MS 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.

The proposed Master's degree in Cybersecurity at the University of Oregon aims to equip students with comprehensive knowledge and skills in safeguarding digital information and infrastructures. Students will engage in rigorous coursework and hands-on projects that address current cybersecurity challenges, such as network security, cryptography, and risk management.

The program's focus is to develop professionals who can anticipate, identify, and mitigate cyber threats in diverse organizational contexts. Learning objectives include mastering advanced cybersecurity techniques, understanding legal and regulatory frameworks, and developing strategic problem-solving skills. Graduates will earn a Master of Science (MS) degree in Cybersecurity, preparing them for leadership roles in both the private and public sectors, where their expertise will be crucial in protecting critical digital assets.

There were more than 4.8 million cybersecurity jobs unfilled globally and more than half a million cybersecurity jobs unfilled nationwide in the US in 2023. Existing training programs and degrees for Cybersecurity workforce development do not have the capacity to address this growing need.
The University of Oregon (UO) is a founding member of the Oregon Cybersecurity Center of Excellence (OCCoE). Workforce development is one of the key goals of this state-funded center.

Over the past few years, the CS department at UO initiated several activities to lay the foundation for creating several cybersecurity programs. The bachelor’s degree in cybersecurity was established in Fall 2023 and the department is actively promoting and expanding this program. We have developed a few cutting-edge experiential learning elements at UO in support of these Cybersecurity programs.

Primary Proposer
Reza Rejaie

Email

reza@uoregon.edu

Is there a co-proposer for this proposal?
Yes

Co-proposer(s)

Name	Home Unit
Dan Carrere	Computer Science

Home department for this program
Computer Science

College
Arts & Sciences, College of

Level
Graduate

Program Type
Master's degree

By default, the program will be approved for the Master of Arts and Master of Science. If you are only requesting one of these, please select the appropriate Degree Type below.

Degree Type
Master of Science ONLY

Primary Location
UO main campus

Program Delivery Format
Traditional classroom/lab

Does the program represent a collaboration of two or more university academic units?
No

Proposed Identification

Full Title
Cybersecurity

Transcript Title
Cybersecurity

CIP Code
110101

What's your desired effective term?
Fall 2026

Relationship to Institutional Mission and Statewide Goals

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

The proposed Master's degree in Cybersecurity aligns closely with the University of Oregon's mission by fostering critical thinking, innovation, and a commitment to public service. This program leverages the university's signature strengths in interdisciplinary education and research excellence, integrating computer science with fields such as network security, system security, data security and privacy, and security operations to address complex cybersecurity challenges. By focusing on emerging technologies and ethical practices, the program supports UO's strategic priorities of enhancing academic and research excellence, promoting inclusivity, and preparing students to be leaders in a rapidly evolving digital landscape. Through this initiative, UO aims to contribute significantly to the protection of global digital infrastructure, while nurturing a diverse cohort of cybersecurity experts poised to make meaningful impacts in their communities and beyond.

All the Cybersecurity programs in our department meet the four goals of the Oregon Rising. In particular, the certificate and master's programs 1) enable students to graduate in a timely manner
2) graduates of these program are career ready and are able to find a position within a few months from graduation 3) Cybersecurity professionals profoundly and positively impact companies and communities around them, 4) these programs support various research and advance development projects in the area of Cybersecurity at UO.

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?

The proposed Master's degree in Cybersecurity will significantly contribute to the University of Oregon's and statewide goals by enhancing student access and diversity through targeted recruitment and inclusive support systems. This program aims to attract a diverse student body, fostering a rich learning environment that reflects the varied perspectives essential for tackling cybersecurity challenges. By offering high-quality education, the program will empower students with cutting-edge knowledge and skills, thereby promoting excellence in learning and research. It will support innovation and knowledge creation by encouraging collaborative research projects and partnerships with industry leaders. Additionally, the program will contribute to the economic and cultural vitality of Oregon by preparing graduates to meet the growing demand for cybersecurity professionals, thereby enhancing the state's workforce and driving technological advancement. This initiative aligns with the broader mission of UO to impact local communities positively and contribute to the state's economic and cultural development.

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?

The proposed Master's degree in Cybersecurity will play a crucial role in meeting regional and statewide needs by enhancing educational attainment through accessible, high-quality learning opportunities in a critical field. It will equip students with the skills needed to address the increasing social, economic, and environmental challenges posed by cyber threats, thereby fostering a more resilient and secure community. By emphasizing interdisciplinary learning and ethical practices, the program will prepare graduates to respond effectively to diverse challenges and opportunities. Additionally, it will support civic and cultural demands by producing informed, responsible citizens who can contribute to the state's economic development and cultural enrichment. This initiative aligns with the broader mission of fostering innovation, inclusivity, and sustainability within Oregon and beyond.

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?

Courses for the Master’s program:

_____

5 Depth Courses (are Required) from this list (20 credits):
_____

CS532: Introduction to Networks

CS533: Computer and Network Security

CS534: Computer and Network Security II

CS536: Secure Software Development

CS537: Computer and Network Security Practicum

_____

3 Breadth Courses (are Required) from this list (12 credits):

_____

CS621: Algorithms and Complexity

CS670: Data Science

CS630: Distributed Systems

_____

1 Writing course (2 credit)s:

_____

CS640: Writing in Computer Research

_____

5 Elective Courses (or Internship, co-op or MS thesis) from this list (20 credits):

_____

CS632: Computer Networks

CS633: Advanced Network Security

CS510: Experimental Course: Ethics

CS510: Experimental Course: Cyberlaw

CS551: Database Processing

CS572: Machine Learning

CS604 Internship: Co-op (up to 12 credits)

CS604 Internship (up to 4 credits)

CS 503 MS Thesis (up to 12 credits)

*CS510: Advanced Crypto and Applications

*CS510: Cryptocurrency and Decentralized Finance

CS551: Database Processing

CS 571: Introduction to Artificial Intelligence

CS572: Machine Learning

CS510: Ethics

CS510 AI/ML for Network and Security Operations

"*" indicates courses that have been recently developed.

Important: the MS program offers a curriculum-integrated co-op option where students are matched with a qualified industry partner to spend 3 quarters of (paid) employment with that company/organization. For example, students in a cohort start the program in Fall quarter, take 3 quarters of specific classes (total of 9courses), then spend summer, Fall and Winter quarters at their co-op, and then return to UO for one quarter to take any remaining courses and graduate with their cohort in 2 years

The core set of required courses for the proposed Master's degree in Cybersecurity includes CS 532: Introduction to Networks, CS 533: Computer and Network Security, CS 534: Computer and Network Security II, CS 536: Secure Software Development, CS 537: Computer and Network Security Practicum, CS 633: Advanced Network Security. These courses are fundamental because they provide a comprehensive foundation in network principles, security protocols, and secure software development, which are critical to the field of cybersecurity. The rationale for emphasizing these courses lies in their ability to equip students with essential skills such as understanding network infrastructures, implementing robust security measures, and developing secure software applications. Central concepts include the fundamentals of network operations, advanced security techniques, and practical skills in cybersecurity applications and threat mitigation. This core curriculum ensures that graduates are well-prepared to address contemporary cybersecurity challenges and excel in both theoretical and practical aspects of the discipline.

Are there tracks or concentrations within the credential? If so, do these start from a common core or are they differentiated from the beginning?

There are currently no tracks or concentrations within the Master's in Cybersecurity.
As the program expands and matures in time, such options will be introduced accordingly.

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.

Cybersecurity Major Requirements

Code	Course List Title	Credits
Depth Courses		
CS 532	Introduction to Networks	4
CS 533	Computer and Network Security	4
CS 534	Computer and Network Security II	4
CS 536	Secure Software Development	4
CS 537	Computer and Network Security Practicum	4
Breadth Courses		
CS 621	Algorithms and Complexity	4
CS 670	Data Science	4
CS 630	Distributed Systems	4
Writing Course		
CS 640	Writing in Computer Research	2
Elective Courses		20
Select 5 of the following (20 credits)		
CS 503	Thesis [1]	
CS 551	Database Processing	
CS 571	Introduction to Artificial Intelligence	
CS 572	Machine Learning	
CS 604	Internship: [Topic] [2]	
CS 632	Computer Networks	
CS 633	Advanced Network Security	

Course List		
Code	**Title**	**Credits**
CS 510	Experimental Course: [Topic]	
Total Credits		54

[1] A maximum of 12 credits is allowed.
[2] A maximum of 4 credits is allowed for CS 604 Internship, and a maximum of 12 credits for CS 604 Internship: Co-op.

Expected Learning Outcomes for Students and Means of Assessment

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
Understand Fundamental Security Concepts: Gain essential knowledge and up-to-date techniques in cybersecurity, including fundamental security concepts and principles, applied cryptography, program security, and system and network security.	CS532 (Net Intro), CS533 (Comp Net Sec I), CS551 (DB Processing), CS632 (Comp Networks), CS630 (Distributed Systems)	CS510 (Forensics), CS534 (Comp Net Sec II), CS551 (DB Processing)	Homework, Discussions, Exams, Projects
Develop Hands-on Skills: Hone hands-on skills through computer and network security lab courses and security operation studies.	CS532 (Net Intro)	CS537 (Comp Net Sec Practicum)	Projects
Design and Implement Solutions: Draw on broad knowledge and hands-on skills to design, implement, and test solutions to cybersecurity tasks.	CS536 (Sec Software Dev), CS551 (DB Processing)	CS551 (DB Processing), CS632 (Comp Networks)	Homework, Discussions, Exams, Projects

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
Interdisciplinary Understanding: Understand the wide-ranging effects and interdisciplinary aspects of cybersecurity while attaining proficiency in one or multiple subdomains within the field.	CS510 (Ethics), CS510 (Law), CS670 (Data Sci)	CS510 (Ethics), SC510(AI/ML for Network and Security Operations), CS670 (Data Sci)	Homework, Discussions, Exams, Projects
Apply Foundational Knowledge: Apply and expand foundational knowledge and skills to new problem domains and emerging technologies.	CS621 (Algorithms and Complexity), CS630 (Distributed Systems), CS670 (Data Science)	CS510 (Crypto Advanced), CS510 (Crypto Finance), CS572, CS630	Homework, Discussions, Exams, Projects
Effective Communication: Possess effective communication and collaboration abilities, expressing ideas clearly and concisely both orally and in written form.	CS640 (Wri in Comp Research)	CS640 (Wri in Comp Research)	Homework, Discussions, Papers
Ethical Decision-Making: Adhere to ethical principles and make well-informed decisions in the field of cybersecurity.	CS510 (Ethics)	CS510 (Ethics)	Homework, Discussions, Papers, Projects

Expected Learning Outcomes (Will Appear in Catalog)

	Learning Outcomes
1	Understand Fundamental Security Concepts: Gain essential knowledge and up-to-date techniques in cybersecurity, including fundamental security concepts and principles, applied cryptography, program security, and system and network security.
2	Develop Hands-on Skills: Hone hands-on skills through computer and network security lab courses and security operation studies.
3	Design and Implement Solutions: Draw on broad knowledge and hands-on skills to design, implement, and test solutions to cybersecurity tasks.
4	Interdisciplinary Understanding: Understand the wide-ranging effects and interdisciplinary aspects of cybersecurity while attaining proficiency in one or multiple subdomains within the field.
5	Apply Foundational Knowledge: Apply and expand foundational knowledge and skills to new problem domains and emerging technologies.
6	Effective Communication: Possess effective communication and collaboration abilities, expressing ideas clearly and concisely both orally and in written form.
7	Ethical Decision-Making: Adhere to ethical principles and make well-informed decisions in the field of cybersecurity.

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
10	15	25	30	40

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

Number of Degrees:

Year 1	Year 2	Year 3	Year 4	Year 5
8	13	20	25	35

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

Collaboration with the CS department and ASU8.

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?

Expected Student Characteristics

Resident: Oregon residents looking to advance their careers locally.

Out-of-State: Students from across the U.S. attracted by the program's reputation and unique offerings along with the growing job market in the area of Cybersecurity.

International: International students seeking specialized education in cybersecurity, leveraging Oregon's diverse academic environment.

Student Type:

Traditional: Recent graduates with a Bachelor's degree in Computer Science, Information Technology, or related fields.

Nontraditional: Career changers or professionals with industry experience looking to deepen their cybersecurity expertise.

Enrollment Status:

Full-Time: Students committed to completing their degree within a typical two-year timeframe.

Part-Time: Working professionals balancing education with their job responsibilities.

Appealing Backgrounds and Career Goals

Technical Backgrounds: Individuals with degrees in Computer Science, Engineering, Information Technology, and related fields.

Professionals in IT or Cybersecurity: Those already working in IT, network security, or cybersecurity roles who seek advanced knowledge and career progression.

Career Changers: Professionals from other fields with a strong interest in transitioning to cybersecurity, leveraging the growing demand in the industry.

Aspiring Security Experts: Students aiming for roles such as Security Analyst, Network Security Engineer, Cybersecurity Consultant, or roles in government and private sectors related to national security.

This program's blend of theoretical knowledge, practical skills, and interdisciplinary understanding is designed to cater to a wide range of students with diverse backgrounds and career aspirations.

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.

Career Paths

Information Security Analyst: These professionals plan and carry out security measures to protect an organization's computer networks and systems. According to the U.S. Bureau of Labor Statistics (BLS), employment for information security analysts is projected to grow by 33% from 2023 to 2033. The median annual wage for this role was $120,360 in 2023. (ref: https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm)

Security Engineer: Security engineers build and implement defense systems against security threats. They can advance to roles like security architect, responsible for an organization's entire security infrastructure. (ref: https://www.coursera.org/articles/cybersecurity-career-paths)

Penetration Tester: These professionals simulate cyberattacks to identify vulnerabilities in systems and networks. This role is crucial for maintaining robust security measures. (ref: https://www.springboard.com/blog/cybersecurity/cybersecurity-career-paths/)

Incident Responder: Incident responders manage and mitigate the impact of security breaches, restoring systems and improving defenses. (ref: https://www.springboard.com/blog/cybersecurity/cybersecurity-career-paths/)

Cybersecurity Consultant: Consultants evaluate an organization's security measures and

provide recommendations for improvement. This role often involves working with various clients and industries. (ref: https://www.springboard.com/blog/cybersecurity/cybersecurity-career-paths/)

Evidence of Prospects for Success

Employment Statistics: The BLS projects a 33% growth in employment for information security analysts from 2023 to 2033, indicating strong job prospects. Additionally, the cybersecurity job market is expected to grow significantly, with an estimated 3.5 million jobs projected to go unfilled by 2025. (ref: https://www.springboard.com/blog/cybersecurity/cybersecurity-career-paths/)

Salary Information: Cybersecurity professionals enjoy competitive salaries. For example, the average salary for information security analysts was over $110,000 in 2021. (ref: https://www.comparitech.com/blog/information-security/cybersecurity-job-statistics/)

Graduate Work Opportunities: Many cybersecurity graduates pursue advanced degrees or certifications to further their careers. Graduate programs in cybersecurity are available at various universities, providing opportunities for further specialization and research. (ref: https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm)

Licensure and Certifications: Professional certifications such as CompTIA Security+, Certified Information Systems Security Professional (CISSP), and Google Professional Cloud Security Engineer are highly valued in the industry. These certifications can enhance job prospects and career advancement. (ref: https://www.coursera.org/articles/cybersecurity-career-paths)

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.]

To ensure that the proposed Master's program in Cybersecurity does not overlap with existing programs or compete for the same population of students, the following steps have been taken:

Course Overlap Policy Review: The program has been reviewed in accordance with the University of Oregon's course overlap policy. This policy allows for some overlap but ensures that it promotes intellectual coherence and does not erode program identity. The program has been designed to offer unique courses that do not duplicate content from other programs. (ref: https://provost.uoregon.edu/course-overlap-between-two-or-more-programs-policy)

Consultation with Other Departments: The Cybersecurity program team has consulted with other departments to identify potential overlaps and ensure that the new program complements rather than competes with existing programs. This includes discussions with departments offering related degrees such as Computer Science and Data Science.

Market Analysis: A market analysis has been conducted to understand the demand for cybersecurity education and identify the target student population. This analysis helps in designing a program that attracts students with specific career goals and backgrounds, ensuring it does not compete with other programs for the same students.

Unique Program Features: The program includes unique features such as hands-on labs, security operation studies, and a focus on emerging technologies, which differentiate it from other programs and attract students interested in practical, applied learning experiences.

These steps help ensure that the proposed Cybersecurity program is distinct and complements the University of Oregon's existing academic offerings.

Attach your communications showing due diligence in consulting with other UO departments or areas.

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

Program(s)
BS in Cybersecurity, PhD Computer Science as NSA CAE-R

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.

OSU offers a Cybersecurity certificate which has a different focus and covers different courses. PSU offers a non-degree certificate in Cybersecurity which does not have a technical depth of our program. Given the huge need for Cybersecurity workforce across the state, there is a clear demand for total capacity of these programs apart from differences in their focus. In fact, Oregon legislature is demanding more training programs at major public universities to address growing Cybersecurity challenges that state is facing. Through the OCCoE, there is coordination (and no competition) among three universities regarding our Cybersecurity offerings.

If applicable, explain why collaborating with institutions with existing similar programs would not take place.

We are not aware of any master's degree in Cybersecurity at UO. We are also exploring ways to involve other units, namely UO Law School, in our Cybersecurity programs.

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

N/A

Document your due diligence in consulting with other Oregon institutions.
Please contact the Office of the Provost for instructions prior to contacting another institution about this program proposal.

If the program's location is shared with another similar Oregon public university program, provide externally validated evidence of need.

N/A

Attach Corroborating Documentation

Resources Required to Offer the Program

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)	Professor	1.0	Director
Jun Li (TT)	Professor	1.0	Faculty
Joe Li (TT)	Professor	1.0	Faculty
Ram Durairajan (TT)	Associate Professor	1.0	Faculty
Dan Carrere (NTT)	Senior Instructor I	1.0	Faculty
Roberto Hoyle	Senior Instructor I	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.

Most faculty have significant experience in their discipline. All listed faculty contributed to the recent recognition of NSA CAE-R designation (for PhD Program).

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 and offer 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.

Students will be advised both via Tykeson Advising and a dedicated program advisor within the computer science department.

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

Given the current level of staffing for Computer Science and Cybersecurity offerings, we have adequate staffing in terms of faculty and support.

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

Our department currently has the facilities, equipment, and other resources that are needed to offer the Master's in Cybersecurity.

Describe your plans for development and maintenance of unique resources (buildings, laboratories, technology) necessary to offer a quality program.

Most of the classwork will use class space and specialized space that is already present and developed via state funds from OCCoE and other sources within industry (such as Ripple, etc.). We are also using these funding sources for Teaching Security Operations Center (TSOC) and Risk Clinic.

What is the targeted student/faculty ratio? (student FTE divided by faculty FTE)

We target 1:15 to 1:20 and as the program matures we aim to have increase the number of students served per section.

What are the resources to be devoted to student recruitment?

Initial recruitment will begin through our industry partners network as we promote the Master's in Cybersecurity to industry employers.
We will also promote to our Computer Science and Cybersecurity majors as well as at partner institutions and other
Our Summer Bridge courses will aid students originating from other majors to transition into the major.
We will also promote to Computer Science and Cybersecurity interested students across the state via Email promotions and via information from our website and including Teaching Security Operations Center (TSOC) and Risk Clinic. We will also collaborate with UO Office of International Scholars to promote the program in addition to other areas to India.
Lastly other associated colleges and universities around the state will have the information shared with them on an ongoing basis.

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.

Grading related criteria for MS in Cybersecurity will mirror the Computer Science policies for MS in Computer Science.

The math courses will continue to be taken for a grade and passed with a C- or better.
The new required ethics course must be taken for a grade and passed with a C- or better.

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.
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.

We follow the same policies that are employed within the Master's in Computer Science.
We are not aware of any specific credentials with overlap limits.
Specifically the Cybersecurity Certificate can be used to graduate into the Master's in Cybersecurity degree. As such, the Cybersecurity Certificate is subset of the Master's in Cybersecurity and has 100 % overlap. It is therefore able to extend into becoming the Master's by design. No other additional overlap exist with other graduate programs.
Students who have taken the required courses in the BS in Cybersecurity / Computer Science can receive credit towards the same course within the masters degree (up to 6 courses).

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:

The proposal does NOT rely on a new course as its a part of its requirements. However, we have recently developed a few new courses to expand the scope our cybersecurity programs

including this MS in Cybersecurity. Some of the newly developed courses are the following:

CS510: Digital Forensics

CS510: AI/ML for Network and Security Operations

CS510: Advanced Crypto and Applications

CS510: Cryptocurrency and Decentralized Finance

We plan to submit these courses for review and approval in a near future.

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?

Admissions criteria for MS in Cybersecurity will mirror the Computer Science policies for MS in Computer Science.

Please describe admission procedures (Will Appear in Catalog)

Bachelor's degree in Computer Science or a related field or department approval.

Minimum GPA, often around 3.0 on a 4.0 scale.

GRE scores (some programs have waived this requirement).

English proficiency (TOEFL or IELTS) for international students.

Letters of recommendation (usually 2–3).

Statement of purpose outlining academic interests and goals.

Resume or CV.

Transcripts from all post-secondary institutions attended.

Program's 'Overview' page in the Catalog (Will Appear in Catalog)

Master's degree in Cybersecurity at the University of Oregon aims to equip students with comprehensive knowledge and skills in safeguarding digital information and infrastructure. Students will engage in rigorous coursework and hands-on projects that address current cybersecurity challenges, such as network security, cryptography, and risk management.

The program's focus is to develop professionals who can anticipate, identify, and mitigate cyber threats in diverse organizational contexts. Learning objectives include mastering advanced cybersecurity techniques, understanding legal and regulatory frameworks, and developing strategic problem-solving skills. Graduates will earn a Master of Science (MS) degree in Cybersecurity, preparing them for leadership roles in both the private and public sectors, where their expertise will be crucial in protecting critical digital assets.

Program Restrictions (Will Appear in Catalog)
Cybersecurity Major cannot Major or Minor in Computer Science.

Residency Requirements (Will Appear in Catalog)
Students must be on campus for all units.

Initial plan is to follow the same residential requirements of other Masters in Computer Science department (Computer Science, Data Science).

We are exploring the option of remote delivery of some courses if/when this MS degree is offered at UO campus in Portland in the future.