University of Oregon Bachelor's Degree in Cybersecurity (draft)

Jun Li, Joe Li, Reza Rejaie
Department of Computer and Information Science
College of Arts and Sciences
University of Oregon

July 15, 2022

1 General Information

This document proposes a bachelor's degree in cybersecurity. The major provides both comprehensive education and training that prepare graduates to succeed in their career, to address the cybersecurity workforce gap, and to adapt to future opportunities.

This program bridges computer science and applications in solving compelling cyber problems with real impact. This major will address the troubling shortfall of cybersecurity professionals in the job market and meets the strong demand for computer security specialists in the future. The cybersecurity field includes both protecting existing systems against threats and design of new systems that will be less vulnerable to threats. These skills are in high demand and will continue to be in demand as technology evolves. The U.S. Bureau of Labor Statistics projected that information security analyst jobs will grow 33% from 2020 to 2030, which is much faster than the 13% in general computer occupations, and the 8% for all occupations [1].

- Home Department: Computer and Information Science
- Level: Undergraduate
- Program Type: Bachelor's Degree; Bachelor of Science
- Primary Location: UO main campus
- Program Delivery Format: Traditional classroom/lab
- Does the program represent a collaboration of two or more university academic units? Yes.

2 Proposed Identification

- Full Title: University of Oregon Bachelor's Degree in Cybersecurity
- Desired effective term: Fall 2023

3 Relationship to Institutional Mission

This newly proposed program serves the mission of UO [2]:

- ***Serving the state, nation and world since 1876:*** *The University of Oregon is a comprehensive public research university committed to exceptional teaching, discovery, and service. We work at a human scale to generate big ideas. As a community of scholars, we help individuals question*

critically, think logically, reason effectively, communicate clearly, act creatively, and live ethically. Through its design and execution, the cybersecurity major program is to address the severe cybersecurity workforce shortfall in Oregon and the nation and meets the strong demand for top-quality computer security specialists in the future. This field will require both technical expertise to deal with the demands of technology, and vision to imagine the secure technology of the future.

- ***Purpose****: We strive for excellence in teaching, research, artistic expression, and the generation, dissemination, preservation, and application of knowledge. We are devoted to educating the whole person, and to fostering the next generation of transformational leaders and informed participants in the global community. Through these pursuits, we enhance the social, cultural, physical, and economic wellbeing of our students, Oregon, the nation, and the world.* This program aims to produce a new generation of transformational leaders and professionals in cybersecurity. The program will instill best knowledge in the field in students, promote their critical, logical, and effective thinking and communication, boost their abilities to solve problems in the cybersecurity space, thus preparing the best graduates to join the cybersecurity workforce.

- ***Vision****: We aspire to be a preeminent and innovative public research university encompassing the humanities and arts, the natural and social sciences, and the professions. We seek to enrich the human condition through collaboration, teaching, mentoring, scholarship, experiential learning, creative inquiry, scientific discovery, outreach, and public service.* The cybersecurity program seamlessly matches the vision of UO. It will involve many activities stated in the vision, including teaching, mentoring, scholarship, experiential learning, creative inquiry, and scientific discovery. It will enrich the human condition in that the graduates from this program will be working in the cybersecurity profession, which is now indispensable to the society and economy, and acting on a multitude of roles such as security architect, secure software developer, cyber defense incident responder, information security analyst, system security analyst, privacy officer, and so on.

- ***Values:*** *We value the passions, aspirations, individuality, and success of the students, faculty, and staff who work and learn here. We value academic freedom, creative expression, and intellectual discourse. We value our diversity and seek to foster equity and inclusion in a welcoming, safe, and respectful community. We value the unique geography, history and culture of Oregon that shapes our identity and spirit. We value our shared charge to steward resources sustainably and responsibly.* The cybersecurity program deeply endorses and promotes these values.

The design of the cybersecurity program also leverages signature strengths of UO. UO has a strong computer science program, and the cybersecurity program is deeply rooted in computer science. The program will produce cybersecurity professionals who receive the same solid training in computer science as other computer science majors at UO. This feature distinguishes our cybersecurity program from other cybersecurity programs in Oregon. UO's embrace of programs in arts, sciences, law, business, etc. provides opportunities for our students to become educated in allied topics related to cybersecurity, such as cyber law. UO's status as an R1 research university will provide opportunities to conduct field studies in cybersecurity, such as doing an internship at information services or conducting research at a lab in UO.

Finally, this cybersecurity program will also help UO's priorities and initiatives [3], especially UO's priority for achieving excellence at ensuring success for students and delivering a rich, excellent educational experience for them. Cybersecurity is an important major that many institutions in the nation have established. Cybersecurity Guide listed 187 cybersecurity bachelor's degree programs in the US for 2020 (it also lists 91 online bachelor's degree in cybersecurity) [4]. UO is uniquely positioned to offer this cybersecurity program to students across the state and beyond.

How will the proposal contribute to meeting UO 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?

This program will provide students with access to a new program that offers bachelor's degree in cybersecurity and enrich the diversity of educational programs offered by UO with a critical expertise for

the 21st century. Coming with the access to the program is also quality teaching and knowledge acquistion that both instructors and students will enjoy and benefit, research and innovation opportunities as new frontiers of this must-have discipline are continuously explored in classrooms and laboratories, and a community with a common goal to address the urgent, critical shortage of cybersecurity workforce in the state of Oregon.

How will the proposal meet regional or statewide needs and enhance the state' capacity to:

- *improve educational attainment in the region;*
- *respond effectively to social, economic and environmental challenges and opportunities; and*
- *address civic and cultural demands of citizenship?*

Students graduated from this program can address the severe statewide shortage of cybersecurity workforce. This program enhances Oregon's capacity in educating and producing capable workforce in the much needed cybersecurity area. Moreover, as many economy sectors, including information technology, transportation, health care, to just name a few, heavily rely on cybersecurity, this program will further strengthen the state's capacity in these sectors. Many social and environmental solutions, such as social media that operate online or power-hungry data centers that have a deep environment impact, are often based in the cyber space and can become more trustworthy if their security and privacy are well-protected. This program also covers legal and ethical issues in cybersecurity, an important civic and cultural aspect of citizenship.

4 Program Description

4.1 Design Philosophy

The cybersecurity program is designed to meet the growing demand for skilled cybersecurity professionals. It is deeply rooted in computer science and offers core and depth courses in cybersecurity. **The learning outcome at the program level is that students in this program should learn essential knowledge and up-to-date techniques in cybersecurity, including those in the main areas of fundamental security concepts and principles, applied cryptography, program security, and system and network security.** It follows NSA definitions and learning outcomes of knowledge units in cybersecurity and leverages NICE framework for defining cybersecurity tasks and associated knowledge and skills. It embraces a focus on hands-on skills and includes computer and network security practicum courses and field studies. Finally, it carefully considers student workload and enables flexible pathways for them to receive the degree while also making the program attractive to them.

The program follows a vertical architecture. The fundamental principles introduced in the lower division will be applied to increasingly complex problems at the upper-division. More specifically, the design supports knowledge units defined by NSA. Knowledge units introduced at an early stage will be helpful, many times necessary, to understand the knowledge units in cybersecurity courses at a later stage.

Students also need to conduct a field study by following the Workforce Framework for Cybersecurity (NICE Framework). While every student's field study may be about different tasks, students need to use the NICE framework to show they have the skills necessary for the tasks, usually after taking certain practicum courses so they can prove they are ready for the field study.

Are there tracks or concentrations within the credential? If so, do these start from a common core or are they differentiated from the beginning? No.

4.2 Courses Overview

To obtain a Cybersecurity degree, students must satisfy the specific major requirements as stated at the time when they are admitted to the major:

- Complete six stage-1 courses, including five CIS lower-division core courses and one Cybersecurity core course.
- Complete six staged-2 courses, including four CIS upper-division core courses at 300 level, and two core Cybersecurity courses.
- Complete eight stage-3 courses, including three CIS upper-division core courses at 400 level, one CIS upper-division elective course, two Cybersecurity core courses, and two Cybersecurity depth courses.
- Complete 16-credit breadth courses from stage-3 depth courses and CIS upper-division elective courses.
- Complete one writing course.
- Complete a field study (for one term).

4.3 Declaring the Cybersecurity Major

Students interested in the Cybersecurity major must meet with a CIS faculty advisor prior to declaring the major. Advising hours may be viewed on the CIS Faculty Advising page in the department's main office, 120 Deschutes Hall.

During the advising appointment, students will present an academic plan for completing the major, receive the feedback, and then incorporate the feedback to finalize the plan. Additional information is available for transfer students to the University of Oregon.

4.4 Satisfactory Progress in the Stage-1 Courses

Students must earn grades of B- or higher in stage-1 courses for automatic advancement to the stage-2 courses. Students with at most one C (any level) in the stage-1 courses and no other warning signs regarding preparedness for other cybersecurity courses (for example, repeated courses or other low grades) may submit a Prerequisite Override Request form to continue in the major. Students should be aware that requests are not automatically approved; approval depends on individual circumstances and will be conditional.

4.5 Satisfactory Progress in the Stage-2 Courses

Students must earn grades of C or higher in stage-2 courses if graded for automatic advancement to the stage-3 courses. Students who cannot advance to stage-3 courses automatically may submit a Prerequisite Override Request form to continue in the major. Students should be aware that requests are not automatically approved; approval depends on individual circumstances and will be conditional.

4.6 Satisfactory Progress in all Cybersecurity Program Courses

All coursework must be completed with a grade of C- or better if graded. Students who receive three grades below C- in all courses will be removed from the major. Below C- grades are cumulative. Retaking and passing a course does not change the total number of below C- grades. Students may schedule an appointment with an advisor to explore options including other majors, or submitting a petition to remain in the major.

4.7 General University Requirements

To earn a UO bachelor's degree, students must satisfy general university requirements as stated in the UO Catalog for the year they entered the major. Reference [5] lists requirements as of the 2021-22 Catalog. The College of Arts and Sciences awards Bachelor of Science (B.S.) degrees to students who major in Cybersecurity. If you fulfill the major requirements, you will automatically qualify for a B.S. degree.

4.8 Petitions

Exceptions or modifications to departmental requirements may be requested via a Petition form to the Undergraduate Education Committee. It is expected that students will have discussed the matter with an advisor before filing the petition.

4.9 Prerequisites

Are there specific course-to-course prerequisites that help students extend or link ideas or are the intellectual connections among courses in your major more general? Yes. See Section 5 for specific prerequisites for every course.

Admission to a given course requires completion of all the prerequisites listed in Section 5. Students with appropriate background who have consulted with an advisor may submit a Cybersecurity Prerequisite Override Request form to the Undergraduate Education Committee to register for a particular course. Prerequisite Override Requests should be submitted 10 days before the registration time for which the student needs that exception. Students should be aware that requests are not automatically approved; approval depends on individual circumstances and will be conditional.

4.10 Concurrent Degrees

Students can receive concurrent degrees with B.S. in Cybersecurity as one of the degrees. For example, a student can receive a B.S. degree in Computer Science and a B.S. degree in Cybersecurity so long as they meet the university concurrent degree requirements, which are described at [5].

5 Course of Study

The coursework as currently designed includes the following parts (plus courses for satisfying general university requirements):

(*: the course still needs to be approved)

- **Stage-1 courses (6 courses, 24 credits)**: Complete the following sequences. All courses must be taken **graded**.
  - CIS 102 Fundamentals of Computer and Information Security (1 course, 4 credits)
  - CIS lower-division core courses (5 courses, 20 credits)
    - CIS 210 (Prereq: MATH 112), 211 (Prereq: 210), 212 (Prereq: 211) Computer Science I-II-III
    - MATH 231 (Prereq: MATH 112 or satisfactory placement test score), 232 Elements of Discrete Mathematics I, II
- **Stage-2 courses (6 courses, 24 credits)**: Complete the following courses. All courses must be taken *graded* except for 332.
  - CIS upper-division core courses at 300 level (4 courses, 16 credits)
    - CIS 313 Intermediate Data Structures (Prereq: CIS 210, CIS 211, CIS 212, MATH 231, MATH 232 with grades of B- or better)
    - CIS 314 Computer Organization (Prereq: CIS 210, CIS 211, CIS 212, MATH 231 with grades of B- or better)
    - CIS 315 Intermediate Algorithms (Prereq: CIS 313)
    - CIS 330 C/C++ and Unix (Prereq: CIS 314)
  - CIS 332* System and Security Administration Lab (4 credits; Prereq: CIS 330)
  - CIS 333 Applied Cryptography (4 credits; Prereq: CIS 212. CIS 102 recommended)

- **Stage-3 courses (8 courses, 32 credits)**: Complete the following courses. All courses must be taken *graded* except for 437.
  - CIS upper-division core courses at 400 level (3 courses, 12 credits)
    - CIS 415 Operating Systems (Prereq: CIS 313, CIS 330)
    - CIS 422 Software Methodology I (Prereq: CIS 313)
    - CIS 425 Principles of Programming Languages (Prereq: CIS 315)
  - CIS 432 Introduction to Computer Networks (4 credits; Prereq: CIS 330. CIS 415 recommended)
  - CIS 433 Computer and Network Security (4 credits; Prereq: CIS 415. CIS 102 recommended)
  - CIS 437* Computer and Network Security Practicum (4 credits; Prereq: CIS 433)
  - Stage-3 depth courses (2 courses, 8 credits). Choose two from:
    - CIS 434 Computer and Network Security II (Prereq: CIS 433)
    - CIS 436 Secure Software Development (Prereq: CIS 330. CIS 102 recommended)
    - J431/CIS 400M. Computer Crime Law (CIS 102 recommended)
- **Breadth courses (16 credits)**: Choose courses from the stage-3 depth courses and CIS upper-division elective courses. A maximum of 8 credits may be taken *Pass/No Pass*.
  - Any additional stage-3 depth courses
  - Any 400-level CS courses and 399
  - A maximum number of 8 credits from courses 399, 400M, and 410 may be counted toward the degree
  - A maximum number of 8 credits from 403 may be counted toward the degree
  - A maximum number of 4 credits from courses 405 and 407 may be counted toward the degree
  - CIS 405, 407, 399, 410 repeatable only with different subtitles
- **Writing requirement (1 course, 4 credits)**: Choose one from the following. The course may be taken *Pass/No Pass* or *Graded*.
  - WR 320 Scientific and Technical Writing
  - WR 321 Business Communications
- **Field study (4 credits)**: Conduct a field study by following the NICE Framework. Students can choose one experience study over one or multiple terms with totally four (4) credits from the following. The course may be taken *Pass/No Pass* or *Graded*.
  - CIS 401 Research
  - CIS 404 Internship
  - CIS 406 Field study

Total credits: 104.

6 Expected Learning Outcomes for Students and Means of Assessment

This program defines its principle learning outcome (concept or skill) by referring to cyber defense knowledge units (KUs) defined by NSA, or more specifically, its National Centers of Academic Excellence in Cybersecurity (NCAE-C). According to NSA, to achieve academic excellence, a bachelor's degree in cybersecurity should cover 3 foundational KUs, 5 core KUs, and at least 14 optional KUs [6]. As shown

in [7], NSA defined totally 3 foundational KUs, 5 *technical* core KUs, 5 *non-technical* core KUs, and 56 optional KUs in cyber defense. The definition of every KU includes a brief summary of the intent of the KU, its learning outcome, topics to be completed, and vocabulary. Not every KU is of similar size or intensity; some may be covered in as few as two lectures, and some may need to be introduced in one course and reinforced in a later course.

Based on our educational strength at UO, as of now our program is designed to cover all 3 foundational KUs, 5 technical core KUs, and 20 optional KUs (which includes 3 non-technical core KUs that can be treated as optional KUs) for *all* students in the program. Our program is poised to excel in offering a sufficient amount of KUs to our students. We will be particularly strong in software, system, and network security.

Table 1 shows in which course(s) of our program a KU is introduced and, sometimes, reinforced. Most courses are aligned to one to three KUs. The only exception is CIS 102, which introduces five KUs, and CIS 433 which reinforce the same five KUs and also introduces another seven. This table does not include elective or optional courses (e.g., the stage-3 depth and breadth courses), as all students should experience all courses indicated in the KU alignment.

An important note here is that a KU is not always perfectly covered by our courses in terms of its learning outcome and topics. For historical or pedagogical reasons, we may choose not to cover all the topics in a KU, or cover more topics beyond those defined in the KU. That said, we will strive to align our teaching to the KU outcome and topics specified by NSA as close as possible.

Table 1

UO Bachelor's Degree in Cybersecurity																			
NSA-Defined Cyber Defense Knowledge Units (KU)		Courses that all Cybersecurity students must take (I: introduced. R: reinforced)																	
		Stage-1						Stage-2						Stage-3					
		CIS 102	CIS 210	CIS 211	CIS 212	Math231	Math232	CIS 313	CIS 314	CIS 315	CIS 330	CIS 332*	CIS 333	CIS 415	CIS 422	CIS 425	CIS 432	CIS 433	CIS 437*
Foundational KU	Cybersecurity foundations (CSF)	I																R	
	Cybersecurity Principles (CSP)	I																R	
	IT Systems Components (ISC)	I							R									R	
Technical Core KU	Basic Cryptography (BCY)												I						
	Basic Networking (BNW)																I		
	Basic Scripting & Programming (BSP)										I								
	Network Defense (NDF)																	I	
	Operating Systems Concepts (OSC)													I					
Non-Technical Core KU	Cyber Threats (CTH)	I																R	
	Cybersecurity Plan & Mngmnt (CPM)																	I	
	Policy,Legal,Ethics & Compliance (PLE)																	I	
	Security Program Management (SPM)																		
	Security Risk Analysis (SRA)																		
Optional KU	Adv. Cryptography (ACR)												I						
	Algorithms (ALG)		I	R	R					R									
	Basic Cyber Operations (BCO)											I							R
	Cloud Computing (CCO)																	I	
	Cyber Crime (CCR)	I																R	
	Cybersecurity Ethics (CSE)																	I	
	Data Structures (DST)		I	R	R			R											
	Low Level Programming (LLP)				I				I										
	Netwk Forensics (NWF)																		I
	Netwk Security Administration (NSA)																		I
	Netwk Tech. and Protocols (NTP)																		I
	Operating System Admin. (OSA)											I							
	Operating Systems Hardening (OSH)											I							
	Operating Systems Theory (OST)													I					
	Privacy (PRI)																	I	
	Secure Programming Practices (SPP)																	I	

We will continuously and iteratively assess the learning outcome of students to improve this program. We will use quizzes, homework, and exercises throughout every teaching term to assess students' mastery of knowledge units, as well as their performance in exams. Student projects, whether in a regular class or a lab-oriented class, often are also very indicative on the efficacy of our teaching. Many times interactions with students in and out of the classroom can also greatly help assess how well students have learned every knowledge unit. We will use all above information as input to improve curriculum and instruction.

7 Need for this Credential

What is the estimated number of degrees awarded per year once the degree is well established? Provide evidence of potential demand.

The Oregon population is approximately 1.3% of the US populations. Right now, there are about 377,000 unfilled cybersecurity jobs in the US [8]. So, there is clearly very high demand even if we scale by Oregon's population. We estimate that this major might be about one quarter to one half the size of the current CS major, and that it will bring students to the UO looking specifically for this kind of training. Thus, we imagine 25 new students in the first year and then about 10% increase per year before it stabilizes.

Does this new degree have the potential to attract new students to the UO as opposed to students who might switch from other UO programs? Please explain.

We expect it will attract "new" students. There are two factors. One is the increasing demand for expertise in this field (that is, a growing job market that has already grown beyond the nation's training capacity). The other is the high public profile of cybersecurity so that interested high school students can be expected to know about the high demand for expertise in this field.

What are the potential post-graduation opportunities for graduates in terms of careers or graduate school?

The U.S. Bureau of Labor Statistics estimated that through 2029, the annual job growth rate in information security roles is 31%. This is much faster than the 11% in general computer occupations, and the 4% for the national average. The top cybersecurity jobs are Chief Information Security Officer, Information Security Analyst, IT Security Administrator, Penetration Tester, and Security Engineer. The U.S. Bureau of Labor Statistics further reported that the mean annual pay in 2021 is $102,600 for information security analysts whose typical entry-level education is a bachelor's degree [9].

Graduates from this program will also have a promising chance to enter graduate school. In fact, many universities nowadays also have a Master program in cybersecurity. As graduates from this program receive the same computer science training as CIS majors, they can also apply to master's degree program in computer science. For those who would like to pursue a Ph.D. degree in cyber security, or computer science, they should also be able to find many good matches in R1 or R2 universities.

We expect that the majority of students that this program attacts are full-time, traditional, resident students, while some students may be part-time or out of state. The program will be particularly appealing to students who would like to pursue a career in cybersecurity, regardless of their backgrounds.

8 Program Integration And Collaboration

Are there similar or related programs currently offered at the University of Oregon? If so, how is this program different enough to warrant its addition? What opportunities exist for collaboration with other UO programs?

UO also has a security track embedded in its Computer and Information Science BS degree program [10, 11], but students of the track only need to take three courses related to cybersecurity, far less than what a B.S. graduate ideally would need in order to become a highly desired cybersecurity professional, and the track is not transcriptable. What we propose here is a new undergraduate major program in the CIS department that awards bachelor's degree in cybersecurity.

Are there similar or related programs currently offered in the State? What is the potential for competition and/or collaboration with those programs?

Cybersecurity Guide listed 187 cybersecurity bachelor's degree programs in the US for 2020 (it also lists 91 online bachelor's degree in cybersecurity) [4]. Our proposal to establish a cybersecurity bachelor's degree program is a critical step to catch up with a national trend that the state is trailing. In Oregon there are cybersecurity certificate programs from Oregon State University (OSU) [12], Portland State University (PSU) [13], and Southern Oregon University (SOU) [14], BS in Computer Science programs with cybersecurity concentration from George Fox University [15] and Western Oregon University (WOU) [16], and multiple cybersecurity training or associate degree programs at community colleges (e.g., MHCC [17], PCC [18], LCC [19]). Several 4-year colleges also have majors related to cybersecurity: OIT has had a cybersecurity BS program since Fall 2019 [20], but as it is focused on "business-savvy cybersecurity professionals", it integrates many business courses and lacks computer science at its core [21]. Western Oregon University has a cybercrime investigation and enforcement B.S. but not focused on cybersecurity science and technologies [22]. Eastern Oregon University has a cybersecurity major but cannot offer the base depth in computer science that UO can [23].

Some of these programs (such as those at community colleges) can feed our cybersecurity degree program. OIT's cybersecurity program is complementary to our proposal and WOU's cybercrime investigation and enforcement B.S. program is focused on legal aspects of cybersecurity. Some will overlap with what we propose, such as EOU's cybersecurity major program, but the need to train students in this area is very high and increasing. We expect to be able to collaborate with all these cybersecurity programs in different ways. All the evidence indicates that a significantly higher capacity in cybersecurity education and training is especially needed in Oregon.

Describe the potential for impact on other institution's programs.

The impact on other programs in terms of student enrollment should be minimal. The demand for cybersecurity education significantly surpasses the current limited availability of the options across the state. Also, available programs in cybersecurity education in Oregon have diverse foci and thus address demand for cybersecurity education at different levels as described above.

9 Resources

One immediate need is to hire an NTTF/instructor to teach some of the new courses (CIS 332, CIS 437). Many of the courses have a strong lab component and may need a GE as well as some basic lab equipment for hands-on exercises. Advisors will need to be trained to guide student through the program.

In the near future, we definitely need to hire another TTF in some area of cybersecurity to support our growing educational and training activities in this critical area.

Advising for students in this new program can be done by Tykeson Hall advisors. As the program grows, we will further consider having an NTTF faculty member to serve as an academic advisor for students in this program.

10 Plan

We will continue to improve syllabi of courses in this program, including having them become more aligned with NSA-CAE cyber defense knowledge units and cover all the topics of every knowledge unit we chosen to cover.

Acknowledgment

We thank Prof. Joe Sventek who helped establish a number of security courses and have them taught before approved as a regular course. We appreciate Kathleen Freeman for many valuable discussions and feedback on the design of the program. And certainly we thank many of our colleagues who teach a plethora of quality courses that form the main body of the curriculum in this program.

References

[1] U.S. Bureau of Labor Statistics. Occupational Outlook Handbook – Information Security Analysts Job Outlook. https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-6.

[2] University of Oregon. Mission Statement. https://www.uoregon.edu/our-mission.

[3] University of Oregon, Office of the President. Priorities and Initiatives. https://president.uoregon.edu/priorities-and-initiatives.

[4] Cybersecurity Guide. Find your cybersecurity degree or certification. https://cybersecurityguide.org.

[5] University of Oregon. 2021-22 Catalog Bachelor's Degree Requirements. https://catalog.uoregon.edu/admissiontograduation/bachelorrequirements.

[6] NSA National Centers of Academic Excellence in Cybersecurity (NCAE-C). CAE 2022 Designation Requirements and Application Process For CAE-Cyber Defense (CAE-CD). https://dl.dod.cyber.mil/wp-content/uploads/cae/pdf/unclass_cae-cyber-defense-program-guidance.pdf. January 2022.

[7] NSA National Centers of Academic Excellence in Cybersecurity (NCAE-C). 2020 CAE Cyber Defense (CAE-CD) Knowledge Units. https://dl.dod.cyber.mil/wp-content/uploads/cae/pdf/unclass-cae-cd_ku.pdf.

[8] (ISC)2 Cybersecurity Workforce Study. A Resilient Cybersecurity Profession Charts the Path Forward. https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx, 2021.

[9] U.S. Bureau of Labor Statistics. Occupational Outlook Handbook – Information Security Analysts Pay. https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-5.

[10] University of Oregon. 2021-22 Catalog, Computer and Information Science Undergraduate Studies. https://catalog.uoregon.edu/arts_sciences/computerandinfoscience/#undergraduatetext.

[11] University of Oregon, Computer and Information Science. Computer Security. https://cs.uoregon.edu/undergraduate/cis-major/computer-security.

[12] Oregon State University. Cybersecurity Undergraduate Certificate. https://ecampus.oregonstate.edu/online-degrees/undergraduate/certificates/cybersecurity. Degrees online.

[13] Portland State University. Cybersecurity Graduate Certificate. https://www.pdx.edu/computer-science/cybersecurity. Maseeh College of Engineering and Computer Science, Computer Science.

[14] Southern Oregon University. Certificate in Cybersecurity. https://catalog.sou.edu/preview_program.php?catoid=14&poid=3880. 2021-22 University Catalog (for both graduate and undergraduate students).

[15] George Fox University. Cyber Security Concentration. https://www.georgefox.edu/college-admissions/academics/major/cyber-security-concentration.html.

[16] Western Oregon University. Cybersecurity Concentration. https://catalog.wou.edu/preview_program.php?catoid=6&poid=2118&hl=cybersecurity&returnto=search. 2021-22 University Catalog.

[17] Mountain Hood Community College. Information Systems and Technology Management - Cyber Security and Networking. https://www.mhcc.edu/Cybersecurity.

[18] Portland Tribune. PCC receives $189,000 for cybersecurity training. https://www.koin.com/local/multnomah-county/pcc-receives-189000-for-cybersecurity-training. March 1, 2022.

[19] Lane Community College. Cybersecurity Program. https://www.lanecc.edu/programs-academics/academic-programs/computer-science-and-information-technology/cybersecurity.

[20] Oregon Institute of Technology. Cybersecurity, BS. https://catalog.oit.edu/preview_program.php?catoid=10&poid=2323&print. 2021-22 University Catalog.

[21] Oregon Institute of Technology. Oregon Tech Announces New Cybersecurity Degree Starting Fall 2019. https://www.oit.edu/news/oregon-tech-announces-new-cybersecurity-degree-starting-fall-2019. May 21, 2019.

[22] Western Oregon University, Criminal Justice Sciences Division. Cybercrime Investigation and Enforcement Bachelor of Science. https://wou.edu/criminal-justice/undergraduate-degrees/bs-cybercrime-investigation-enforcement.

[23] Eastern Oregon University. Cyber Security Major. https://www.eou.edu/academics/cyber-security-major.