

**Second Regular Session
Seventieth General Assembly
STATE OF COLORADO**

REREVISED

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

LLS NO. 16-0927.01 Nicole Myers x4326

HOUSE BILL 16-1453

HOUSE SPONSORSHIP

Hamner, Young, Rankin, Hullinghorst, Duran, Lee, Nordberg, Becker K., Carver, Foote, Joshi, Klingenschmitt, Landgraf, Lundeen, Melton, Pabon, Primavera, Priola, Rosenthal, Roupe, Ryden, Williams

SENATE SPONSORSHIP

Lambert, Grantham, Steadman, Cadman, Scheffel, Guzman, Merrifield, Baumgardner, Carroll, Cooke, Crowder, Garcia, Heath, Hill, Hodge, Jahn, Johnston, Jones, Kefalas, Kerr, Lundberg, Marble, Martinez Humenik, Newell, Scott, Tate, Todd, Ulibarri, Woods

House Committees
Appropriations

Senate Committees
Appropriations

A BILL FOR AN ACT

101 **CONCERNING MEASURES TO ENHANCE CYBERSECURITY, AND, IN**
102 **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://www.leg.state.co.us/billsummaries>.)

Joint Budget Committee. The Colorado cybersecurity council (council) is created in the department of public safety to operate as a steering group to develop cybersecurity policy guidance for the governor, develop comprehensive goals, requirements, initiatives, and milestones, and to coordinate with the general assembly and the judicial branch regarding cybersecurity. The council is comprised of specified officers

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

SENATE
3rd Reading Unamended
May 4, 2016

SENATE
Amended 2nd Reading
May 3, 2016

HOUSE
3rd Reading Unamended
April 29, 2016

HOUSE
2nd Reading Unamended
April 28, 2016

from the governor's office, executive branch agencies, military organizations, institutions of higher education, the attorney general's office, and the state auditor's office.

The department of public safety may coordinate with specified entities to define the operational requirements for in-state and interstate operational and training networks. The coordinating entities may:

- ! Consider establishing memoranda of understanding or interstate compacts with entities that encourage the interstate sharing of information for cybersecurity;
- ! Support the requirements for the fusion of cyber defense, cyber surveillance, and international and domestic intelligence and law enforcement operations;
- ! Consider network infrastructures for interstate cyber training and operations;
- ! Support secure Colorado requirements to identify threats and vulnerabilities, defend state cyber infrastructures, and investigate and enforce cyber-related crimes; and
- ! Conduct training, inspections, and operational exercises.

The university of Colorado at Colorado Springs (UCCS), in partnership with a nonprofit organization that supports national, state, and regional cybersecurity initiatives (nonprofit organization), may establish and expand cyber higher education programs and establish needed cyber education and training laboratories in specified subject areas. UCCS and the nonprofit organization may:

- ! Coordinate with the United States department of homeland security and the national security agency to certify cyber courses and curricula;
- ! Coordinate planning for cyber education with appropriate institutions of higher education;
- ! Identify appropriate curricula for community college and technical certification programs and for elementary and secondary education feeder programs;
- ! Establish a public policy think tank as an academic research center of excellence for government, academic, and industrial communications, conferences, research, and publications; and
- ! Establish education, training, and academic symposia for government leaders at all levels.

UCCS and the nonprofit organization also may establish a secure environment for research and development, initial operational testing and evaluation, and expedited contracting for production for industrial cyber products and techniques and may consider:

- ! Creating a business plan to develop a secure facility on the property of UCCS to allow physical, electronic, proprietary, and administrative security;

- ! Exploring secure facility development and use at other Colorado universities and facilities;
- ! 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;
- ! Consider establishing relationships with certain existing federally funded research and development corporations, or consider creating a new organization to focus on defense and homeland security requirements;
- ! Establishing cooperative relationships with Colorado cyber companies and other businesses, local governments, and other Colorado institutions with requirements for cybersecurity participation;
- ! Establishing cooperative relations with civilian industrial producers; and
- ! 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.

The cybersecurity cash fund (fund) is created in the state treasury. The fund consists of any money that the general assembly may appropriate or transfer to the fund. Subject to annual appropriation, the regents of the university of Colorado may expend money from the fund for the purposes of the bill. The cybersecurity gifts, grants, and donations account (account) is created in the fund. The regents of the university of Colorado may seek, accept, and expend gifts, grants, or donations from private or public sources for the purposes of the bill and are required to credit any such gifts, grants, or donations to the account. The moneys in the account are continuously appropriated to the department of higher education for use by the regents of the university of Colorado for the purposes of the bill.

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

2 **SECTION 1.** In Colorado Revised Statutes, **add** part 19 to article
3 33.5 of title 24 as follows:

4 PART 19

5 COLORADO CYBERSECURITY

6 **24-33.5-1901. Legislative declaration.** (1) THE GENERAL
7 ASSEMBLY HEREBY FINDS AND DECLARES THAT:

1 (a) CYBER THREATS HAVE CONTINUED TO GROW IN SIGNIFICANCE,
2 SCALE, SCOPE, AND SOPHISTICATION IN THE PAST SEVERAL YEARS;

3 (b) A DRAMATIC INCREASE IN THE NUMBER OF CYBER ATTACKS
4 AGAINST PUBLIC, PRIVATE, AND NONPROFIT ENTITIES AND INDIVIDUAL
5 CITIZENS, COUPLED WITH INADEQUATE RESOURCES TO RESPOND TO SUCH
6 ATTACKS, HAVE MADE CYBERSECURITY A TOP PRIORITY;

7 (c) COLORADO IS WELL-SUITED TO SERVE AS A LOCATION FOR
8 COMPREHENSIVE CROSS-SECTOR AND INTERSTATE STRATEGY TO SUPPORT
9 THE RESPONSE AGAINST THESE ATTACKS AND THE EDUCATION AND
10 TRAINING NEEDED TO PREPARE GOVERNMENT AND PRIVATE SECTOR
11 LEADERS TO RESPOND TO THESE ATTACKS;

12 (d) IT IS IN THE STATE'S INTEREST TO SUPPORT A PARTNERSHIP OF
13 ACADEMICS AND SYSTEMS EXCELLENCE AT THE UNIVERSITY OF COLORADO
14 AT COLORADO SPRINGS AND OTHER INSTITUTIONS OF HIGHER EDUCATION
15 THAT CAN LEVERAGE THE MILITARY, FEDERAL, STATE, AND LOCAL
16 GOVERNMENT, AND PRIVATE SECTOR ASSETS IN COLORADO TO SUPPORT
17 THE CYBERSECURITY OF OUR STATE AND LOCAL GOVERNMENTS AND TO
18 SUPPORT THE CYBERSECURITY OF FEDERAL PARTNERS AND OTHER STATES
19 AND LOCAL GOVERNMENTS ACROSS THE COUNTRY; AND

20 (e) IT IS ALSO IN THE STATE'S INTEREST TO SUPPORT SUCH A
21 PARTNERSHIP AS A TOOL TO ENSURE THAT COLORADO'S PRIVATE SECTOR
22 IS BETTER PREPARED TO RESPOND TO THREATS AND IN TURN MAKE
23 COLORADO A STRONGER HUB FOR THE CYBER INDUSTRY AND THE
24 COMMERCIALIZATION OF CYBER TECHNOLOGY.

25 (2) THE GENERAL ASSEMBLY FURTHER FINDS AND DECLARES THAT
26 THE INTENT OF THIS PART 19 IS TO IDENTIFY SPECIFIC ACTIONS TO DEFINE
27 AND IMPROVE CYBERSECURITY, INCLUDING THE CREATION OF A

1 COLORADO CYBERSECURITY COUNCIL, COORDINATING CYBER OPERATIONS
2 CENTERS, ESTABLISHING OR EXPANDING CYBER HIGHER EDUCATION
3 PROGRAMS TO PROMOTE EDUCATION, TRAINING, AND WORKFORCE
4 DEVELOPMENT FOR CYBERSECURITY, ESTABLISHING A SECURE
5 ENVIRONMENT FOR RESEARCH AND DEVELOPMENT, AND ESTABLISHING A
6 REVENUE SOURCE TO SUPPORT SUCH EFFORTS.

7 **24-33.5-1902. Colorado cybersecurity council - creation -**
8 **council members.** (1) THERE IS CREATED IN THE DEPARTMENT OF PUBLIC
9 SAFETY AND WITHIN EXISTING RESOURCES THE COLORADO
10 CYBERSECURITY COUNCIL. THE COUNCIL OPERATES AS A STEERING GROUP
11 TO DEVELOP CYBERSECURITY POLICY GUIDANCE FOR THE GOVERNOR;
12 DEVELOP COMPREHENSIVE SETS OF PRIORITIZED GOALS, REQUIREMENTS,
13 INITIATIVES, AND MILESTONES; AND COORDINATE WITH THE GENERAL
14 ASSEMBLY AND THE JUDICIAL BRANCH REGARDING CYBERSECURITY AS
15 DEEMED NECESSARY AND APPROPRIATE BY THE COUNCIL.

16 (2) THE COLORADO CYBERSECURITY COUNCIL IS COMPRISED OF
17 THE FOLLOWING MEMBERS:

18 (a) THE GOVERNOR, ACTING AS THE CHAIRPERSON OF THE
19 COUNCIL, OR THE GOVERNOR'S DESIGNEE;

20 (b) THE CHIEF INFORMATION OFFICER OF THE GOVERNOR'S OFFICE
21 OF INFORMATION TECHNOLOGY, OR THE CHIEF INFORMATION OFFICER'S
22 DESIGNEE;

23 (c) THE CHIEF INFORMATION SECURITY OFFICER OF THE
24 GOVERNOR'S OFFICE OF INFORMATION TECHNOLOGY, OR THE CHIEF
25 INFORMATION SECURITY OFFICER'S DESIGNEE;

26 (d) THE EXECUTIVE DIRECTOR OF THE DEPARTMENT OF PUBLIC
27 SAFETY, OR THE EXECUTIVE DIRECTOR'S DESIGNEE;

1 (e) A REPRESENTATIVE OF THE COLORADO NATIONAL GUARD TO
2 BE APPOINTED BY THE ADJUTANT GENERAL OF THE DEPARTMENT OF
3 MILITARY AND VETERANS AFFAIRS;

4 (f) THE ADJUTANT GENERAL OF THE DEPARTMENT OF MILITARY
5 AND VETERANS AFFAIRS;

6 (g) THE DIRECTOR OF THE COLORADO OFFICE OF ECONOMIC
7 DEVELOPMENT, OR THE DIRECTOR'S DESIGNEE;

8 (h) THE AEROSPACE AND DEFENSE INDUSTRY CHAMPION IN THE
9 COLORADO OFFICE OF ECONOMIC DEVELOPMENT;

10 (i) THE DIRECTOR OF THE GOVERNOR'S OFFICE OF STATE PLANNING
11 AND BUDGETING, OR THE DIRECTOR'S DESIGNEE;

12 (j) THE EXECUTIVE DIRECTOR OF THE DEPARTMENT OF REVENUE,
13 OR THE EXECUTIVE DIRECTOR'S DESIGNEE;

14 (k) THE STATE CONTROLLER;

15 (l) THE STATE ATTORNEY GENERAL, OR THE ATTORNEY GENERAL'S
16 DESIGNEE;

17 (m) THE DIRECTOR OF THE PUBLIC UTILITIES COMMISSION OR THE
18 DIRECTOR'S DESIGNEE;

19 (n) REPRESENTATIVES FROM INSTITUTIONS OF HIGHER EDUCATION
20 DEEMED NECESSARY AND APPROPRIATE BY THE GOVERNOR;

21 (o) THE STATE AUDITOR, OR THE STATE AUDITOR'S DESIGNEE;
22 EXCEPT THAT THE STATE AUDITOR OR THE STATE AUDITOR'S DESIGNEE
23 SHALL BE A NONVOTING MEMBER OF THE COUNCIL AND SHALL ACT SOLELY
24 IN AN ADVISORY CAPACITY WITH RESPECT TO THE COUNCIL'S ACTIVITIES;

25 (p) THE CHAIR OF THE CYBERSECURITY SUBCOMMITTEE OF THE
26 HOMELAND SECURITY AND ALL-HAZARDS SENIOR ADVISORY COMMITTEE;

27 (q) THE DIRECTOR OF THE DIVISION OF HOMELAND SECURITY AND

1 EMERGENCY MANAGEMENT IN THE DEPARTMENT OF PUBLIC SAFETY, OR
2 THE DIRECTOR'S DESIGNEE; AND

3 (r) ANY OTHER PERSON DEEMED NECESSARY AND APPROPRIATE BY
4 THE GOVERNOR.

5 (3) THE COUNCIL DOES NOT HAVE ANY DIRECT AUTHORITY OVER
6 THE UNIVERSITY OF COLORADO AT COLORADO SPRINGS.

7 (4) NOTHING IN THIS SECTION SHALL BE CONSTRUED TO INTERFERE
8 WITH THE DUTIES OF THE CHIEF INFORMATION SECURITY OFFICER
9 PURSUANT TO PART 4 OF ARTICLE 37.5 OF THIS TITLE.

10 **24-33.5-1903. Cyber operation center - coordination of**
11 **missions.** (1) THE DEPARTMENT OF PUBLIC SAFETY, USING THE OFFICE OF
12 PREVENTION AND SECURITY WITHIN THE DIVISION OF HOMELAND SECURITY
13 AND EMERGENCY MANAGEMENT, AND USING ANY OTHER FACILITIES
14 DEEMED NECESSARY AND APPROPRIATE BY THE DEPARTMENT OF PUBLIC
15 SAFETY, MAY COORDINATE WITH THE DIVISION OF HOMELAND SECURITY
16 AND EMERGENCY MANAGEMENT, THE COLORADO BUREAU OF
17 INVESTIGATION, THE FEDERAL BUREAU OF INVESTIGATION, THE COLORADO
18 NATIONAL GUARD AND OTHER RELEVANT MILITARY ORGANIZATIONS, AND
19 OTHER RELEVANT INFORMATION-SHARING ORGANIZATIONS TO DEFINE THE
20 OPERATIONAL REQUIREMENTS FOR IN-STATE AND INTERSTATE
21 OPERATIONAL AND TRAINING NETWORKS.

22 (2) IN FURTHERANCE OF THE PROVISIONS OF SUBSECTION (1) OF
23 THIS SECTION, THE COORDINATING ENTITIES MAY:

24 (a) CONSIDER ESTABLISHING APPROPRIATE MEMORANDA OF
25 UNDERSTANDING OR INTERSTATE COMPACTS WITH ENTITIES THAT
26 ENCOURAGE THE INTERSTATE SHARING OF INFORMATION FOR
27 CYBERSECURITY;

1 (b) SUPPORT THE REQUIREMENTS FOR THE FUSION OF CYBER
2 DEFENSE, CYBER SURVEILLANCE, AND INTERNATIONAL AND DOMESTIC
3 INTELLIGENCE AND LAW ENFORCEMENT OPERATIONS;

4 (c) CONSIDER SECURE, DISTRIBUTED, AND INTERACTIVE NETWORK
5 INFRASTRUCTURES FOR INTERSTATE CYBER TRAINING AND OPERATIONS;

6 (d) SUPPORT SECURE COLORADO REQUIREMENTS TO IDENTIFY
7 THREATS AND VULNERABILITIES AND PROTECT STATE CYBER
8 INFRASTRUCTURES;

9 (e) CONDUCT TRAINING, INSPECTIONS, AND OPERATIONAL
10 EXERCISES;

11 (f) ESTABLISH PROTOCOLS FOR COORDINATING AND SHARING
12 INFORMATION WITH STATE AND FEDERAL LAW ENFORCEMENT AND
13 INTELLIGENCE AGENCIES RESPONSIBLE FOR INVESTIGATING AND
14 COLLECTING INFORMATION RELATED TO CYBER-BASED CRIMINAL AND
15 NATIONAL SECURITY THREATS; AND

16 (g) SUPPORT STATE AND FEDERAL LAW ENFORCEMENT AGENCIES
17 WITH THEIR RESPONSIBILITIES TO INVESTIGATE AND PROSECUTE THREATS
18 TO AND ATTACKS AGAINST CRITICAL INFRASTRUCTURE.

19 **24-33.5-1904. Education - training - workforce development.**

20 (1) THE UNIVERSITY OF COLORADO AT COLORADO SPRINGS MAY
21 PARTNER WITH OTHER INSTITUTIONS OF HIGHER EDUCATION AND A
22 NONPROFIT ORGANIZATION THAT SUPPORTS NATIONAL, STATE, AND
23 REGIONAL CYBERSECURITY INITIATIVES TO ESTABLISH AND EXPAND CYBER
24 HIGHER EDUCATION PROGRAMS AND ESTABLISH NEEDED CYBER
25 EDUCATION AND TRAINING LABORATORIES. THE SUBJECT AREAS OF SUCH
26 HIGHER EDUCATION PROGRAMS MAY INCLUDE, BUT NEED NOT BE LIMITED
27 TO, COURSES CERTIFIED BY THE NATIONAL SECURITY AGENCY AND THE

1 UNITED STATES DEPARTMENT OF HOMELAND SECURITY; A SYSTEMS
2 ENGINEERING APPROACH TO THE STUDY OF CYBER NETWORK
3 ARCHITECTURES, THREATS, AND DEFENSES; BUSINESS MANAGEMENT;
4 FOREIGN LANGUAGE SKILLS; LEGAL ISSUES; CRYPTOLOGY; TECHNOLOGY
5 DEVELOPMENT; AND SCIENCE, TECHNOLOGY, ENGINEERING, AND
6 MATHEMATICS COURSES.

7 (2) IN FURTHERANCE OF THE PROVISIONS OF SUBSECTION (1) OF
8 THIS SECTION, THE UNIVERSITY OF COLORADO AT COLORADO SPRINGS, IN
9 CONJUNCTION WITH OTHER INSTITUTIONS OF HIGHER EDUCATION AND A
10 NONPROFIT ORGANIZATION, MAY:

11 (a) COORDINATE WITH THE UNITED STATES DEPARTMENT OF
12 HOMELAND SECURITY AND THE NATIONAL SECURITY AGENCY TO CERTIFY
13 CYBER COURSES AND CURRICULA;

14 (b) COORDINATE PLANNING FOR CYBER EDUCATION WITH
15 APPROPRIATE INSTITUTIONS OF HIGHER EDUCATION IN COLORADO, THE
16 UNITED STATES ARMY RESERVE CYBER CONSORTIUM, AND APPROPRIATE
17 NATIONAL INSTITUTIONS OF HIGHER EDUCATION THAT HAVE PROGRAMS
18 CERTIFIED BY THE DEPARTMENT OF HOMELAND SECURITY OR THE
19 NATIONAL SECURITY AGENCY;

20 (c) COORDINATE WITH COMMUNITY COLLEGES IN THE
21 DEVELOPMENT AND TRANSFERABILITY OF APPROPRIATE CURRICULUM AND
22 TECHNICAL CERTIFICATION PROGRAMS, AND PROVIDE COORDINATION FOR
23 THE DEVELOPMENT OF ELEMENTARY AND SECONDARY EDUCATION FEEDER
24 PROGRAMS;

25 (d) ESTABLISH A PUBLIC POLICY THINK TANK AS AN ACADEMIC
26 RESEARCH CENTER OF EXCELLENCE FOR GOVERNMENT, ACADEMIC, AND
27 INDUSTRIAL COMMUNICATIONS, CONFERENCES, RESEARCH, AND

1 PUBLICATIONS;

2 (e) ESTABLISH EDUCATION, INCLUDING ONLINE COURSES IF
3 APPROPRIATE, TRAINING, AND ACADEMIC SYMPOSIA FOR GOVERNMENT
4 LEADERS AT ALL LEVELS;

5 (f) ESTABLISH PROTOCOLS FOR COORDINATING AND SHARING
6 INFORMATION WITH STATE AND FEDERAL LAW ENFORCEMENT AND
7 INTELLIGENCE AGENCIES RESPONSIBLE FOR INVESTIGATING AND
8 COLLECTING INFORMATION RELATED TO CYBER-BASED CRIMINAL AND
9 NATIONAL SECURITY THREATS; AND

10 (g) SUPPORT STATE AND FEDERAL LAW ENFORCEMENT AGENCIES
11 WITH THEIR RESPONSIBILITIES TO INVESTIGATE AND PROSECUTE THREATS
12 TO AND ATTACKS AGAINST CRITICAL INFRASTRUCTURE.

13 (3) THE UNIVERSITY OF COLORADO AT COLORADO SPRINGS SHALL
14 PARTICIPATE IN ACTIVITIES IN FURTHERANCE OF THIS SECTION ONLY UPON
15 THE APPROVAL OF THE BOARD OF REGENTS OF THE UNIVERSITY OF
16 COLORADO, IF REQUIRED BY THE LAWS AND POLICIES OF THE BOARD OF
17 REGENTS.

18 **24-33.5-1905. Research and development.** (1) THE UNIVERSITY
19 OF COLORADO AT COLORADO SPRINGS MAY PARTNER WITH A NONPROFIT
20 ORGANIZATION THAT SUPPORTS NATIONAL, STATE, AND REGIONAL
21 CYBERSECURITY INITIATIVES TO WORK TO ESTABLISH A SECURE
22 ENVIRONMENT FOR RESEARCH AND DEVELOPMENT, INITIAL OPERATIONAL
23 TESTING AND EVALUATION, AND EXPEDITED CONTRACTING FOR
24 PRODUCTION FOR INDUSTRIAL CYBER PRODUCTS AND TECHNIQUES.

25 (2) IN FURTHERANCE OF THE PROVISIONS OF SUBSECTION (1) OF
26 THIS SECTION, THE UNIVERSITY OF COLORADO AT COLORADO SPRINGS
27 AND ANY NONPROFIT ORGANIZATION WITH WHICH THE UNIVERSITY HAS A

1 PARTNERSHIP, MAY CONSIDER THE FOLLOWING:

2 (a) CREATING A BUSINESS PLAN TO DEVELOP A SECURE FACILITY
3 ON THE PROPERTY OF THE UNIVERSITY OF COLORADO AT COLORADO
4 SPRINGS THAT PROVIDES PHYSICAL, ELECTRONIC, PROPRIETARY, AND
5 ADMINISTRATIVE SECURITY;

6 (b) EXPLORING SECURE FACILITY DEVELOPMENT AND USE AT
7 OTHER COLORADO UNIVERSITIES AND FACILITIES THAT MAY AUGMENT THE
8 CAPACITY AT THE UNIVERSITY OF COLORADO AT COLORADO SPRINGS AND
9 ENABLE COLLABORATIVE ACTIVITIES;

10 (c) ESTABLISHING RELATIONSHIPS WITH APPROPRIATE FEDERALLY
11 FUNDED RESEARCH AND DEVELOPMENT CORPORATIONS UNDER THE
12 SPONSORSHIP OF THE UNITED STATES DEPARTMENT OF DEFENSE AND THE
13 UNITED STATES DEPARTMENT OF HOMELAND SECURITY AS AN
14 ADMINISTRATIVE PARTNER TO:

15 (I) ESTABLISH AND CERTIFY A TOP SECRET AND SPECIAL
16 ACCESS-CERTIFIED FACILITY;

17 (II) ESTABLISH COOPERATIVE RELATIONS WITH STATE AND
18 FEDERAL LAW ENFORCEMENT AND INTELLIGENCE AGENCIES RESPONSIBLE
19 FOR INVESTIGATING AND COLLECTING INFORMATION RELATED TO
20 CYBER-BASED CRIMINAL AND NATIONAL SECURITY THREATS;

21 (III) ACT AS A CONDUIT FOR FEDERAL AND INTERSTATE RESEARCH
22 AND DEVELOPMENT REQUIREMENTS;

23 (IV) ESTABLISH AND MONITOR NONDISCLOSURE AGREEMENTS TO
24 PROTECT PROPRIETARY INTELLECTUAL PROPERTY; AND

25 (V) PROCESS AND HOLD SECURITY CLEARANCES FOR AUTHORIZED
26 COLORADO GOVERNMENT PERSONNEL;

27 (d) CONSIDER ESTABLISHING RELATIONSHIPS WITH THE EXISTING

1 MITRE NATIONAL CYBERSECURITY FEDERALLY FUNDED RESEARCH AND
2 DEVELOPMENT CENTER; THE AEROSPACE CORPORATION FEDERALLY
3 FUNDED RESEARCH AND DEVELOPMENT CENTER; OR CREATING A NEW
4 PARALLEL ORGANIZATION FOCUSED ON CYBERSECURITY FOR NATIONAL
5 DEFENSE AND HOMELAND SECURITY REQUIREMENTS;

6 (e) ESTABLISHING COOPERATIVE RELATIONSHIPS WITH COLORADO
7 CYBER COMPANIES AND OTHER BUSINESSES, LOCAL GOVERNMENTS,
8 INSTITUTIONS OF HIGHER EDUCATION, AND OTHER COLORADO
9 ORGANIZATIONS WITH REQUIREMENTS FOR CYBERSECURITY
10 PARTICIPATION;

11 (f) ESTABLISHING COOPERATIVE RELATIONS WITH CIVILIAN
12 INDUSTRIAL PRODUCERS THROUGH ENTITIES THAT ENCOURAGE THE
13 INTERSTATE SHARING OF INFORMATION FOR CYBERSECURITY;

14 (g) LINKING TO LOCAL AND NATIONAL MILITARY, HOMELAND
15 SECURITY, AND INTELLIGENCE COMMUNITY ACTIVITIES TO SUPPORT
16 RESEARCH AND DEVELOPMENT, RAPID TEST AND EVALUATION,
17 CONTRACTING, AND PRODUCTION REQUIREMENTS;

18 (h) ESTABLISH PROTOCOLS FOR COORDINATING AND SHARING
19 INFORMATION WITH STATE AND FEDERAL LAW ENFORCEMENT AND
20 INTELLIGENCE AGENCIES RESPONSIBLE FOR INVESTIGATING AND
21 COLLECTING INFORMATION RELATED TO CYBER-BASED CRIMINAL AND
22 NATIONAL SECURITY THREATS; AND

23 (i) SUPPORT STATE AND FEDERAL LAW ENFORCEMENT AGENCIES
24 WITH THEIR RESPONSIBILITIES TO INVESTIGATE AND PROSECUTE THREATS
25 TO AND ATTACKS AGAINST CRITICAL INFRASTRUCTURE.

26 (3) THE UNIVERSITY OF COLORADO AT COLORADO SPRINGS SHALL
27 PARTICIPATE IN ACTIVITIES IN FURTHERANCE OF THIS SECTION ONLY UPON

1 THE APPROVAL OF THE BOARD OF REGENTS OF THE UNIVERSITY OF
2 COLORADO, IF REQUIRED BY THE LAWS AND POLICIES OF THE BOARD OF
3 REGENTS.

4 **24-33.5-1906. Cybersecurity cash fund - cybersecurity gifts,**
5 **grants, and donations account - creation.** (1) (a) THE CYBERSECURITY
6 CASH FUND, REFERRED TO IN THIS SECTION AS THE "FUND", IS HEREBY
7 CREATED IN THE STATE TREASURY. THE FUND CONSISTS OF THE MONEY
8 TRANSFERRED TO THE FUND PURSUANT TO PARAGRAPH (b) OF THIS
9 SUBSECTION (1) AND ANY OTHER MONEY THAT THE GENERAL ASSEMBLY
10 MAY APPROPRIATE OR TRANSFER TO THE FUND.

11 (b) ON JULY 1, 2016, THE STATE TREASURER SHALL TRANSFER
12 SEVEN MILLION NINE HUNDRED THIRTY-TWO THOUSAND TWENTY DOLLARS
13 FROM THE GENERAL FUND TO THE FUND.

14 (2) THE STATE TREASURER SHALL CREDIT ALL INTEREST AND
15 INCOME DERIVED FROM THE DEPOSIT AND INVESTMENT OF MONEY IN THE
16 FUND TO THE FUND.

17 (3) THE STATE TREASURER SHALL CREDIT ANY UNEXPENDED AND
18 UNENCUMBERED MONEYS REMAINING IN THE FUND AT THE END OF A
19 FISCAL YEAR TO THE FUND.

20 (4) EXCEPT FOR MONEYS IN THE CYBERSECURITY GIFTS, GRANTS,
21 AND DONATIONS ACCOUNT CREATED IN SUBSECTION (5) OF THIS SECTION,
22 SUBJECT TO ANNUAL APPROPRIATION BY THE GENERAL ASSEMBLY, THE
23 REGENTS OF THE UNIVERSITY OF COLORADO MAY EXPEND MONEY FROM
24 THE FUND FOR THE PURPOSES OF THIS PART 19.

25 (5) (a) THE CYBERSECURITY GIFTS, GRANTS, AND DONATIONS
26 ACCOUNT, REFERRED TO IN THIS SUBSECTION (5) AS THE "ACCOUNT", IS
27 HEREBY CREATED IN THE CYBERSECURITY CASH FUND. THE ACCOUNT

1 CONSISTS OF ANY GIFTS, GRANTS, OR DONATIONS CREDITED TO THE
2 ACCOUNT PURSUANT TO PARAGRAPH (b) OF THIS SUBSECTION (5). MONEYS
3 IN THE ACCOUNT ARE CONTINUOUSLY APPROPRIATED TO THE DEPARTMENT
4 OF HIGHER EDUCATION FOR USE BY THE REGENTS OF THE UNIVERSITY OF
5 COLORADO FOR THE PURPOSES OF THIS PART 19.

6 (b) THE REGENTS OF THE UNIVERSITY OF COLORADO MAY SEEK,
7 ACCEPT, AND EXPEND GIFTS, GRANTS, OR DONATIONS FROM PRIVATE OR
8 PUBLIC SOURCES FOR THE PURPOSES OF THIS PART 19. THE REGENTS OF
9 THE UNIVERSITY OF COLORADO SHALL TRANSMIT ALL MONEY RECEIVED
10 THROUGH GIFTS, GRANTS, OR DONATIONS TO THE STATE TREASURER, WHO
11 SHALL CREDIT THE MONEY TO THE ACCOUNT.

12 **SECTION 2.** In Colorado Revised Statutes, 24-75-402, **add** (5)
13 (jj) as follows:

14 **24-75-402. Cash funds - limit on uncommitted reserves -**
15 **reduction in amount of fees - exclusions - repeal.** (5) Notwithstanding
16 any provision of this section to the contrary, the following cash funds are
17 excluded from the limitations specified in this section:

18 (jj) THE CYBERSECURITY CASH FUND CREATED IN SECTION
19 24-33.5-1906.

20 **SECTION 3. Appropriation.** For the 2016-17 state fiscal year,
21 \$7,932,020 is appropriated to the department of higher education for use
22 by the regents of the university of Colorado. This appropriation is from
23 the cybersecurity cash fund created in section 24-33.5-1906 (1), C.R.S.
24 To implement this act, the regents of the university of Colorado may use
25 this appropriation for the university of Colorado at Colorado Springs for
26 establishing and expanding cyber higher education programs and cyber
27 education training laboratories and for establishing a secure environment

1 for research and development, initial operational testing and evaluation,
2 and expedited contracting for production for industrial cyber products and
3 techniques.

4 **SECTION 4. Appropriation.** (1) For the 2016-17 state fiscal
5 year, \$67,980 is appropriated to the department of public safety for use
6 by the office of prevention and security. This appropriation is from the
7 general fund. To implement this act, the office may use this appropriation
8 as follows:

9 (a) \$62,327 for personal services, which amount is based on an
10 assumption that the office will require an additional 1.0 FTE; and

11 (b) \$5,653 for operating expenses.

12 **SECTION 5. Effective date.** This act takes effect July 1, 2016.

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