Second Regular Session
Seventy-first General Assembly
STATE OF COLORADO

REREVISED
This Version Includes All Amendments
Adopted 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,

HOUSE
Amended 3rd Reading
May 4, 2018

HOUSE
Amended 2nd Reading
May 2, 2018

SENATE
3rd Reading Unamended
April 6, 2018

SENATE
Amended 2nd Reading
April 5, 2018

Senate Committees
Business, Labor, & Technology
Appropriations

House Committees
Business Affairs and Labor
Appropriations

A BILL FOR AN ACT

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

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.

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

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

24-37.5-407. Cyber coding cryptology for the transmission and storage of state records - legislative declaration - intent. (1) (a) THE GENERAL ASSEMBLY HEREBY FINDS, DETERMINES, AND DECLARES THAT:

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

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

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

CRITICAL INFRASTRUCTURE, AND PRIVATE DATA AND DEVICES.

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

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

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

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

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

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

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

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

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

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

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

(E) BETTER PROTECT PERSONAL PRIVACY INFORMATION;

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

USERS;

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

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

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

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

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

RECEIVED BY TAXATION OF CONTROLLED SUBSTANCES.

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

(2) THE OFFICE OF THE CHIEF INFORMATION SECURITY OFFICER SHALL IDENTIFY, ASSESS, AND MITIGATE CYBER THREATS TO STATE GOVERNMENT. IN FURTHERANCE OF THIS RESPONSIBILITY, THE CHIEF INFORMATION SECURITY OFFICER SHALL, ON AN ANNUAL BASIS AND THROUGH ANNUAL PUBLIC AGENCY ENTERPRISE CYBERSECURITY PLANS, COLLECT INFORMATION FROM ALL PUBLIC AGENCIES AS DEFINED IN SECTION 24-37.5-402 (9) 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. INSTITUTIONS OF HIGHER EDUCATION AND THE GENERAL ASSEMBLY MAY PROVIDE THE INFORMATION SPECIFIED IN THIS SUBSECTION (2) TO THE CHIEF INFORMATION SECURITY OFFICER.

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

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

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

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

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

(6) A COUNTY OR MUNICIPAL GOVERNMENT SHALL NOT:

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

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

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

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

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

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

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

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

(f) Establish 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; ~~and~~

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

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

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

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

24-33.5-1905. Research and development. (2) In furtherance of ~~the provisions 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:

(h) ~~Establish~~ 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; ~~and~~

(i) ~~Support~~ 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.

(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)(b) 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.

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

24-34-101. Department created - executive director. (14) IN CONJUNCTION WITH THE EFFORTS OF THE OFFICE OF INFORMATION TECHNOLOGY REGARDING CYBER CODING CRYPTOLOGY FOR STATE RECORDS PURSUANT TO SECTION 24-37.5-407, THE EXECUTIVE DIRECTOR OF THE DEPARTMENT OF REGULATORY AGENCIES OR THE DIRECTOR'S DESIGNEE SHALL CONSIDER SECURE ENCRYPTION METHODS, ESPECIALLY DISTRIBUTED LEDGER TECHNOLOGIES, TO PROTECT AGAINST FALSIFICATION, CREATE VISIBILITY TO IDENTIFY EXTERNAL HACKING THREATS, AND TO IMPROVE INTERNAL DATA SECURITY, ESPECIALLY TO SECURE BUSINESS OWNERSHIP AND STOCK LEDGER OWNERSHIP DATA THAT MIGHT BE POTENTIAL HIGH-RISK TARGETS FOR CORPORATE CYBER THEFT AND TRANSACTION FALSIFICATION. THE CONSIDERATIONS FOR DISTRIBUTED LEDGER TECHNOLOGIES SHALL INCLUDE BEST PRACTICE ATTEMPTS TO MAINTAIN PRIVACY OF PERSONALLY IDENTIFYING INFORMATION OF THE DISTRIBUTED USER BASE WHILE UTILIZING THE VISIBILITY OF DISTRIBUTED TRANSACTIONS.

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

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

(13) BEGINNING ON THE EFFECTIVE DATE OF THIS SUBSECTION

(13), IN THE ADMINISTRATION OF ANY NEW MAJOR INFORMATION TECHNOLOGY PROJECT, THE OFFICE, IN CONJUNCTION WITH THE STATE AGENCY WITH WHICH IT IS WORKING, SHALL EVALUATE THE POTENTIAL USE OF BLOCKCHAIN AND DISTRIBUTED LEDGER TECHNOLOGIES AS PART OF THE PROJECT.

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

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

23-18-308. Fee-for-service contracts - limited purpose. (1) Subject to available appropriations, the department shall enter into ~~a~~ fee-for-service ~~contract~~ CONTRACTS for the following ~~purpose~~ PURPOSES:

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

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

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

SECTION 8. Appropriation. (1) For the 2018-19 state fiscal year, $250,000 is appropriated to the office of the governor for use by the office of information technology. This appropriation is from the general

fund and is based on an assumption that the office of information technology will require an additional 1.0 FTE. To implement this act, the office of information technology may use this appropriation for security governance to evaluate the potential use of distributed ledger technologies, including blockchain, in state data systems.

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

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

Governing Boards

Trustees of Colorado Mesa university	$300,000
Trustees of Metropolitan state university of Denver	$300,000
Trustees of Western state Colorado university	$200,000
Board of governors of the Colorado state university system	$1,200,000

Regents of the university of Colorado		$2,800,000
State board for community colleges and occupational education state system community colleges		$300,000.

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