BS in CYBERSECURITY

General Information

Give a brief (1-2 paragraphs) overview of the proposed credential, including its disciplinary foundations and connections, its focus and learning objectives for students, and the specific degree (e.g. bachelors, masters, doctorate) and/or credentials (e.g. major, certificate, minor, concentrations) to be offered. This should be based largely on your descriptions in the following sections but it should be shorter than their combined length. Moreover, it should use language that is capable of communicating your ideas to audiences increasingly distant from your academic field as your proposal moves through the review process.

We propose 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].

It might be possible to offer this as a "track" in the Computer Science major, but that would have two unfortunately effects: it would reduce the cybersecurity focus of the major, and it would also reduce the visibility of the program for prospective students because majors are much more visible than tracks within other majors.

[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.

Primary Proposer

Jun Li

Is there a co-proposer for this proposal?

Yes

Co-proposer(s)

Name	Home Unit
Yingjiu (Joe) Li	Computer and Information Science
Reza Rejaie	Computer and Information Science

Home department

Computer & Information Science

College

Arts & Sciences, College of

Level

Undergraduate

Program Type

Bachelor's Degree

By default, the program will be approved for the Bachelor of Arts and Bachelor of Science. If you are only requesting one of these, please indicate below:

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

Proposed Identification

Full Title

Cybersecurity

Transcript Title

Cybersecurity

What's your desired effective term?

Fall 2023

Fall term is the default term unless an alternative is specifically requested and approved.

Relationship to Institutional Mission and Statewide Goals

How is the program connected with the UO's mission, signature strengths and strategic priorities?

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

This program will connect UO's growing faculty and research strengths in cybersecurity to the growing demand for professional training in this field and in particular the cybersecurity workforce shortfall in Oregon and the nation.

This program aims to produce 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.

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]. As a program with direct ties to workforce demand, this can address UO's priority for student success, and we can deliver a rich, excellent education including experiential learning opportunities, and this major will expand the reach and breadth of the university's nascent School of Computer and Data Science.

Cybersecurity is a 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.

[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.

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.

There is no other bachelors level cybersecurity major in Oregon, and the existing non-bachelors programs don't offer the deep connection to computer science embedded in this major.

A major such as this that addresses specific (and enormous) workforce needs will appeal to students who come to college from economic situation that make connecting to a career at an early stage a "must." Thus this program simultaneously addresses meaningful access to higher education for certain groups of students, and the economic support 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?

As mentioned above, this will be the first bachelors-level cybersecurity program grounded in computer science in Oregon, and one of the first in the Pacific Northwest.

This program can address the severe statewide cybersecurity workforce shortage. 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.

Students will also address legal and ethical issues in cybersecurity, which are becoming ever more important as so much data and activity is mediated by computers and the internet.

Program Description

Is there a core set of required courses?

Yes

What is the core set of required courses and what is the rationale for giving these courses this prominent role? What are the central concepts and/or skills you expect students to take from the core?

The core (Stages 1 and 2) is directed at
- understanding computer systems and networks well enough to come to grips with the issues central to cybersecurity (vulnerabilities, protections, privacy, etc.)
- understanding basic techniques addressing cybersecurity.

Cybersecurity is a discipline growing out of computer science which is focused on protecting computer networks from disruption, securing computer systems against intrusions or disruption, and making sure data can be stored, accessed and transmitted by the data owners without exposing it to other parties.

It is an intrinsic part of using computer systems for financial, medical, and other business and industrial purposes, as well as personal use. It underlies efforts to ensure that computer systems and networks can't be pirated, hijacked or ransomed, and to safeguard private data.

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.

The degree program is structured around groups of courses (stage 1, stage 2, and stage 3). Students

• complete all six stage-1 courses, including five CIS lower-division core courses and one Cybersecurity core course,
• complete all six stage-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).

In addition, 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 cybersecurity program is designed to meet the growing demand for skilled cybersecurity professionals as articulated by the NSA [6, 7]. It is deeply rooted in computer science and offers core and depth courses in cybersecurity. It follows NSA definitions and learning outcomes of knowledge units in cybersecurity and uses the National Initiative for Cybersecurity Career and Studies NICE framework for defining cybersecurity tasks and associated knowledge and skills [6,7]. 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.

[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.

What is the relationship between upper-division courses and the lower-division curriculum? For example, are fundamental principles introduced in the lower division and then applied to increasingly complex problems at the upper-division? This vertical architecture is common in the sciences, but is by no means universal. In the humanities, a more horizontal structure is often appropriate. For example, students might read and analyze literature at each level (100-400), but do so with increasing sophistication and the capacity to draw on a widening array of literary forms and ideas.

The program is highly sequential like many science majors. 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.

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, there are specific course-to-course prerequisites. Please see the attached document entitled "University of Oregon Bachelor's Degree in Cybersecurity" Section 3.

Admission to a given course requires completion of all the prerequisites. 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.

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.

Course of Study

Programs are required to display their curriculum in grid format to meet degree guide specifications. Proposed curriculum should include course numbers, titles, and credit hours.

Course of Study

Code	Title	Credits
Stage 1	**All courses must be taken graded.**	**24**
CS 102	Fundamentals of Computer and Information Security	4
CS lower-division core courses		20
CS 210	Computer Science I	
CS 211	Computer Science II	
CS 212	Computer Science III	
MATH 231	Elements of Discrete Mathematics I	
MATH 232	Elements of Discrete Mathematics II	
Stage 2	**All courses must be taken graded except for 332.**	**24**
CS upper-division core courses at 300 level		16
CS 313	Intermediate Data Structures	
CS 314	Computer Organization	
CS 315	Intermediate Algorithms	
CS 330	C/C++ and Unix	
CS 332	Course CS 332 Not Found (System and Security Administration Lab) to be submitted for approval soon	4
CS 333	Applied Cryptography	4
Stage 3	**All courses must be taken graded except for 437.**	**32**
CS upper-division core courses at 400 level		12
CS 415	Operating Systems	
CS 422	Software Methodology I	
CS 425	Principles of Programming Languages	
CS 432	Introduction to Networks	4
CS 433	Computer and Network Security	4
CS 437	Course CS 437 Not Found (Computer and Network Security Practicum) to be submitted for approval soon	4
Stage-3 depth courses		8
CS 434	Computer and Network Security II	
CS 436	Secure Software Development	
J 431	Media Structures and Regulation: [Topic] (Computer Crime Law)	
Breadth Courses	**A maximum of 8 credits may be taken Pass/No Pass.**	**16**
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: one of the two	**The course may be taken Pass/No Pass or Graded.**	**4**
WR 320	Scientific and Technical Writing	
WR 321	Business Communications	
Field Study	**Over one or multiple terms with totally four (4) credits. The course may be taken Pass/No Pass or Graded.**	**4**
CS 401	Research: [Topic]	
CS 404	Internship; [Topic]	
CS 406	Practicum: [Topic]	

Expected Learning Outcomes for Students and Means of Assessment

Only one learning outcome should be listed per row. Additional fields are added once a row has been filled.

Principle Learning Outcome (Concept or Skill)	Part of curriculum where this learning outcome introduced	Part of curriculum where this learning outcome developed	How student learning for this outcome will be assessed
Cybersecurity foundations (CSF)	CS 102	CS 433	Homework, discussions, exam
Cybersecurity Principles (CSP)	CS 102	CS 433, CS 436	Homework, discussions, exam
IT Systems Components (ISC)	CS 102	CS 314, CS 433	Homework, discussions, exam
Basic Cryptography (BCY)	CS 333	-	Homework, discussions, exam
Basic Networking (BNW)	CS 432	-	Homework, exercises, discussions, exam
Basic Scripting & Programming (BSP)	CS 330	CS 436	Homework, exercises, discussions, exam
Network Defense (NDF)	CS 433	CS 434	Homework, discussions, exam
Operating Systems Concepts (OSC)	CS 415	CS 436	Homework, exercises, discussions, exam
Cyber Threats (CTH)	CS 102	CS 433	Homework, discussions, exam
Cybersecurity Plan & Management (CPM)	CS 433	-	Homework, discussions, exam
Policy, Legal, Ethics & Compliance (PLE)	CS 433	-	Homework, discussions, exam
Adv. Cryptography (ACR)	CS 333	-	Homework, discussions, exam
Algorithms (ALG)	CS 210	CS 211, 212, 315	Homework, exercises, discussions, exam
Basic Cyber Operations (BCO)	CS 332	CS 437	Exercises, discussions
Cloud Computing (CCO)	CS 433	CS 434	Homework, discussions, exam
Cyber Crime (CCR)	CS 102	CS 433	Homework, discussions, exam
Cybersecurity Ethics (CSE)	CS 433	-	Homework, discussions, exam
Data Structures (DST)	CS 210	CS 211, 212, 313	Homework, exercises, discussions, exam
Low Level Programming (LLP)	CS 212	CS 314, CS 436	Homework, exercises, discussions, exam
Netwk Forensics (NWF)	CS 437	-	Exercises, discussions
Netwk Security Administration (NSA)	CS 437	-	Exercises, discussions
Netwk Tech. and Protocols (NTP)	CS 437	-	Exercises, discussions
Operating System Admin. (OSA)	CS 332	-	Exercises, discussions
Operating Systems Hardening (OSH)	CS 332	-	Exercises, discussions
Operating Systems Theory (OST)	CS 415	-	Homework, discussions, exam
Privacy (PRI)	CS 433	-	Homework, discussions, exam
Secure Programming Practices (SPP)	CS 433	CS 436	Homework, discussions, exam

-	-	-	Note: Discussions can help an instructor assess the learning of students on the fly during the discussion. We didn't include quizzes, but each individual instructor may decide whether and how to use quizzes for learning assessments. Different from homework, exercises in our context mainly refer to program assignments and hands-on activities.

Expected Learning Outcomes (Will Appear in Catalog)

Students in this program will learn essentials of secure computing and applications; network structure, vulnerabilities and protections; cryptographic principles and techniques; policy, methods and ethics of data security and privacy. These outcomes follows National Security Agency definitions and learning outcomes in cybersecurity and embrace a focus on hands-on skills.

Accreditation

Is or will the program be accredited?

No

Please explain why accreditation is not being sought:

We don't have any plan for accreditation in the near future but will explore it after the program is fully established. In the short term we choose to focus on the execution and continuous improvement of the program based on the feedback from students, faculty, and the industry. We will look into the accreditation in the long run as the program matures.

Need for this Credential

What is the anticipated fall term headcount over each of the next five years?

Fall Term Headcount = number of students enrolled in the program as of Fall term.

Year 1	Year 2	Year 3	Year 4	Year 5
25	52	82	115	120

What are the expected degrees/certificates over the next five years.

Number of Degrees:

Year 1	Year 2	Year 3	Year 4	Year 5
0	5	5	20	22

How did you arrive at the above estimates? Please provide evidence. (e.g. surveys, focus groups, documented requests, occupational/ employment statistics and forecasts, etc.)

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.

We expect to see students who enrolled in this program as freshmen to graduate within 4-5 years, starting Year 4. We expect a small number of current CS students may elect to pursue the BS Cybersecurity degree, concurrent with their current BS Computer Science degree. So we estimate a small number of graduates in Year 2 and Year 3 of these students.

[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.

What are the characteristics of students you expect this program to attract (e.g., resident/out-of-state/international; traditional/ nontraditional; full-time/part-time)? Will it appeal to students from particular backgrounds or with specific careers in mind?

We expect that the majority of students that this program attacts are full-time, traditional, resident/non-resident/international students, mirroring the demography of students in the CIS program. Some students may be part-time. The program will be particularly appealing to students who would like to pursue a career in cybersecurity, regardless of their backgrounds.

What are possible career paths for students who earn this credential? Describe and provide evidence (e.g. surveys, focus groups, documented requests, occupational/employment statistics and forecasts, etc.) for the prospects for success of graduates in terms of employment, graduate work, licensure, or other professional attainments, as appropriate.

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.

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

Describe the steps that have been taken to ensure that the proposed program(s) does not overlap other existing UO program(s) or compete for the same population of students. [Provide documentation that relevant departments or areas have been informed of the proposal and have voiced no objections.]

The pre-proposal was brought to the Deans Council on May 10th for consideration. No objections were brought forward.

There is overlap with the Computer Science major. This major currently has a security track, but students of the track only need to take three courses related to cybersecurity, which is much less content on cybersecurity than is in this proposal.

List any existing program(s) that are complemented or enhanced by the new major.

Program(s)
BS/BA in Computer Science

Program Integration And Collaboration

Are there closely-related programs in other Oregon public or private universities?

Yes

List similar prorgrams and indicate how the proposal complements them. Identify the potential for new collaboration.

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 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.

[12] Oregon State University. Cybersecurity Undergraduate Certificate. https://ecampus. oregonstate.edu/online-degrees/undergraduate/certificates/cybersecurity. Degrees on- line.
[13] Portland State University. Cybersecurity Graduate Certificate. https://www.pdx.edu/ computer-science/cybersecurity. Maseeh College of Engineering and Computer Science, Com- puter 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 under- graduate 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 Cy- bersecurity 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 En- forcement 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.

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.

Resources Required to Offer the Program or Move to New Location

List any faculty who will have a role in this this program, indicating those who have leadership and/or coordinating roles. For each individual, indicate status with respect to tenure track (TT or NTT), rank, and full-time or part-time.

Faculty Name	Faculty Classification and Rank	FTE	Role
Reza Rejaie	TT – Full	1.0	Director
Yingjiu (Joe) Li	TT – Full	1.0	Faculty
Jun Li	TT – Full	1.0	Faculty
Bryce Newell	TT – Assistant	1.0	Faculty

Please describe the adequacy and quality of the faculty delivering the program, including how the mix of tenure-track, career and pro tem faculty are strategically used to ensure effective delivery of the curriculum.

All the CS courses listed in the program have already been taught by current faculty, including the following security courses:
* CS 102, 333, 436 by Yingjiu (Joe) Li, who is a Ripple Professor who has been teaching and researching cybersecurity for about 22 years since his PhD study.
* CS 432, 433, 434 by Jun Li, who is the Founding Director of Center for Cyber Security and Privacy at UO, has 26 years of experience in studying, developing, and publishing at top venues solutions related to cybersecurity.
* J 431 by Bryce Newell, who is an assistant professor from School of Journalism and Communication, who studies law enforcement adoption and use of technology, privacy law, information ethics, and the social implications of information and communication technologies.

In addition, we are developing CS 332 and 437. Teaching these courses regularly will require one new faculty member. The department needs new faculty in any case as retirements and the COVID hiring freeze have decreased faculty size considerably while student demand remains strong.

What is the nature and level of research and/or scholarly work expected of program faculty that will be indicators of success in those areas?

This program is an educational program and its success is not directly connected to the research work of program faculty. However cybersecurity is already an area of relative strength in the department, so an investment in more faculty in that area will build on this strength. Faculty research projects in cybersecurity alsi offer a opportunities for students in this program to become involved in those research projects to fulfill the field study requirement of this program.

Describe how students will be advised in the new program.

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.

Describe the staff support for the proposed program, including existing staff and any additional staff support that will be needed.

Many existing courses are large or have a strong lab component and thus require a GE. To the extent that this grows existing courses (at a steady state of 120 students in this major, that is a 20% increase in students taking the core computer science and mathematics courses) additional GEs may be needed.

It is impossible to predict this accurately since some students may be in courses that will not push over the edge of GE requirements, but we estimate up to two new GEs will be required once this is at steady state (6 GE terms).

Are special facilities, equipment, or other resources required as a result of this proposal (e.g., unusual library resources, digital media support,

Some courses will need some basic lab equipment for hands-on exercises such as a couple of servers for creating sand-boxes for students to do hands on experiments for lab courses. The CS department will provide this equipment, as it already does for computer science majors. No unusual or special library resources are needed, at least as of this point.

Other Program Characteristics

Must courses be taken for a letter grade and/or passed with a minimum grade to count toward the proposed program? If so, please list the courses and the requirements of each. Note: Although there is variation in detail, UO undergraduate majors typically require that most of the courses be taken for a letter grade (not "pass/no pass") and that the grade be C- or better.

Please see the footnotes attached to the courses of study above.
Master's programs require at least 24 credits to be taken for a letter grade, but individual programs may require a higher number. There are no specific graded credit policies for doctoral and certificate programs; each program should determine what is appropriate within their discipline.

How much course overlap will be allowed to count toward both this programs and some other credential a student might be earning (a minor, certificate, or another program)? If there are specific credentials with overlap limits, please list those and the limits. For Accelerated Master's Program proposals, include in this section the proposed credit allocation structure for graduate credits taken as an undergraduate, i.e., how many graduate credits may count only toward the master's degree and how many may be used to clear requirements for both the bachelor's and the master's.

Students will be allowed to overlap any applicable material Cybersecurity Major and the Computer Science major.
[5] University of Oregon. 2021-22 Catalog Bachelor's Degree Requirements. https://catalog.uoregon.edu/admissiontograduation/bachelorrequirements.

Does your proposal call for new courses, or conversion of experimental courses into permanent courses? If so, please list courses in the text box below and indicate when they will be submitted to UOCC for approval:

Two new courses to be approved for this program:
CS 332 System and Security Administration Lab
CS 437 Computer and Network Security Practicum

We expect to submit 332 for approval within a week and 437 for approval early July.

Will admission to the program be limited?

No

Will students be required to apply for entry to this program?

Yes

What are the conditions for admission?

High school students who plan to major in cybersecurity should have completed a strong academic program, including substantial work in mathematics, sciences, and writing. Courses in algebra, geometry, and more advanced topics should be included. Courses or prior experience in computer programming or security would be appreciated but not required. (Upon arrival at the university, students should consult with an advisor to determine the entry-level course best suited to the student's background.)

Please describe admission procedures (Will Appear in Catalog)

Students may be admitted to the major after consultation with an adviser in the Department of Computer Science or with an advisor in Tykeson Hall. Students should seek admission to this major early in their career at the university as the requirements have a number of course dependencies.

Residency Requirements (Will Appear in Catalog)

24 credits from the Computer Science department must be earned in residence at the University of Oregon.