

**Docket Item:**

University Program Approval: Eastern Oregon University, Bachelor of Art (B.A.)/ Bachelor of Science (B.S.)/  
Bachelor of Applied Science (B.A.S.) in Cyber Security.

**Summary:**

Eastern Oregon University proposes a new degree program leading to a B.A./B.S./B.A.S. in Cyber Security. The statewide Provosts' Council has unanimously recommended approval. Higher Education Coordinating Commission (HECC) staff completed a review of the proposed program. After Analysis, HECC staff recommends approval of the program as proposed.

**Staff Recommendation:**

The HECC recommends the adoption of the following resolution:

RESOLVED, that the Higher Education Coordinating Commission approve the following program:

B.A./B.S./B.A.S., in Cyber Security at Eastern Oregon University.



## Proposal for a New Academic Program

**Institution:** Eastern Oregon University

**College/School:** College of STM and Health Science

**Department/Program Name:** Computer Science

**Degree and Program Title:** BA/BS/BAS of Cyber Security

### 1. Program Description

- a. Proposed Classification of Instructional Programs (CIP) number.

*11.1003 Computer and Information Systems Security*

- b. Brief overview (1-2 paragraphs) of the proposed program, including its disciplinary foundations and connections; program objectives; programmatic focus; degree, certificate, minor, and concentrations offered.

*We are proposing the establishment of Bachelor of Art (BA), Bachelor of Science (BS) and Bachelor of Applied Science (BAS) degrees in Cyber Security at Eastern Oregon University. The BA/BS options for Cyber Security carry requisite general education, elective, and institutional requirements in satisfaction of the degree. The BAS option for Cyber Security requires an earned Applied Associate's degree that is transferred in, plus satisfaction of 45 general education credits and satisfaction of all other upper division required elective and institutional requirements towards the degree.*

*The Cyber Security program at EOU will be a practical, skill-focused, technical degree with a strong foundation in computer science. Students will be taught from multiple domains of information security, with alignment to industry certifications and standards. The proposed courses emphasize labs and hands-on assignments. Classroom time will focus on the operational aspects that will provide students an applied vs theoretical understanding of the field. Likewise, managerial or business elements will be spoken to, but not the priority. The goal is students will graduate with the technical background of a cyber security generalist who can later specialize in their areas of interest while in the workforce.*

- c. Course of study – proposed curriculum, including course numbers, titles, and credit hours.

### Core Computer Science Courses

## Existing EOU Courses

<b>Num.</b>	<b>Course Name</b>	<b>Credits</b>	<b>Description</b>
CS 221	C/C++ Programming	4	An introduction to the basics of programming as used in C and C++, including selection statements, loops, arrays, string handling, pointers, registers and functions. Practical exercises will require the construction, compilation, debugging, and execution of complete programs that implement given algorithms to solve simple problems. The emphasis in this course will be on the common features of C and C++; however, memory allocation and the use of pointers will be discussed.
CS 314	Architecture & Assembly	4	A study of how computers are designed and organized at the hardware level. Topics covered include basic logic circuits, gates, processors, memory, instruction sets and programming in assembly language.
CS 335	Networking & Network Admin	4	An introductory examination of the Open System Interconnection Reference Model (OSI). Topics covered include network architecture, data flow control, transmission control, path control, recovery, and routing techniques.
CS 361	Software Engineering I	4	Covers models of software development, with emphasis on the prototyping model, and user interface design. Students will design an interactive product, producing deliverables for each stage of design up to the development of a working prototype.

## Core Cyber Security Courses

### *New courses to be developed*

<b>Num.</b>	<b>Course Name</b>	<b>Credits</b>	<b>Description</b>
CS 372	Operational Cyber Security Essentials	4	A hands-on examination of cyber security concepts that cover both the defensive and offensive arenas. This course provides students with foundational technical cyber security skills needed for success in both a Windows and Linux environment.
CS 373	Foundations of Information Security Management	4	A survey of the principal topics across the information security field. This course provides students a broad understanding of the field, the terminology, and the industry standards governing it.
CS 350	Wireless & RF Fundamentals and Security	4	A study of basic radio frequency communication & the associated security implementations. This course provides students with a foundation in how systems communicate over various wireless technologies, such as WiFi, RFID & Bluetooth and the actions taken to secure them.
CS 386	System Hardening & Secure	4	An applied study of how to secure Windows and

## Configurations

				Linux environments. This course provides students the necessary skills to build defensible environments in order to both limit the likelihood of a breach, as well as detect a security incident. Defensive concepts will be paired with the attack scenarios to aid students in understanding why certain actions are preferred.
CS 412	Incident Response & System Forensics	4		A practical examination of how to respond to a security breach and perform system forensics. This course provides students the skills and knowledge necessary to aid during a security breach or malicious activity at an organization. Topics start with the necessary planning preparations and continues through detecting, containing, performing system forensics, and finally documenting and dealing with law enforcement or governing agencies.
CS 431	Application Security	4		A pragmatic study of application security from development through deployment. This course provides students the skills for finding common vulnerabilities in software, identifying deployment and configuration failures, understanding how vulnerable software is exploited and documenting findings for business leaders.
CS 432	Offensive Security Techniques & Tactics	4		An in-depth examination of the tactics and techniques used by security professionals to assess the defensive posture of an organization, as well as those used by malicious attackers. This course provides students with the necessary skills to perform "red team" and network penetration assessments used in a corporate environment, as well as provide a foundation in threat intelligence.
Cs 413	Reverse Engineering & Malware Analysis	4		A study of reverse engineering applications with a focus on the analysis of malicious software. This course covers a review of assembly languages, the use of a decompiler & debugger, static & behavioral analysis. Students will understand the tools and methodology used to reverse applications, and the techniques used by malware.

- d. Manner in which the program will be delivered, including program location (if offered outside of the main campus), course scheduling, and the use of technology (for both on-campus and off-campus delivery).

*The program curriculum will be offered on Campus and online delivery formats. The initial focus will be in person at EOU's La Grande campus. For beginning online students, the required core computer science courses are already offered online in a combination of asynchronous and synchronous activities. Likewise, the newly developed courses will feature this mixture of activities, using formats such as recorded lectures or "virtual live" classes where teleconferencing technology is used to present to remote students. It is acknowledged that information security is a field into which many transition from*

*related career fields. Therefore, delivery for those who cannot attend traditional class hours will be important to the program success.*

- e. Adequacy and quality of faculty delivering the program.

*Mr. Kiel Wadner has taken lead on the development of courseware and will be the primary instructor. He obtained a B.S. in Software Engineering from the Oregon Institute of Technology, and later a M.S. in Information Security Engineering from the SANS Technology Institute. He holds 10 industry certifications across the spectrum of information security. His industry experience spans 14 years with 8 focused on information security.*

- f. Adequacy of faculty resources – full-time, part-time, adjunct.

*Mr. Wadner is currently part-time at Eastern Oregon University, which is sufficient for development of the curriculum and for instruction of the first year of the program. The use of adjuncts or hiring additional part-time instructor will be necessary after the first year. Due to maintaining a presence in the industry, it is plausible Mr. Wadner's contacts can be used to recruit adjuncts with deep industry experience.*

- g. Other staff.

*EOU's Computer Science Department is currently staffed with quality faculty to handle the core computer science courses that are part of the program curriculum.*

- h. Adequacy of facilities, library, and other resources.

*Due to ability to virtualizing computer systems and cloud computing, an additional on premises lab environment will not be necessary. This also allows students to work on their own systems, utilize the existing lab infrastructure or incurring lab costs as OPEX per term if desired. As this is a highly technical degree, students will be required to have a computer meeting minimum standards. A new laptop meeting those standards is currently between \$800 – 1,000*

*Some additional books may need to be added to the campus library over time. However, as a digital first career field, many quality resources are available in digital formats and often free.*

- i. Anticipated start date.

*Fall 2021*

## **2. Relationship to Mission and Goals**

- a. Manner in which the proposed program supports the institution's mission, signature areas of focus, and strategic priorities.

*By offering a BA/BS/BAS of Cyber Security, EOU is reinforcing the commitment to partner with other educational institutions, specifically the community colleges of the region. It*

*will also add to the quality of education by providing additional areas of focus in a growing computer science department.*

*This program fulfills multiple goals stated in EOU's Strategic Plan, i.e. Goal 1 (Student Success: Objective 1: All graduates engage in high-impact, experiential learning activities), Goal 2 (Transformational Education: Objective 2: Graduates possess the essential learning outcomes employers seek), Goal 3 (Grow the Number of Lives Impacted: Objective 1: Serve as a growing and thriving rural university), and Goal 5 (Relevance and Interconnection: Objective 2: Be recognized as a leader in promoting rural community prosperity and resilience).*

- b. Manner in which the proposed program contributes to institutional and statewide goals for student access and diversity, quality learning, research, knowledge creation and innovation, and economic and cultural support of Oregon and its communities.

*The information security field is globally diverse and interconnected. A yearly conference that started in 1993 now attracts over 30,000 individuals across the globe. However, talent pools tend center around urban areas to the exclusion of rural populations. As Oregon's Rural University, a quality information security program will provide opportunities for those who presently chose a life outside of city centers.*

- c. Manner in which the program meets regional or statewide needs and enhances the state's capacity to:
  - I. improve educational attainment in the region and state;
  - II. respond effectively to social, economic, and environmental challenges and opportunities; and
  - III. address civic and cultural demands of citizenship.

*A Cyber Security program at EOU fulfills two needs (1) Oregon currently does not have a Bachelor's degree program in information security with an emphasis on operational application. Students who wish to pursue this must look at institutions outside of the state of Oregon. (2) Growth in the information security field continues and increasingly impacts other fields. As industries change through automation and technical transformation there will be individuals who need avenues to other career options. Combined, the needs of this program are likely to expand. By partnering with other institutions who offer AAS degrees, a regional two-step process will exist for those with an interest in information security. Thus, this program meets a regional need, first by providing students in regional community colleges a path for continuation to a baccalaureate degree at a regional institution, and, second, meets with the workforce needs of a growing regional industry base in computer science/information security/data center operations as well as the growing need of business with a critical need for a secure online presence.*

### **3. Accreditation**

- a. Accrediting body or professional society that has established standards in the area in which the program lies, if applicable.

*Northwest Commission on Colleges and Universities (NWCCU)*

- b. Ability of the program to meet professional accreditation standards. If the program does not or cannot meet those standards, the proposal should identify the area(s) in which it is deficient and indicate steps needed to qualify the program for accreditation and date by which it would be expected to be fully accredited.

*Program will meet all NWCCU standards.*

- c. If the proposed program is a graduate program in which the institution offers an undergraduate program, proposal should identify whether or not the undergraduate program is accredited and, if not, what would be required to qualify it for accreditation.

*Not Applicable.*

- d. If accreditation is a goal, the proposal should identify the steps being taken to achieve accreditation. If the program is not seeking accreditation, the proposal should indicate why it is not.

*NWCCU notification will occur after HECC approval.*

**4. Need**

- a. Anticipated fall term headcount and FTE enrollment over each of the next five years.

*Is expected that student headcounts for the first five years will be (separated by modality):*

Number of Students	Year 1	Year 2	Year 3	Year 4	Year 5
On Campus	7	22	41	52	52
Online	10	23	39	52	66
Total	17	45	80	104	118

- b. Expected degrees/certificates produced over the next five years.

*BA/BS/BAS of Cyber Security*

*Certificate of Cyber Security*

- c. Characteristics of students to be served (resident/nonresident/international; traditional/ nontraditional; full-time/part-time, etc.).

*The program will be tailored to students who have achieved an AAS from another institution and to students who enter as freshmen. Mathematics requirements were chosen appropriately for the degree content and the expected student clientele. (The existing computer science degree requires substantively higher mathematics knowledge.) It is expected those who enroll will be a combination of full-time and part-time residence of Oregon or the surrounding region.*

- d. Evidence of market demand.

*Burning Glass Technologies stated in a recent market analysis that “From September 2017 through August 2018, there were 313,735 cybersecurity job openings across the United States, accounting for 13% of all IT jobs. Demand for these roles has grown at a*

*rapid pace, increasing 94% since 2013. By comparison, demand for all IT jobs grew only 30% during the same period.” (Recruiting Watchers for the Virtual Walls, June 2019).*

- e. If the program’s location is shared with another similar Oregon public university program, the proposal should provide externally validated evidence of need (e.g., surveys, focus groups, documented requests, occupational/employment statistics and forecasts).

*Not applicable*

- f. Estimate the prospects for success of program graduates (employment or graduate school) and consideration of licensure, if appropriate. What are the expected career paths for students in this program?

*Probability of employment success can be mapped to three factors: Skills, available jobs, long term needs. (1) By focusing the program curriculum on applied skills, it will assist students to both know the necessary information for interviews to get a job, but also to perform with success from the start. (2) With market demand growing and high number of vacancies existing, the potential opportunity is high. (3) Technology will continue to become more integrated into human lives. As the integration happens the value society places on security and safety will likely increase as well. This provides long-term prospects for employment.*

*With those three factors, it is believed graduates will have a strong prospect for a career or foundation needed for graduate schools.*

## **5. Outcomes and Quality Assessment**

- a. Expected learning outcomes of the program.
  - (1) *An understanding of the different areas of specialization in information security such as forensics, incident response, application security, etc.*
  - (2) *An ability to explain the foundational concepts of information security such as authorization, accessibility, privacy, data security, least privilege, etc.*
  - (3) *An ability to demonstrate the core technical skills used across the field such as a proficiency in scripting, system administration, vulnerability analysis, networking, etc.*
  - (4) *An ability to explain and demonstrate entry-level proficiency in defensive areas such as secure architecture, incident response, and forensics.*
  - (5) *An ability to explain and demonstrate entry-level proficiency in offensive areas such as application and network security assessments, attacker tactics and techniques, and the mitigating actions to take.*
  - (6) *A demonstrated ability to organize and communicate deliverables from information security projects and activities to both technical and non-technical audiences.*
- b. Methods by which the learning outcomes will be assessed and used to improve curriculum and instruction.

*Learning objectives will be continually compared to industry certification standards to ensure relevancy of topics. Student scores on assessments will be used to measure what learning objectives are receiving an appropriate amount of attention to convey the needed skill sets.*

- c. Nature and level of research and/or scholarly work expected of program faculty; indicators of success in those areas.

*With the fast-changing pace of technology and the information security field, faculty that remain involved in the professional industry will be preferred. Continued research and publication through informal means will provide credence to the quality of the program.*

## **6. Program Integration and Collaboration**

- a. Closely related programs in this or other Oregon colleges and universities.

*Mt. Hood Community College offers an AAS related to cyber security and conversations with them has begun. Additional outreach to other schools including Portland Community College and the Oregon Institute of Technology is will be conducted.*

- b. Ways in which the program complements other similar programs in other Oregon institutions and other related programs at this institution. Proposal should identify the potential for collaboration.

*By offering both a BA/BS and a BAS program at the start, several students entry levels will exist. The BAS degree will allow close collaboration with those institutions offering technical AAS programs. Collaboration with Mt. Hood Community College has started, and more collaboration is desired.*

- c. If applicable, proposal should state why this program may not be collaborating with existing similar programs.

*Not applicable*

- d. Potential impacts on other programs.

*No negative impacts known at this time.*



EASTERN OREGON  
UNIVERSITY

## Program Approval Format for HECC Docket Submission

### Consent Agenda Sentence

Eastern Oregon University seeks the Oregon Higher Education Coordinating Commission approval to offer an instructional program leading to a BA/BS/BAS of Cyber Security.

### Program Description and Justification

1. Identify the institution, degree, and title of the program.  
Eastern Oregon University BA/BS/BAS of Cyber Security

2. Describe the purpose and relationship of the proposed program to the institution's mission and strategic plan.

The Cyber Security program at EOU will be a practical, skill-focused, technical degree with a strong foundation in computer science. Students will be taught from multiple domains of information security, with alignment to industry certifications and standards. The proposed courses emphasize labs and hands-on assignments. Classroom time will focus on the operational aspects that will provide students an applied vs theoretical understanding of the field. The goal is students will graduate with the technical background of a cyber security generalist who can later specialize in their areas of interest while in the workforce.

This program fulfills multiple goals stated in EOU's Strategic Plan, i.e. Goal 1 (Student Success: Objective 1: All graduates engage in high-impact, experiential learning activities), Goal 2 (Transformational Education: Objective 2: Graduates possess the essential learning outcomes employers seek), Goal 3 (Grow the Number of Lives Impacted: Objective 1: Serve as a growing and thriving rural university), and Goal 5 (Relevance and Interconnection: Objective 2: Be recognized as a leader in promoting rural community prosperity and resilience).

3. What evidence of need does the institution have for the program?

The information security field is globally diverse and interconnected. Burning Glass Technologies stated in a recent market analysis that "From September 2017 through August 2018, there were 313,735 cybersecurity job openings across the United States, accounting for 13% of all IT jobs. Demand for these roles has grown at a rapid pace, increasing 94% since 2013. Talent pools, however, tend to center around urban areas to the exclusion of rural populations. As Oregon's Rural University, a quality information security program will provide opportunities for those who presently chose a life outside of city centers and provide ubiquitous information security to these regions. Regional demand was assessed by screening job databases using the corroding SOC codes. Moreover, the BAS degree option is provided following conversations with community colleges for a cyber security degree pathway for their AAS graduates in cyber security and related fields.

4. Are there similar programs in the state? If so, how does the proposed program supplement, complement, or collaborate with those programs?

While there are cyber-security-related program in the State of Oregon, EOU's proposed program is distinct in that it focusses on the cyber security needs of small businesses, school districts, agencies in particularly in rural Eastern Oregon and other rural areas and, hence, has practical, skill-focused, technical curriculum that provides a broad technical background of a cyber security generalist who can later specialize in their areas of interest while in the workforce.

*In a separate paragraph, include the following sentence:*

All appropriate University committees and the Statewide Provosts Council have approved the proposed program. The Eastern Oregon University Board of Trustees approved the program on June 4, 2020.

### **Recommendation to the Commission**

The Statewide Provosts Council recommends that the Oregon Higher Education Coordinating Commission authorize Eastern Oregon University to establish an instructional program leading to a **BA/BS/BAS** of Cyber Security, effective Fall 2021.

Note: A signature page showing how the provosts voted on the program will need to be submitted along with this write-up.

*Revised May 2016*

**Institution: Eastern Oregon University**  
**Program: BA/BS/BAS of Cyber Security**

**Action:** At the **May 7, 2020** meeting, the Statewide Provosts Council approved a new program for **EOU, BA/BS/BAS of Cyber Security** to move forward to the Oregon Higher Education Coordinating Commission for its review and approval. The **EOU** Board of Trustees approved the **BA/BS/BAS of Cyber Security** program at its **June 4, 2020** meeting.

---

**Eastern Oregon University**

Sarah Witte, provost

Approved  
 Opposed  
 Abstained



**Oregon Health & Science University**

Elena Andresen, interim provost

Approved  
 Opposed  
 Abstained



**Oregon State University**

Ed Feser, provost

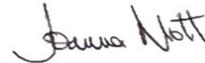
Approved  
 Opposed  
 Abstained



**Oregon Tech**

Joanna Mott, provost

Approved  
 Opposed  
 Abstained



**Portland State University**

Susan Jeffords, provost

Approved  
 Opposed  
 Abstained



**Southern Oregon University**

Susan Walsh, provost

Approved  
 Opposed  
 Abstained



**University of Oregon**

Patrick Phillips, provost

Approved  
 Opposed  
 Abstained



**Western Oregon University**

Rob Winningham, provost

Approved  
 Opposed  
 Abstained

