STATE BOARD FOR COMMUNITY COLLEGES AND OCCUPATIONAL EDUCATION

TOPIC: Bachelor of Applied Science in Cybersecurity

PRESENTED BY: Dr. Patricia Erjavec, President of Pueblo Community College, and Dr. Michele Haney, President of Red Rocks Community College

RELATIONSHIP TO CCCS STRATEGIC PLAN:
Transform the student experience; create education without barriers through transformational partnerships; and refine our value proposition through accessibility, affordability, quality, accountability, resource development, and operational excellence.

EXPLANATION:
Pursuant to CCCS's role and mission (§23-60-201, C.R.S.), CCCS may offer technical, career, and workforce development Bachelor of Applied Science (BAS) degree programs. Authority for the Colorado Community College System to offer BAS degrees was made possible by SB14-004 (Community College Four-year Programs), signed by the Governor on February 27, 2014.

This proposal seeks approval from the State Board for Community Colleges and Occupational Education (SBCCOE) for a BAS degree in Cybersecurity for 4 of the CCCS Community Colleges:

- Arapahoe Community College (ACC)
- Pikes Peak State College (PPSC)
- Pueblo Community College (PCC)
- Red Rocks Community College (RRCC)

The legislative criteria for approval of a BAS degree are set forth, with a summary and data demonstrating that the criteria have been met. Additional information is provided in board packets prepared by each of the colleges.

Executive Summary

The Colorado Community College System (CCCS) continues to make strides in creating a suite of Bachelor of Applied Science (BAS) degrees to support the statewide student population. The consortium of colleges listed above have collaborated extensively and will continue to do so. This approach has resulted in:

- Development of this degree
    - Unique, new courses including materials
    - Course sequencing
    - Program Learning Outcomes
    - Specialized emphases for the BAS in Cyber Security
- Utilization of industry credentials
    - Expedite time to completion through Credit for Prior Learning
    - Provides added value to students
    - Increases a student's employment marketability

- Strategic approaches to
  - Cost-effective compensation for instructors
  - Consistent, quality course delivery

Cybersecurity impacts every industry in the global economy, including but not limited to finance and banking, manufacturing, healthcare, information, technology, and education. Within the state of Colorado, occupations addressing Information Security have high projected growth rates. Below is a sample of occupations illustrating projected growth rates, annual job openings, and the 2022 median wages, all in the state of Colorado. A bachelor's degree is predominantly listed as the educational attainment level.

- 15.1212.00. Information Security Analysts, 28% projected growth from 2020-2030 with 420 annual job openings, 2022 median wage of $53.85 hour.
- 15.1299.04. Penetration Testers, 22% projected growth from 2020-2030 with 1,470 annual job openings, 2022 median wage of $47.47 hour.
- 15.1244.00. Network and Computer Systems Administrators, 22% projected growth from 2020-2030 with 1,120 annual job openings, 2022 median wage of $43.52 hour.
- 15.1211.00. Computer Systems Analysts, 21% projected growth from 2020-2030 with 900 annual job openings, 2022 median wage of $49.15 hour.

Data obtained from the Bureau of Labor Statistics, as published per occupation at https://www.onetonline.org/. (January 2024).

Each participating college has submitted a comprehensive packet demonstrating the criteria needed to fulfill the program approval (key assessment) requirements. These include:

- **Workforce demand**. Lightcast reports illustrate regional industry demand for
  - 11.1003, Computer and Information Systems Security/Auditing/Information Assurance
  - 15.1299, Computer Engineering Technologies/Technicians/Others
- **Student demand** as demonstrated through institutional surveys
- **Financial analysis**
- **Staffing analysis**, and
- **Student support services analysis**

Financial Analysis Methodology

The financial analysis for the BAS in Cybersecurity utilizes the Colorado Online Consortia model. For at least the first two years, the BAS course offerings will be delivered through Colorado Online. After that the four participating colleges will determine if additional modalities of educational delivery will enhance student success for the consortia and local student populations. However, it is highly likely that most courses will continue to be delivered online, as the current population enrolled in the AAS pipeline programs are adult, working students attending school on a part time basis. The Summary Financial Analysis includes total enrollments for all four colleges and the instructional costs are aggregated for all four colleges. The board packets prepared by the each of the individual colleges include a college-based financial analysis. These analyses incorporate the percentage of enrollment represented by their college and the instructional costs for the courses delivered by that institution. Specific planning of course delivery is strategically based on ability to deliver, expertise of the faculty, and equitable distribution among participating colleges.

A simplified model was used for the financial statements in which COF is distributed based on the percentage of enrollment for each college. Additionally, a consistent pay rate for faculty and instructors was used and reflects a rate at the high end of the spectrum. Some colleges will have lower compensation rates but the difference is minor.

Bachelor of Applied Science Degree Requirements

The Bachelor of Applied Science degree is a flexible baccalaureate program designed to create additional opportunities for workforce development and advancement through increased technical skill attainment. The Program Learning Outcomes for the BAS Program in Cyber Security are as follows:

1. Describe cyber defense tools, methods, and components and apply cyber defense methods to proactively repel attacks.
2. Analyze common security failures by identifying violations of specific design principles and the corrective action steps.
3. Identify unethical practices in cyberspace and compare their resources, capabilities/ techniques, motivations, and aversion to risk.
4. Explain the applicable laws and policies related to cyber defense, the major components of data storage and transmission, and legal and ethical issues associated with cyber threats, including the circumstances in which vulnerabilities and incidents must be disclosed internally and externally.
5. Evaluate industry tools and techniques used to identify vulnerabilities, create a vulnerability map, and trace a vulnerability to its root cause; to propose and analyze countermeasures that mitigate potential and real damage.
6. Describe and perform the digital forensics steps from the initial recognition of an incident, evidence gathering, preservation, analysis, and the subsequent legal proceedings and the formal Security Incident Analysis and Response.
7. Identify, develop, and implement plans to include adjustments for lessons learned, alternative solutions, and strategies for holistic organization-wide security and business continuity.

The BAS degree in Cyber Security consists of 120 credits. As a stackable credential, 60 or more credits from a relevant Associate Degree will meet BAS degree requirements. The degree is designed so that students who have earned an AAS degree in Cyber Security, Networking, and Secure Software Development will be prepared to enter the program as a junior. Students entering the program with an AGS, an AA in Computer Science, or from a program outside of the Community College System, may need to take some additional technical courses to be fully prepared for the upper division Cyber Security courses. However, it is likely that they will have more of their general education requirements completed upon entering the program.

BAS Cyber Security Program Credits

Course Level	Description	Credits
AAS Courses	General Education Courses[1]	16
	Non-GE courses	44
BAS Courses	General Education Courses	9
	Elective or Bridge Courses	7
	BAS Core Requirements	28
	CNG 3020, Cyber Law, Ethics and Policy	(4)
	CNG 3036, Business Continuity and Disaster Recover	(4)
	CNG 3040, Cyber Operations	(4)
	CNG 3050, Cyber investigations and Forensics	(4)
	CNG 3056, Vulnerability Assessment II	(4)
	CNG 4000, Active Cyber Defense	(4)
	CNG 4010, Cyber Threat Intelligence	(4)
	Specialization Emphasis Courses[2]	16
	Network Security Operations Emphasis Options (Choose 16 Credits)	
	CNG 3010, Fundamentals of Cyber Security	(4)
	CNG 3030, Methods of Network Analysis	(4)
	CNG 4020, Zero Trust Networks	(4)
	CNG 4030, Cyber War	(4)
	CNG 4054, Malware Threats and Analysis	(4)
	CNG 4XXX (A course to be developed or an Internship)	(4)
	TOTAL CREDITS	**120**

1. General Education Courses must include an ENG GT: CO1 (3 CR), an ENG GT: CO2 (3 CR), MAT 1340, College Algebra GT:MA1 (4 CR), and MAT 1400, Survey of Calculus GT:MA1 (4 CR) or higher.
2. This proposal is for the Cyber Security BAS with an Emphasis in *Network Security Operations*. Students will choose 16 credits from a list of courses within the Specialized Emphasis Content. Future emphases with the corresponding courses will be constructed utilizing this model.

Attachments:

Lightcast Labor Market Report for the State of CO
Summary Financial Analysis for Consortium
BAS Cybersecurity Courses
Board Packets: ACC, PPSC, PCC, RRCC