNMENT ACT" HEARING  
19 OF THE JOINT BUSINESS AND JOINT EDUCATION COMMITTEES IN 2021 AND  
20 AT SUCH HEARING EVERY THREE YEARS THEREAFTER, THE JOINT BUSINESS  
21 COMMITTEE SHALL MAKE A RECOMMENDATION TO THE JOINT BUDGET  
22 COMMITTEE REGARDING WHETHER THE FUNDING RECEIVED BY THE  
23 INSTITUTIONS OF HIGHER EDUCATION PURSUANT TO SUBSECTION (4)(a) OF  
24 THIS SECTION SHALL CONTINUE IN SUBSEQUENT FISCAL YEARS.

25 **SECTION 5.** In Colorado Revised Statutes, 24-34-101, **add** (14)  
26 as follows:

27 **24-34-101. Department created - executive director.** (14) IN

1 CONJUNCTION WITH THE EFFORTS OF THE OFFICE OF INFORMATION  
2 TECHNOLOGY REGARDING CYBER CODING CRYPTOLOGY FOR STATE  
3 RECORDS PURSUANT TO SECTION 24-37.5-407, THE EXECUTIVE DIRECTOR  
4 OF THE DEPARTMENT OF REGULATORY AGENCIES OR THE DIRECTOR'S  
5 DESIGNEE SHALL CONSIDER SECURE ENCRYPTION METHODS, ESPECIALLY  
6 DISTRIBUTED LEDGER TECHNOLOGIES, TO PROTECT AGAINST  
7 FALSIFICATION, CREATE VISIBILITY TO IDENTIFY EXTERNAL HACKING  
8 THREATS, AND TO IMPROVE INTERNAL DATA SECURITY, ESPECIALLY TO  
9 SECURE BUSINESS OWNERSHIP AND STOCK LEDGER OWNERSHIP DATA THAT  
10 MIGHT BE POTENTIAL HIGH-RISK TARGETS FOR CORPORATE CYBER THEFT  
11 AND TRANSACTION FALSIFICATION. THE CONSIDERATIONS FOR  
12 DISTRIBUTED LEDGER TECHNOLOGIES SHALL INCLUDE BEST PRACTICE  
13 ATTEMPTS TO MAINTAIN PRIVACY OF PERSONALLY IDENTIFYING  
14 INFORMATION OF THE DISTRIBUTED USER BASE WHILE UTILIZING THE  
15 VISIBILITY OF DISTRIBUTED TRANSACTIONS.

16 **SECTION 6.** In Colorado Revised Statutes, 24-37.5-105, **add**  
17 (12), (13), and (14) as follows:

18 **24-37.5-105. Office - responsibilities - rules.** (12) IN  
19 CONJUNCTION WITH THE EFFORTS OF THE OFFICE OF THE CHIEF  
20 INFORMATION SECURITY OFFICER REGARDING CYBER CODING CRYPTOLOGY  
21 FOR STATE RECORDS PURSUANT TO SECTION 24-37.5-407, THE OFFICE  
22 SHALL CONSIDER THE ANNUAL METRICES CREATED PURSUANT TO SECTION  
23 24-37.5-407 (3) TO RECOMMEND PROGRAMS, CONTRACTS, AND UPGRADES  
24 OF DATA SYSTEMS THAT HAVE GOOD COST-BENEFIT POTENTIAL OR RETURN  
25 ON INVESTMENT.

26 (13) BEGINNING ON THE EFFECTIVE DATE OF THIS SUBSECTION  
27 (13), IN THE ADMINISTRATION OF ANY NEW MAJOR INFORMATION

1 TECHNOLOGY PROJECT, THE OFFICE, IN CONJUNCTION WITH THE STATE  
2 AGENCY WITH WHICH IT IS WORKING, SHALL EVALUATE THE POTENTIAL  
3 USE OF BLOCKCHAIN AND DISTRIBUTED LEDGER TECHNOLOGIES AS PART  
4 OF THE PROJECT.

5 (14) THE OFFICE SHALL CONDUCT AN ASSESSMENT AND BRING  
6 RECOMMENDATIONS FOR DISTRIBUTED LEDGER OR BLOCKCHAIN  
7 IMPLEMENTATIONS TO THE JOINT TECHNOLOGY COMMITTEE OF THE  
8 GENERAL ASSEMBLY. THE STUDY MUST PRODUCE RECOMMENDATIONS OF  
9 POTENTIAL USE CASES WHERE BLOCKCHAIN OR DISTRIBUTED LEDGER  
10 TECHNOLOGIES CAN BE IMPLEMENTED INSIDE OF STATE TECHNOLOGY  
11 SOLUTIONS.

12 **SECTION 7. In Colorado Revised Statutes, 23-18-308, amend**  
13 **(1) as follows:**

14 **23-18-308. Fee-for-service contracts - limited purpose.**

15 **(1) Subject to available appropriations, the department shall enter into a**  
16 **fee-for-service contract CONTRACTS for the following purpose PURPOSES:**

17 **(a) The creation of career pathways for students pursuant to**  
18 **sections 23-60-109 and 24-46.3-104; C.R.S.; and**

19 **(b) The inclusive higher education pilot program pursuant to**  
20 **section 23-75-104; AND**

21 **(c) CYBERSECURITY AND DISTRIBUTED LEDGER TECHNOLOGIES,**  
22 **SUCH AS BLOCKCHAINS, AS SET FORTH IN SECTIONS 24-33.5-1904 AND**  
23 **24-33.5-1905.**

24 **SECTION 8. Appropriation.** (1) For the 2018-19 state fiscal  
25 year, \$250,000 is appropriated to the office of the governor for use by the  
26 office of information technology. This appropriation is from the general  
27 fund and is based on an assumption that the office of information

1 technology will require an additional 1.0 FTE. To implement this act, the  
2 office of information technology may use this appropriation for security  
3 governance to evaluate the potential use of distributed ledger  
4 technologies, including blockchain, in state data systems.

5 (2) For the 2018-19 state fiscal year, \$5,100,000 is appropriated  
6 to the department of higher education. This appropriation is from the  
7 general fund. To implement this act, the department may use this  
8 appropriation for the college opportunity fund program to be used for  
9 limited purpose fee-for-service contracts with state institutions.

10 (3) For the 2018-19 state fiscal year, \$5,100,000 is appropriated  
11 to the department of higher education. This appropriation is from  
12 reappropriated funds received from the limited purpose fee-for-service  
13 contracts with state institutions under subsection (2) of this section. To  
14 implement this act, the department may use this appropriation as follows:

15 **Governing Boards**

16	<u>Trustees of Colorado Mesa university</u>	<u>\$300,000</u>
17	<u>Trustees of Metropolitan state university</u>	
18	<u>of Denver</u>	<u>\$300,000</u>
19	<u>Trustees of Western state Colorado university</u>	<u>\$200,000</u>
20	<u>Board of governors of the Colorado state</u>	
21	<u>university system</u>	<u>\$1,200,000</u>

1                           Regents of the university of Colorado                           \$2,800,000

2                           State board for community colleges and  
3                           occupational education state system  
4                           community colleges                           \$300,000.

5                   **SECTION 8. Safety clause.** The general assembly hereby finds,  
6 determines, and declares that this act is necessary for the immediate  
7 preservation of the public peace, health, and safety.