AY23-41-C

Dear Chair Carhart and Faculty Senators,

The attachment below includes a proposal for a PhD in Cybersecurity. The proposed PhD program will help to increase the number of graduate students at ODU, which is a distinct strategic plan goal. A few points are worth highlighting:

1. The program builds on the successful MS program in Cybersecurity, which was approved by the senate five years ago.
2. A survey of ODU's cybersecurity students found significant demand for the program. The survey was completed by 27 cybersecurity seniors and 50 graduate students. Of 50 MS students in the survey, the vast majority (86%) said they would definitely (20), very likely (16), or likely (7) enroll in the proposed program. Of the 27 undergraduate students, 70% were in these same categories.
3. The required courses will be covered by cybersecurity faculty. The electives include courses from across campus. The structure of the electives, or as the nursing faculty refer to them – "selectives" – is such that no one department would be overwhelmed by cybersecurity enrollments. Because of the interdisciplinary nature of cybersecurity, students are required to select electives from three different disciplines. The curriculum was shared with all chairs/directors that had courses in the list of electives. No chair/director asked to have courses removed, though one asked to have a course added.
4. Funds from the Coastal Virginia Center for Cyber Innovation, supported by the Commonwealth Cyber Initiative, will support the program.

Because of the timing it takes for new PhD programs to be created in the Commonwealth, in order to have this program begin in Fall 2025, we would need senate approval this semester.

Please let me know if you have any questions.

Regards,

Brian K. Payne, PhD
Vice Provost for Academic Affairs

STATE COUNCIL OF HIGHER EDUCATION FOR VIRGINIA
PROGRAM PROPOSAL COVER SHEET

1. Institution Old Dominion University	2. Academic Program (Check one): New program proposal ___X___ Spin-off proposal _____ Certificate document _____
3. Name/title of proposed program Cybersecurity	4. CIP code 11.1003
5. Degree/certificate designation Doctor of Philosophy	6. Term and year of initiation Fall 2025
7a. For a proposed spin-off, title and degree designation of existing degree program 7b. CIP code (existing program)	
8. Term and year of first graduates Summer 2028	9. Date approved by Board of Visitors XXXXX
10. For community colleges: date approved by local board date approved by State Board for Community Colleges	
11. If collaborative or joint program, identify collaborating institution(s) and attach letter(s) of intent/support from corresponding chief academic officers(s)	
12. Location of program within institution (complete for every level, as appropriate and specify the unit from the choices). Departments(s) or division of _____ School(s) or college(s) of School of Cybersecurity Campus(es) or off-campus site(s) Main Campus, Norfolk Mode(s) of delivery: face-to-face ___X___ distance (51% or more web-based) ___X___ hybrid (both face-to-face and distance) ___X___	
13. Name, title, telephone number, and e-mail address of person(s) other than the institution's chief academic officer who may be contacted by or may be expected to contact Council staff regarding this program proposal. Sierra Croker, scroker@odu.edu, 757-683-3154	

TABLE OF CONTENTS

DESCRIPTION OF THE PROPOSED PROGRAM.. 1

PROGRAM BACKGROUND 1
MISSION 5
ONLINE DELIVERY..... 5
ADMISSION CRITERIA..... 5
TARGET POPULATION..... 6
CURRICULUM 6
STUDENT RETENTION AND CONTINUATION PLAN 6
TIME TO DEGREE 7
FACULTY 7
PROGRAM ADMINISTRATION 11
STUDENT ASSESSMENT 12
EMPLOYMENT SKILLS/WORKPLACE COMPETENCIES 15
PROGRAM ASSESSMENT 15
BENCHMARK OF SUCCESS 16
EXPANSION OF EXISTING PROGRAM 17
RELATIONSHIP TO EXISTING ODU DEGREE PROGRAMS..... 17
COMPROMISING EXISTING DEGREE PROGRAM 17
COLLABORATION OR STANDALONE..... 17

JUSTIFICATION FOR THE PROPOSED PROGRAM.……..……..……17

RESPONSE TO CURRENT NEEDS (SPECIFIC DEMAND) 17
EMPLOYMENT DEMAND ……..……. 21
STUDENT DEMAND ……..21
DUPLICATION 24

PROJECTED RESOURCE NEEDS ……...……..…

RESOURCE NEEDS …….
RESOURCE NEEDS: PARTS A-D .....

APPENDICES ……..……..…….

APPENDIX A - SAMPLE PLAN OF STUDY
APPENDIX B - COURSE DESCRIPTIONS
APPENDIX C - FACULTY CURRICULUM VITAE (ABBREVIATED)
APPENDIX D - EMPLOYMENT DEMAND - JOB ANNOUNCEMENTS
APPENDIX E - STUDENT DEMAND-STUDENT SURVEY
APPENDIX F - UNSOLICITED EMAILS DEMONSTRATING DEMAND

Description of the Proposed Program

Program Background

Old Dominion University (ODU) seeks approval to initiate a Doctor of Philosophy in Cybersecurity, scheduled to begin Fall 2025 in Norfolk, Virginia. This proposed program will be housed in the interdisciplinary School of Cybersecurity.

The proposed research-based interdisciplinary PhD in Cybersecurity combines a strong technical foundation with policy, management, and social sciences perspectives. It is designed to educate students to become cybersecurity scholars capable of teaching about and studying complex topics related to the subject matter. Graduates of the program will be prepared to educate future cybersecurity professionals, so those professionals are able to develop solid solutions that secure the cyber space of individuals and organizations in various sectors of industry, military, and government. The program will prepare individuals who have a strong understanding of cybersecurity topics and the ability to translate subject matter to students seeking knowledge about topics such as cyber systems, cyber threats, cyber defense, and operation technologies. In addition, graduates will have the skills to enter research careers where they will be able to study the theory, technologies, skills, and practices necessary to address the daily challenges in protecting critical cyber infrastructure and assets. They will have enhanced oral and written communication skills to articulate cybersecurity problems and decisions in a cohesive and well-structured way. Finally, graduates will clearly understand ethical standards and rules for cybersecurity scholars, allowing them to promote social responsibility in cybersecurity coursework, research, and innovations. The interdisciplinary nature of the proposed program distinguishes it from traditional doctoral degree programs in computer science, engineering, or social sciences.

This program is designed to help prepare cyber security professors and researchers. Graduates will develop skills and competencies in technical aspects of cyber security in a diversity of current and emerging cyber security technologies and will be prepared to conduct empirical cybersecurity research. The program will prepare graduates to teach in higher education programs and conduct research in public and private sectors aiming to build scientific understanding about cybersecurity.

The proposed PhD in Cybersecurity responds to the urgent need for cybersecurity professionals in the Commonwealth of Virginia, the nation, and the world. Virginia has more cybersecurity job vacancies than any other state. Across the United States, there were 572,392 cybersecurity job vacancies in the February 2024. More than ten percent of those job vacancies (n=58,407) were in Virginia.[1] The most recent data from the Bureau of Labor Statistics confirms that Virginia employs more information security analysts than any other state.[2] The need nationally and in Virginia for cybersecurity professionals stems from the need to protect cyberspace. As noted in Apple's report *The Continued Threat to Personal Data: Key Factors Behind the 2023 Increase*, "For US organizations, data breaches are now at an all-time high. In just the first nine months of 2023, data breaches in the US have already increased by nearly 20% compared to all

[1] Cyberseek.org.

[2] Bureau of Labor Statistics. Available online at Information Security Analysts (bls.gov)

of 2022."[3] This increase in data breaches results in significant economic losses given estimates that each breach costs $4.45 million.[4]

There is widespread agreement that cybersecurity job vacancies in government and industry careers have required the development of new cybersecurity programs in higher education institutions across the United States. Programs that have been developed have been housed in a wide range of programs including computer science, information technology, computer engineering, and others. Interdisciplinary programs have also been developed. Faculty who have developed these programs have relied on their own disciplinary backgrounds in developing cybersecurity curricula for Bachelor of Science and Master of Science degrees. With the growth of cybersecurity programs and cybersecurity scholarship, it has become increasingly clear that cybersecurity doctoral programs are needed.

To be sure, Bachelor's and Master's degree programs in cybersecurity have been developed in Virginia and across the United States to prepare professionals who are able to fill the growing number of job vacancies and guard against and respond to security challenges. In Virginia, twenty-two associate's, bachelor's and Master's degree programs in cybersecurity have been developed, but no PhD program has been developed.[5] According to one author team, "The challenge of meeting the cybersecurity work-force shortage through degree programs is intensified by the reality of the limited number of cybersecurity and engineering faculty at colleges and universities."[6] (Burrell et al., 2020). The proposed degree program will prepare faculty and researchers to educate future professionals and study complex topics. Graduates will become the new generation of cybersecurity scholars able to teach about and study strategies for preparing the cybersecurity workforce to safeguard information relating to national security and various sensitive business and personnel data.

In recent years, cyber attacks have become more common, sophisticated, and harmful. In fact, no organization or individual with an online presence is immune to attacks, and the impact of cyber attacks can be devastating. As the volume and sophistication of cyber attacks grow, there is a strong demand for a well-trained cybersecurity workforce to address the multifaceted cybersecurity problems,[7] which require an advanced education to develop skillsets that not only cover basic cybersecurity coursework but that will also provide students with multidisciplinary perspectives to examine security from a holistic view. Moreover, many cybersecurity careers require the completion of a master's degree. While efforts have been underway to grow cybersecurity programs at the undergraduate and master's level, efforts to build doctoral

---

[3] https://www.apple.com/newsroom/pdfs/The-Continued-Threat-to-Personal-Data-Key-Factors-Behind-the-2023-Increase.pdf

[4] Cost of a data breach 2023 | IBM

[5] https://research.schev.edu/rdPage.aspx?rdReport=degreeinventory.DegreeInventory_SCHEV&Tab=cip

[6] Burrell, D. N., Dawson, M. E., & Nobles, C. (2020). Innovative doctorate programs in cybersecurity, engineering, and technology in the USA and UK that can be completed by professionals around the world without relocation. In *ICRMAT* (pp. 1-3). Available online.

[7] "Multifaceted security: preparing your cyber offense", Page 2, http://www.ey.com/Publication/vwLUAssets/EY-top-of-mind-four-themes-multifaceted-security/$FILE/EY-top-of-mind-four-themes-multifaceted-security.pdf

programs have lagged behind. The result is that it has become increasingly difficult to hire and credential cybersecurity faculty in associate's, bachelor's, and master's degree programs.[8]

Rationale for the Program at Old Dominion University

Old Dominion University began its formal cybersecurity initiative in 2015 with the creation of the Center for Cybersecurity Education and Research and the development of an interdisciplinary undergraduate major in cybersecurity. Since then, the Center evolved into one of the nation's first Schools of Cybersecurity and degree programs were added at the bachelor's and master's levels. The School of Cybersecurity at ODU now houses one of the largest cybersecurity programs in the nation. It represents an interdisciplinary effort bringing together more than three dozen faculty members with a wide range of expertise in computer science, electrical and computer engineering, information technology, criminal justice, cyber laws, psychology, and philosophy. The interdisciplinary team enables a holistic approach to cybersecurity problems. The School offers a BS in Cybersecurity with majors in cybersecurity and cyber operations, and an MS in Cybersecurity with a total of more than 1,500 students. It has been designated by NSA as a National Center of Academic Excellence in Cyber Operations (CAE-CO) and a National Center of Academic Excellence in Cyber Defense (CAE-CD). Cybersecurity research is flourishing in the School. The School works closely with the cybersecurity industry, military units, government agencies, and educational institutions, to promote cybersecurity workforce development and research and innovation.

The ODU School of Cybersecurity offers two degree programs – a BS degree and an MS degree. In Fall 2015, ODU established a cybersecurity major offered as an Interdisciplinary Studies (IDS) Bachelor of Science (BS) degree through the College of Arts and Letters. That major evolved into a standalone degree major while maintaining its interdisciplinary foundations. The 120-hour curriculum provides opportunities for students to integrate education and training with application of problem-solving skills in the laboratory. Courses are drawn from the disciplines of Philosophy, Computer Science, Computer Engineering, Modeling and Simulation, Information Technology, English, Interdisciplinary Studies, and Criminal Justice. The cybersecurity BS curriculum is divided into four sections: (1) the interdisciplinary core, (2) law and ethics, (3) cybersecurity foundations, and (4) cybersecurity applications. This curriculum is in addition to general education courses, prerequisites, and electives which students take to complete the 120 credit hours.

The primary advantage of the cybersecurity BS curriculum at ODU is that it responds to the interdisciplinary nature of cybersecurity. The equal emphasis on cybersecurity foundations and applications parallels the philosophy of the Computing Research Association; namely: "Computer science and computer engineering graduates should possess a thorough education in cybersecurity and related fundamentals and principles as well as training in cybersecurity-specific technologies, tools, and skills."[9]

---

[8] Burrell, D. N., Dawson, M. E., & Nobles, C. (2020). Innovative doctorate programs in cybersecurity, engineering, and technology in the USA and UK that can be completed by professionals around the world without relocation. In *ICRMAT* (pp. 1-3). Available online.

[8] "Multifaceted security: preparing your cyber offense", Page 2,

[9] McGgettrick, A. (2013). Toward curricular guidelines for cybersecurity. Association for Computing Machinery.

Building on the success of the undergraduate programming, ODU created a Master of Science in Cybersecurity in 2018. The MS program grew quickly from 14 students in Fall 2018 to 203 students in Fall 2023. The undergraduate program grew in even larger numbers. When the program was first created in 2015, 11 students were enrolled in the program. In Fall 2023, 1,244 students identified as cybersecurity majors. In other words, the cybersecurity programs experienced a more-than 100-fold over an eight-year time period.

To support the growth in the degree programs and enhance cybersecurity research, ODU has invested significantly to support the cybersecurity initiative, including about a half million dollars equipment fund to create a state-of-the-art cybersecurity infrastructure, named Cybersecurity Research Environment (CRE). This environment supports research, education, and outreach activities. It enriches course projects by implementation and experimental activities, providing students with hands-on experience, which has been shown to be an important factor in stimulating students' interest and sharpening their scientific reasoning and problem-solving skills. An additional $3 million was invested in creating the Cyber Innovation Park, the physical location where the School is housed. The School occupies 10,000 square feet of newly renovated space for classrooms, student commons, cyber labs, offices, meeting rooms, and a data center. The School operates a unique cybersecurity research and education infrastructure, established in 2017 and enhanced since then by multi-million dollars of cyberinfrastructure grants and state investment. It enables students to carry out hands-on exercises, learn cybersecurity tools and techniques, and work with faculty on research projects.

In addition, Old Dominion University has taken a lead in developing and fostering community partnerships between businesses, non-profits, public service units, and regional contractors. Three programs central to these partnerships are the Hampton Roads Cybersecurity Education, Workforce, and Economic Development Alliance (HRCyber), the Virginia Cyber Alliance, and the Coastal Virginia Cybersecurity Initiative. Created in 2016, HRCyber was designed to promotion regional collaboration between high school programs, higher education institutions, businesses, and non-profits. Supported through a grant from the National Institute for Standards and Technology, HRCyber formalized degree pathways between regional institutions, led to the development of a regional cybersecurity internship program, created cybersecurity partnerships between businesses and higher education institutions, and resulted in ODU changing its cybersecurity curriculum to better meet the needs of the business community. The HRCyber Co-Laboratory expanded on HRCyber to create additional internships and a digital entrant program, which provides businesses salary support for hiring new cybersecurity workers. More recently, as part of Virginia's Commonwealth Cybersecurity Initiative, ODU led the development of the Coastal Virginia Center for Cyber Innovation. CoVA CCI provided an opportunity to fiscally sustain the HRCyber initiative and connects cybersecurity researchers, faculty, students, and businesses across the region and the state.

ODU's growth in cybersecurity programming, investment in its cybersecurity research infrastructure, and leadership in business partnerships provides the foundation needed for a vibrant and innovative PhD program in cybersecurity.

Mission

The mission of the institution states: "Old Dominion University, located in the City of Norfolk in the metropolitan Hampton Roads region of coastal Virginia, is a dynamic public research institution that serves its students and enriches the Commonwealth of Virginia, the nation and the world through rigorous academic programs, strategic partnerships, and active civic engagement." The PhD in Cybersecurity aligns with this mission by (1) offering a robust curriculum that trains individuals in the field of cybersecurity, (2) enhances research on cybersecurity, and (3) strengthening ODU's commitment to contributing to the economy and workforce of the Hampton Roads region and the Commonwealth of Virginia through cybersecurity research.

Online Delivery

The proposed doctoral degree program will be available on-campus and through a fully online format, with students accessing course materials through Canvas, the University's course management system. All assignment submissions and other course management actions will take place in Canvas. Further, faculty-student interaction is available via email, phone, in-person meetings, and Zoom.

Faculty members who teach in the web-based format are trained in course development and delivery through ODUGlobal. There, instructional designers and technologists work individually with each faculty member to convert course content, assignments, testing, and other course work to a web-based platform. Faculty work closely with the designers to ensure web-based content is the same as content taught in face-to-face settings.

Beyond the usual online offerings at ODU, cybersecurity is a field that requires extensive hands-on experience, which has been shown to be an important factor in stimulating students' interest and sharpening their scientific reasoning and problem-solving skills. To this end, ODU has made significant investments in the creation of a state-of-the-art cybersecurity infrastructure, including a cybersecurity lab consisting of dedicated workstations, a Nutanix hyper-converged system that supports virtual machines, two Cisco lab switches, a Cisco N3k-3172-T data center grade switch, and a Palo Alto 850 NGFW firewall. On-campus and online students can remotely connect to the lab facility to conduct various real-world cybersecurity experiments.

Admission Criteria

All students applying to graduate degrees at Old Dominion University will meet criteria established by the Graduate School. Criteria for acceptance into the Doctor of Philosophy in Cybersecurity include the following:

- Online application and application fee
- A bachelor's degree from a regionally accredited university in the U.S. or an equivalent foreign institution
- Official copies of transcripts of all regionally accredited colleges and universities attended.

- Two letters of recommendation from individuals familiar with the applicant's professional and/or academic background
- A current resume
- A statement of professional goals
- Current scores on the Test of English as a Foreign Language (TOEFL) with a minimum of 230 on the computer based TOEFL or 80 on the TOEFL iBT, if the applicant's native language is not English.

Students with previously completed work at a regionally accredited institution may submit a request for a maximum of 12 elective graduate credit hours to be transferred into the program. If approved by the admission committee, it will be added to the transcript.

Target Population

Three sets of students will be targeted for the proposed program. The first will be Old Dominion University students who are currently enrolled in the cybersecurity programs at ODU. For many, it will represent a natural progression, particularly if they are currently working in, or have plans to, work higher education or research.

The second target group includes cybersecurity students enrolled in bachelor's and master's degree programs across the Commonwealth of Virginia and nation. In particular, those with interest in teaching about and researching cybersecurity will be the target group. The availability of the online option will allow us to target students from across the Commonwealth of Virginia who otherwise may not be able to move.

The third target group includes current cybersecurity instructors who have a master's degree but no doctoral degree and are teaching at community colleges across the Commonwealth and nation. Other doctoral programs at ODU have successfully provided doctoral training to this segment of the higher education community by offering online degree programs in their disciplinary areas.

Curriculum

The Doctor of Philosophy in Cybersecurity is a 78-credit hour degree program. A dissertation is required. Students who begin the PhD program after having earned a Master's degree will complete a 48-credit hour degree program.

The proposed program will establish a solid educational foundation and prepare graduates for careers as higher education researchers, industry researchers, and cybersecurity leaders. Those entering the program straight from an undergraduate program will take coursework that include all core components of cybersecurity including cryptography, critical infrastructures, cyber threats and vulnerabilities, risk assessment and management, cyber defense and operation techniques, forensic investigation, and cyber laws and ethics. These students will also take four core courses that focus on the fundamental knowledge of cybersecurity, covering advanced cybersecurity principles, techniques, and operations, as well as advanced topics in law, policy, management, and leadership in cybersecurity.

Students entering from an undergraduate degree program will have opportunities to choose five restricted electives to learn about different aspects of cybersecurity, e.g., in information systems, network systems, clouds, mobile and wireless systems, operating systems, and cyber-physical systems (including the emerging Internet-of-Things). Courses are also offered to address such important cybersecurity topics as reverse software engineering, digital forensics, thread modeling, and ethical hacking and penetration testing. Students will learn how to identify problems, gather information, analyze data, define hypotheses, develop solutions, establish contingencies, and effectively articulate and communicate results. They will also have opportunities to interact with potential employers through recruitment and networking events.

After students have completed the foundational cybersecurity coursework and the master's project, they will begin to take advanced core requirements and advanced electives. Those who enter with a master's degree, will begin their curriculum with the advanced courses. The advanced core courses focus on topics such as ethical issues from emerging technologies, how to approach cybersecurity through an interdisciplinary lens, the use of multi-method strategies to study cybersecurity, and applied experiences in the areas of teaching and studying cybersecurity.

Students must successfully complete a dissertation. While working on the dissertation, students will enroll in dissertation research coursework (CYSE 899).

Program Requirements

Cybersecurity Core Courses* (30 hours)
CYSE 600 Cybersecurity Principles
CYSE 601 Advanced Cybersecurity Techniques and Operations
CYSE 603 Advanced Cybersecurity Law and Policy
CYSE 605 Leadership and Management in Cybersecurity
CYSE 616 Cyber Defense Fundamentals.
CYSE 800 Research Methods in Cybersecurity
CYSE 701/801 Advanced Cybersecurity Techniques and Operations II
CYSE 802 Cybersecurity Seminar
CYSE/PHIL 703/803 Moral Reasoning for Emerging Technologies
CYSE 868 Cybersecurity Practicum
*The 600 level courses would not be required for those entering with an MS degree.

Restricted Foundational Electives (15 hours)**
Select 15 credits of the following:
CYSE 519 Cyber Physical System Security
CYSE 520 Applied Machine Learning in Cybersecurity
CYSE 525 Cybersecurity Strategy and Policy
CYSE 526 Cyber War
CYSE 595 Topics in Cybersecurity
CYSE 607 Advanced Digital Forensics
CYSE 610 Advanced Cryptography
CYSE 615 Mobile and Wireless Security

CYSE 625 Advanced Ethical Hacking and Penetration Testing
CYSE 635 AI Security and Privacy
CYSE 695 Advanced Topics in Cybersecurity
CYSE 697 Independent Study in Cybersecurity
CS 564 Networked Systems Security
CS 565 Information Assurance for Cybersecurity
CS 566 Principles and Practice of Cyber Defense
CS 567 Introduction to Reverse Software Engineering
CS 761/ 861 Malware Analysis and Reverse Engineering (3 Credit Hours)
CS 569 Data Analytics for Cybersecurity
CS 522 Introduction to Machine Learning (3 Credit Hours)
CS 580 Introduction to Artificial Intelligence (3 Credit Hours)
CS 624 Data Analytics and Big Data (3 Credit Hours)
CS 722/ 822 Machine Learning (3 Credit Hours)
CS 733/ 833 Natural Language Processing (3 Credit Hours)
ENMA 625 Introduction to Homeland Security Logistics
MSIM 670 Cyber Systems Engineering
**Students entering with an MS will not take these courses.

Advanced Electives (15 hours)
Select 15 hours from three different disciplines.
CRIM 832 Advanced Cybercriminology (3 Credit Hours)
CS 764 Blockchains and Cryptocurrencies: Fundamentals, Technologies, and Economics (3 Credit Hours)
CS 865 Internet of Things Security (3 Credit Hours)
CS 872 Advanced Computer and Network Security (3 Credit Hours)
CS 873 Data Mining and Security (3 Credit Hours)
CS 874 Distributed System Security with .Net (3 Credit Hours)
CYSE 897. Independent Study (3 credit hours).
ENGL 830 The Digital Humanities (3 Credit Hours).
ENMA 801 Digital Systems Engineering (3 Credit Hours)
ENMA 824 Risk Analysis (3 Credit Hours)
ENMA 825 System Risk and Failure Analysis (3 Credit Hours)
ENMA 850 System of Systems Engineering (3 Credit Hours)
ENMA 855 Human System Engineering (3 Credit Hours)
ENMA 871 Risk and Vulnerability Management of Complex Interdependent Systems (3 Credit Hours)
ECE 742 Computer Communication Networks (3 Credit Hours)
IDT 830 Principles and Practices of Human Performance Technology
IS 721/821 New World Order: Chaos or Coherence?
PSYC 870 Human Factors Psychology (3 Credit Hours)
PSYC 876 Human-Computer Interaction (3 Credit Hours)
Other approved electives.

<u>Dissertation Research:</u>
CYSE 899 Doctoral Dissertation (18+ credits)

Candidacy Examination
Students in the PhD in Cybersecurity will be required to pass written and oral examinations to qualify for candidacy for the degree of Doctor of Philosophy. These examinations will assess the student's ability to coherently relate information taken from the core and research skills courses in a critical and scholarly manner. The student's advisor must recommend the student for the candidacy exam during the semester in which he/she is scheduled to complete all coursework (except for dissertation hours) required for the degree. The graduate program director (GPD) is responsible for coordinating the administration of the written and oral candidacy examinations and will appoint a committee to administer the exams. The examination committee will be made up of at least three (3) faculty members, all of whom must be graduate certified and two of whom must be affiliated with the School of Cybersecurity. The procedure for candidacy exams will follow guidelines in the Old Dominion University Graduate Catalog.

After successful completion of the written examination, an oral examination, which must be taken prior to the end of the next semester, is given addressing topics discussed in the written examination and possible additional materials. All students must pass both the written and oral candidacy examinations. Any student not passing an examination will be allowed to take it a second time. If a student does not pass an exam on the second attempt, that student will be suspended from the program.

Dissertation Research
Once the written and oral candidacy examinations have been passed, a dissertation committee will be formed to supervise dissertation research. This committee will be formed by the student, in consultation with his or her advisor and approved by the GPD. After approval of the dissertation proposal, the chair of the dissertation committee shall recommend the student's admission to candidacy to the GPD and the Dean. Each student will complete at least 18 credit hours of dissertation research (CYSE 899: Doctoral Dissertation) during which major work will result in development of a doctoral dissertation that represents original research efforts by the student.

The dissertation may take the form of one major project, or three related research projects prepared for journal publication. Upon completion of the dissertation, the student's dissertation committee will conduct a public examination and defense of the dissertation. Final approval is the responsibility of the dissertation chair, the GPD, and ultimately the Dean of the Interdisciplinary Studies, who together certify the candidate for graduation.

Appendix A provides sample schedules for full-time and part-time students. Course descriptions may be found in Appendix B.

Student Retention and Continuation Plan

Pre-emptive approaches will be adopted to ensure students succeed in the proposed program. Specific plans for student retention and continuation include:

- Requiring an online orientation session for all new students, aimed at introducing the program, curriculum, requirements, expectations, faculty, facility, and other relevant resources that are online or remotely accessible through the myODU portal.
- Providing an up-to-date curriculum and a long-range course schedule to help students plan their enrollment and time to completion.
- Requiring a minimum of one advising session per semester (online or face-to-face) and providing personalized advising throughout students' program of study.
- Holding special advising sessions for nontraditional students (e.g., working professionals).
- Connecting students with the network of cybersecurity students in the Coastal Virginia Center for Cyber Innovation.
- Assigning each student a faculty mentor; and

When individual student performance demonstrates a lack of success, faculty will explore ways to encourage success. These include:

- Individualized advising and mentoring to help the student pass course(s).
- Connecting students to other PhD students who are willing to provide peer mentoring.
- Assigning additional faculty mentors.
- Involvement in state-of-the-art cybersecurity projects to stimulate student's interest to become motivated and excited to study cybersecurity; and
- Creating a cohort to increase interactions and peer learning.

Time to Degree

Full-time students who enter directly from a bachelor's degree program will be able to complete the program in five years while part-time students will be able to finish the program in eight years. Full-time students who enter from a master's degree program will be able to complete the program in three years while part-time students will be able to finish the program in six years.

Faculty

The School of Cybersecurity has 9 faculty with credentials to teach in a Doctor of Philosophy in Cybersecurity Program. An additional 10 faculty affiliated with the School are also credentialed and have the subject matter expertise to teach in a cybersecurity doctoral program. These affiliate faculty hold tenure or tenure-track positions in five colleges: College of Arts and Letters (Sociology and Criminal Justice; Philosophy and Religious Studies), Strome College of Business (Information Technology and Decision Science), Batten College of Engineering and Technology (Electrical and Computer Engineering; Engineering Management and Systems Engineering), College of Education and Professional Studies (Education Foundations and Leadership and Instructional Design and Technology), and College of Sciences (Computer Science; Psychology).

Among the nineteen faculty members, six will teach the core coursework, including 3 professors, one of whom serves as the director of the School of Cybersecurity, 1 associate professor, 1 assistant professor, and 1 senior lecturer.

The faculty have breadth and depth in areas of cybersecurity, ranging from software to hardware security and from fundamental cybersecurity technologies to human factors in cybersecurity. Combined, they have an extensive record of scholarship with over 200 recent publications (during the past three years) in peer-reviewed journals and conferences in cybersecurity fields. They currently have 25 active research grants from prestigious organizations such as the National Science Foundation, Department of Homeland Security, Department of Defense, National Security Agency, Air Force Research Laboratory, Army Research Office, Department of Energy, Small Business Administration, the Commonwealth Cyber Initiative (CCI), Circadence Corporation, Deloitte Consulting LLP, Frontier Technology Inc (FTI), and Booz Allen Hamilton.

Abbreviated CVs for existing full-time faculty members can be found in Appendix C.

Program Administration

This proposed program will be administered by the School of Cybersecurity. The School of Cybersecurity was established to weave together distinct threads of programmatic and facility resources to create a strong education and research program focusing on cybersecurity. While offering two degrees and housing sixteen faculty, the School represents an interdisciplinary effort related to faculty, degree programs, certificates, and research initiatives from five colleges, eight academic departments, the Office of Research, Information Technology Services, and the Virginia Modeling, Analysis and Simulation Center.

A tenured cybersecurity faculty will be appointed as the graduate program director (GPD). She or he will assume responsibility for setting class schedules, coordinating student meetings and activities, gathering student input, handling students' concerns, providing admission and enrollment information to the Graduate School, and meeting with the faculty, the School director, and vice provost of academic affairs to discuss programmatic matters.

A graduate committee, to include the graduate program director and other faculty members affiliated with the School of Cybersecurity, will be formed to review applicants for admission, evaluate curriculum in meeting student and employer needs, and conduct regular program assessments.

An administrative assistant in the School of Cybersecurity will support faculty and students in this program; approximately 20% of this individual's time will be devoted to the proposed program. The assistant will help with the processing of applications, scheduling of courses, handling registration issues, updating the catalog, and website management.

Student Assessment

Students will be evaluated throughout the program using formative assessments such as case studies, papers, research projects, and presentations. Student learning outcomes cover many of the professional and empirical competencies required of higher education professors and researchers. Specifically, graduates will be able to:

1. Analyze ethical and social issues in the area of cybersecurity and communicate the underlying implications of those issues to multiple audiences.
2. Conduct independent research on cybersecurity using multiple research methods.
3. Communicate in writing the results of their research for both scholarly and non-scholarly audiences.
4. Integrate principles and methods from a variety of disciplines to study cybersecurity.
5. Apply their interdisciplinary expertise through course instruction and scholarly research; and
6. Orally communicate their understanding of cybersecurity and explain decisions in cohesive and well-structured presentations to both technical and non-technical audience.

These student learning outcomes are provided in the following assessment map.

Curriculum Map of Cybersecurity Program Core Courses

Student Learning Objectives	Courses that Develop Competency Course Number and Title	Courses and Activities that Demonstrate Mastery Course Number and Title
1. Ethics Analyze ethical and social issues in the area of cybersecurity to and communication the underlying implications of those issues to multiple audiences;	CYSE 600. Cybersecurity Principles CYSE 603. Advanced Cybersecurity Law and Policy CYSE/ PHIL 803. Moral Reasoning for Emerging Technologies	CYSE 600 • 80% of students will analyze real-world cybersecurity cases using ethics theory and concepts from the fundamental cybersecurity principles introduced in the class. (Exam) CYSE 603 • 80% of students will successfully present and debate on alternative methods to accomplish ethics in the cybersecurity industry. (Presentation) CYSE/ PHIL 803 • 80% of students will successfully write delineate the way that new cyber technologies create ethical dilemmas for policy makers and businesses (Research paper)
2. **Independent Research** Conduct independent research on cybersecurity using multiple research methods.	CYSE 601. Advanced Cybersecurity Techniques and Operations CYSE 605. Leadership and Management in Cybersecurity CYSE 800. Research Methods in Cybersecurity	CYSE 601 • 80% of students will analyze security problems of a wireless network, produce a written report, and give an in-class presentation. (Research project) CYSE 605 • 80% of students will analyze security problems through a leadership lens, produce a written report, and give an in-class presentation (Research project) CYSE 800 • 80% of students will design and complete a multi-method cybersecurity study (Research paper)

3. Written Research Communicate in writing the results of their research for both scholarly and non-scholarly audiences;	CYSE 899 Doctoral Dissertation	CYSE 899 • 80% of students will successfully complete a dissertation project (either as one comprehensive study or three journal articles)
4. Integrated Perspective Integrate principles and methods from a variety of disciplines to study cybersecurity;	CYSE 802 Cybersecurity Seminar CYSE 801 Advanced Cybersecurity Techniques and Operations II	CYSE 802 • 90% of students will develop a cybersecurity research proposal that integrates ideas from at least three disciplines (Research proposal) CYSE 801 • 90% of students will complete a cybersecurity diagnosis and be able to explain how the diagnosis would be explained through multidisciplinary frameworks.
5. Instruction and Research Apply interdisciplinary expertise through course instruction and scholarly research;	CYSE 802 Cybersecurity Seminar CYSE 868 Cybersecurity Practicum	CYSE 802 • 90% of students will develop a cybersecurity lecture and research proposal and present to the class. (Presentation) CYSE 868 • 90% of students will successfully teach a cybersecurity class or work in a cybersecurity research laboratory.
6. Oral Communication Orally communicate cybersecurity research through well-structured presentations to both technical and non-technical audience.	CYSE 802 Cybersecurity Seminar CYSE 899 Doctoral Dissertation	CYSE 802 • 90% of students will develop a cybersecurity lecture and research proposal and present to the class. (Presentation) CYSE 899 • 80% of students will successfully complete their dissertation defense.

Employment Skills/Workplace Competencies

Graduates of the proposed Doctor of Philosophy program in Cybersecurity will have the skills and abilities needed for employment and workplace competencies to work in higher education and in industry.

As faculty members, graduates will be able to:

1. Develop and deliver effective cybersecurity instruction in an undergraduate or graduate college or university program.
2. Conduct cybersecurity research studies independently and in collaboration with other scholars.
3. Advise and mentor cybersecurity students.
4. Serve as professional consultants and advisors to government and industry bodies seeking guidance.
5. Expand scientific knowledge about cybersecurity through multiple disciplinary frameworks.

As a cybersecurity researcher working in industry or government settings, graduates will be able to:

1. Develop original research projects focused on cybersecurity.
2. Secure funding for cybersecurity research projects.
3. Translate cybersecurity research findings into practice.
4. Effectively communicate with various audiences about cybersecurity research findings.
5. Provide technical leadership in cybersecurity settings.

Program Assessment

The program will be assessed by faculty and administrators in the School of Cybersecurity and the provost's office. The review will be completed annually in the fall starting from the second year after the program is approved, and will consist of:

- Analyzing retention and attrition rates in order to maximize the positive influences and improve the negative ones that affect program completion.
- Analyzing the results of the Old Dominion University Graduate Student Satisfaction Survey for areas where additional student support is needed.
- Analyzing graduate job placement to assess if the program is preparing students with the knowledge, skills, and abilities for jobs in cybersecurity and evaluate the program's ability to meet market demands (following initial graduates' completion)

Results of these assessments will be used to evaluate the quality of the program, to stimulate program development, and to assess the role of the program in fulfilling Old Dominion University's institutional mission. The program review may (a) result in strategic decisions about the program, (b) identify areas of improvement, (c) make resource recommendations, (d) articulate considerations for expansion or consolidation, and/or (e) consider other aspects of programmatic quality with respect to policies and practices relative to:

- Student recruitment, admissions, advising, and retention.
- Enrollment projections including consideration of the context of the SCHEV 5-year benchmark and other on-going enrollment targets.
- Course descriptions and implementation.
- Approved curricular changes and development.
- Faculty development and research activities.
- Facilities.
- Internal and external funding; and
- Description of strengths and weaknesses with attention to action items for the future.

The dean and associate dean in the Graduate School will read the program review each year to ensure that benchmarks are met and excellence is maintained. The Graduate School's annual evaluation of the program will be sent each year to the vice provost for review. The vice provost will offer guidance, as needed, for improvement, and will provide updates about the review to the provost.

Benchmarks of Success

Benchmarks of success for the Doctor of Philosophy in Cybersecurity include the following student enrollment and graduate goals:

- 10-12 new students will be admitted each year.
- The program will graduate a minimum of 8 students annually by the completion of the program's target year.
- 80% of the students who begin the program will successfully complete the program within five years of matriculation.
- 80% of graduates will be employed in cybersecurity positions using knowledge acquired in their graduate studies within six months of completion.
- 80% of students will be satisfied with the program as determined by the university's Graduate Student Satisfaction Survey
- 80% of alumni will be satisfied with the program as determined by the university's Graduate Alumni Survey, administered within one year of completion.

After the first year and subsequent years, periodic evaluations of the success of the program in meeting these benchmarks will be undertaken. If program benchmarks are not achieved, the graduate program director and the program faculty will examine the program's admissions policies, curriculum, instructional methods, advising practices, and course evaluations to determine where changes need to be made.

Expansion of an Existing Program

This program is not an expansion of an existing certificate, concentration, emphasis, focus, major, minor, or track at ODU.

Relationship to Existing ODU Degree Programs

There are no similar or related Old Dominion University programs at the doctoral level in the area of this proposed program.

Compromising Existing Programs

No degree programs will be compromised or closed as a result of the initiation and operation of the proposed degree program.

Collaboration or Standalone

This is a standalone program. No other organization was involved in its development, and no other organization will collaborate in its operation.

Justification for the Proposed Program

Response to Current Needs (Specific Demand)

Cybersecurity is a rapidly growing field that is expected to generate a significant number of new jobs over the next decade, as both government and industry make substantial investments to protect their cyber space. With the increasing reliance on computer systems and networks, more pervasive, sophisticated, and destructive cyber attacks are occurring with greater frequency. In fact, no organization or individual anywhere in the world is completely immune to cyber attacks. While institutions have made progress in developing programs for undergraduate and Master's students, the presence of cybersecurity doctoral programs has lagged behind.

Cybersecurity Job Vacancies and Higher Education

Scholars, policy makers, businesses, and others have highlighted to high number of job openings in cybersecurity. Reports suggest that there are 714,000 cybersecurity job openings in the United States[10] and 3.5 million vacancies across the world.[11] Few would argue with the data suggesting a high demand for cybersecurity workers. The high demand has resulted in the development of cybersecurity curricula in academic programs across the world. A cursory review of the programs suggests that the new programs have been designed to prepare workers for the

[10] Cyberseek.org. (2022). Cybersecurity career map. Available online.
[11] Morgan, S. (2021). Cybersecurity jobs report. Available online at https://cybersecurityventures.com/jobs/.

industrial and governmental workforce. The new curricula have primarily been for associate's, Bachelor's, and Master's degrees. To date, the development of cybersecurity PhD programs has lagged behind in the United States. This is somewhat ironic given that educators will be needed for the growing number of academic cybersecurity programs. Indeed, researchers have made observations such as, "The cybersecurity workforce needs additional skilled personnel, from the technician to the cybersecurity leader *to the teacher"*[12] and "Cybersecurity is a fast-growing field, and there has been a large and increasing demand for cybersecurity experts, leaders and *college faculty with advanced education preferably at the doctoral level*."[13] (emphasis added).

To date, cybersecurity doctoral programs in the United States tend to be professional doctoral programs in cybersecurity (D.SCI) or concentrations within other disciplinary PhD programs. While very few cybersecurity doctoral programs have been created in the United States, scholars have drawn attention to the need for doctoral training in cybersecurity. Justifications for PhD program in cybersecurity include (1) addressing workforce demand in industry and government, (2) building bridges between higher education and industry, (3) responding to higher education and cybersecurity professionals' interest, (4) adhering to accreditation requirements, (5) advancing cybersecurity research, (6) strengthening cybersecurity as a discipline, and (7) embracing the interdisciplinary foundations of cybersecurity.

Regarding the development of curricula to help address workforce demand, conversations typically focus on how academic programs are needed to develop the cybersecurity talent pipeline for the hundreds of thousands of job vacancies. Often missing from these conversations is the fact that higher education also has a workforce gap when it comes to cybersecurity professors. Indeed, some scholars have concluded that "To help educate future cybersecurity students, a strong cybersecurity Ph.D. program is needed."[14] A review of technology-related doctoral programs by another author led the authors to conclude that "The challenge of meeting the cybersecurity workforce shortage through degree programs is intensified by the reality of the limited number of cybersecurity and engineering faculty at colleges and universities."[15] Another author noted that "as universities launch [cybersecurity] programs, they may be doing so with no terminal degree faculty in cybersecurity."[16] This point is emphasized by Andrew Hall and his colleagues who wrote the following about the development of new cybersecurity programs:

---

[12] Hall, A., Liu, X. M., & Murphy, D. (2021, October). Integrating Andragogy Theory into a Multidisciplinary Curriculum to Achieve a Connected Program for a Doctorate in Cybersecurity. In *2021 IEEE Frontiers in Education Conference (FIE)* (pp. 1-8). IEEE.

[13] Wang, P., & Kohun, F. (2019). Designing a doctoral program in cybersecurity for working professionals. *Issues in Information Systems*, *20*(1).

[14] Ahmad, N., Laplante, P., Defranco, J., & Kassab, M. H. (2021). A Cybersecurity Educated Community. IEEE Transactions on Emerging Topics in Computing.

[15] Burrell, D. N., Dawson, M. E., & Nobles, C. (2020). Innovative doctorate programs in cybersecurity, engineering, and technology in the USA and UK that can be completed by professionals around the world without relocation. In ICRMAT (pp. 1-3).

[16] Dawson, M. (2020). National cybersecurity education: bridging defense to offense. Land Forces Academy Review, 25(1), 68-75.

> In many cases, emergent cybersecurity academic programs relied on these practitioners as adjunct faculty to transfer and impart knowledge to students. However, this approach proved insufficient to develop an overall academic discipline of cybersecurity with effective educational programs to meet the growing and changing need for cybersecurity professionals.[17]

Cybersecurity doctoral programs have also been justified on the belief that such programs could build bridges between industry and higher education. From this perspective, the pool of possible doctoral students would include cybersecurity professionals who use their cybersecurity knowledge, skills, and abilities as a foundation for subsequent doctoral training. Such training, coupled with industry experience, could result in "scholarly practitioners." Here is how one group of authors describes this possibility:

> When a cybersecurity professional could have come from any of variety of undergraduate programs, and many had earned master's degrees before cybersecurity was recognized as a discipline, the signal of expertise from a terminal degree (doctorate) in cybersecurity is an intriguing opportunity. From the perspective of academia, the opportunity to create scholarly practitioners, prepared to educate, train, and mentor our students while serving as the next generation of guild masters, is equally attractive. Creating scholarly practitioners is our best chance to bootstrap the experience from within the community of practice and finally address the higher levels of the workforce.[18]

A related justification for the development of PhD programming has to do with the demand for such programming from both higher education and cybersecurity professionals. Higher education professionals recognize the need for cybersecurity doctoral programming to prepare cybersecurity college students for the workforce.[19] [20] According to Wang and Kohun, in 2019, there were more than "300 unfilled Cybersecurity-related college and university faculty positions that require or prefer a relevant doctorate degree." Regarding demand from professionals, a survey of 237 cybersecurity and information technology professionals by the same authors found "that 83.54% of the respondents have an expressed interest in pursuing a Ph.D. degree in Cybersecurity in the near future."[21]

---

[17] Hall, A., Liu, X. M., & Murphy, D. (2023, October). Advancing Cybersecurity Through Knowledge Conversion: Industry-Academia Interchange in a Doctoral Program. In *2023 IEEE Frontiers in Education Conference (FIE)* (pp. 1-4). IEEE.

[18] Hall, A., Liu, X. M., & Murphy, D. (2021, October). Integrating Andragogy Theory into a Multidisciplinary Curriculum to Achieve a Connected Program for a Doctorate in Cybersecurity. In 2021 IEEE Frontiers in Education Conference (FIE) (pp. 1-8). IEEE. (Hall et al., p. 2)

[19] Ahmad, N., Laplante, P., Defranco, J., & Kassab, M. H. (2021). A Cybersecurity Educated Community. IEEE Transactions on Emerging Topics in Computing.

[20] Wang, P., & Kohun, F. (2019). Designing a doctoral program in cybersecurity for working professionals. *Issues in Information Systems*, *20*(1).

[21] Wang, P., & Kohun, F. (2019). Designing a doctoral program in cybersecurity for working professionals. *Issues in Information Systems*, *20*(1).

Cybersecurity doctoral programs are also needed to address accreditation requirements, particularly those of regional accreditors. For example, regional accreditors typically require that university faculty hold terminal degrees in their teaching discipline. As a newer discipline, cybersecurity programs have been able to justify the credentials of those teaching their courses by hiring computer scientists, engineers, or others from related fields. As the discipline grows, it is plausible that accreditors will come to expect more cybersecurity faculty with terminal degrees in cybersecurity.

The growth of cybersecurity research is another justification for PhD programs in cybersecurity. In effect, doctoral programs foster research in disciplinary areas. As one author team points out, "[Cybersecurity] PhD candidates will advance the state of the art in cybersecurity research."[22]Another author teams concurs observing, "there are growing and abundant needs and opportunities for advanced research for doctoral programs and students in Cybersecurity."[23] While cybersecurity research has grown over the years, much of the research is conducted through specific disciplinary lenses.

In a related way, the discipline of cybersecurity will become stronger through the development of doctoral programs, particularly PhD programs, in the field. The strength of any discipline can be directly connected to the number of doctoral graduates. Consider that program rankings are typically connected to the number of graduates from those programs. In a similar way, disciplines are stronger when their number of graduates is balanced with the number of careers in those disciplines. In addition, having more doctoral students translates into more research on a specific topic. A study in Canada, in fact, found that doctoral students in Quebec accounted for nearly a third of all research conducted in that province over a seven-year timeframe.[24] While that study focused on all disciplines, the conclusion is obvious – absent expanded cybersecurity doctoral programming, growth in cybersecurity is potentially stinted.

A final justification for creating PhD programs in cybersecurity has to do with the interdisciplinary foundation of cybersecurity. In recent years, cybersecurity education experts have increasingly drawn attention to the interdisciplinary underpinnings of the cybersecurity field.[25] While it is clear that cybersecurity, by its nature, is interdisciplinary, the vast majority of cybersecurity education programs are housed within singular disciplines such as computer engineering, computer science, or information technology. The results can be problematic given that for some careers an interdisciplinary understanding of cybersecurity is "required in order to

[22] Callen, J., & James, J. E. (2020). Cybersecurity engineering: The growing need. Issues in Information Systems, 21(4).
[23] Wang, P., & Kohun, F. (2019). Designing a doctoral program in cybersecurity for working professionals. *Issues in Information Systems*, *20*(1).
[24] Larivière, V. (2012). On the shoulders of students? The contribution of PhD students to the advancement of knowledge. *Scientometrics*, *90*(2), 463-481.
[25] Greitzer, F.L., and Frincke, D. (2010). Combining traditional cyber security audit data with psychosocial data: towards predictive modeling for insider threat mitigation. In *Insider Threats in Cyber Security*, pp. 85-113. New York: Springer.

obtain the right skills in the field."[26] Another team noted that while disciplinary degrees were appropriate for some cybersecurity careers, interdisciplinary approaches were preferable for some occupations.[27] When cybersecurity doctoral training is embedded in existing disciplinary PhD programs, those programs are justifiably driven by the tenets of the broader discipline. Cybersecurity scholars increasingly recognize the interdisciplinary foundation of the discipline. The benefit of creating new PhD programs is that they can be developed on interdisciplinary foundations.

Interdisciplinary cybersecurity programs are justified on several practical grounds including: (1) Such programs focus on solving a real-world problem from a holistic perspective; (2) The complex nature of cybersecurity makes it virtually impossible for one discipline to "claim ownership" over the topic; (3) Some careers that have recently been created, and some that will be developed in the future, will require an interdisciplinary understanding of cybersecurity; and (4) It is plausible that interdisciplinary programs will increase the number of women and minorities in cybersecurity programs.

Despite these advantages, barriers make it difficult to implement interdisciplinary cybersecurity programs. These barriers include faculty resistance, disciplinary silos, as well as structural and other features of universities. A handful of universities such as Old Dominion University have overcome these barriers and developed interdisciplinary cybersecurity programming. As noted above, most of these programs have been developed as BS or MS programs and very few doctoral programs have been created.

Employment Demand

National Focus

The demand for cybersecurity professors is growing across the nation. As an example, the National Science Foundation recently changed its Scholarship for Service program to meet the demand for cybersecurity professors. The SFS program offers students stipends and tuition scholarships in exchange for commitment to work for the federal government for a select period of time. In 2023, the government agreed to allow employment in certain higher education cybersecurity programs to count towards the SFS graduate's service expectations. Data showing the national growth in cybersecurity enrollments bolster the need for doctoral-trained graduates in cybersecurity. Consider, for example, the following:

- The number of students enrolled in cybersecurity bachelor's degree programs more than doubled between 2018 and 2022, increasing from less than 25,000 to nearly 50,000 students across the U.S.
- The number of graduates of cybersecurity degree programs increased from 10,013 to 23,476 between 2016 and 2022.

[26] LeClair, J., Abraham, S., & Lifang, S. (2013). An interdisciplinary approach to educating an effective cyber security workforce. In *Proceedings of the 2013 on InfoSecCD'13: Information Security Curriculum Development Conference*, p. 71. ACM, 2013.

[27] McDuffie, E., & Piotrowski, V. (2014). The future of cybersecurity education. *Computer* 47, no. 8: 67-69.

- Cybersecurity annual enrollment increases were 15 percent between 2018 and 2022.[28]

The number of new academic programs also increased over recent years. In 1999, seven institutions were designated as National Centers of Academic Excellence in cybersecurity education. Today, more than 400 institutions hold that designation.[29] Despite this growth in enrollment and academic programming, the development of doctoral programs in cybersecurity has not kept pace. In fact, there are just four cybersecurity doctoral programs in the United States. These include the following:

- Northeastern University, an institution with an NSA Center of Academic Excellence in Research, offers a PhD in Cybersecurity. The program is available on-campus.
- Marymount University, an institution with an NSA Center of Academic Excellence in Cyber Defense, offers a Doctor of Science in Cybersecurity. The program is available online and on-campus.
- NOVA Southeastern University, an institution with an NSA Center of Academic Excellence in Cyber Defense, offers a PhD in Cybersecurity Management. The program is available online and on-campus.
- Purdue University, an institution with an NSA Center of Academic Excellence in Research, offers an interdisciplinary PhD in Information Security. The program is available online on-campus.

Some institutions offer cybersecurity concentrations within existing doctoral programs. While filling a need, the absence of programs specifically in cybersecurity keeps the field from moving forward and keeping pace with enrollment and job demand growth.

Virginia Focus

Cybersecurity higher education programs have increased rapidly in the Commonwealth of Virginia. Tables 1 and 2 show enrollments in associate's and bachelor's degree programs in 2017, 2020, and 2023. The trends are striking. The number of students enrolled in Bachelor's degree programs increased tenfold between 2017 and 2023 and the number of associate's degree students more than doubled.

Table 1 Enrollment in Cybersecurity Bachelor's Degree Programs in Virginia, 2017, 2020, 2023

	Fall 2017	Fall 2020	Fall 2023
Computer and Information Systems Security/Auditing/Information Assurance. (11.1003)	244	1087	2594
Cyber/Computer Forensics and Counterterrorism. (43.0403)	35	54	137
Cyber/Electronic Operations and Warfare (29.0207)		29	31
Cybersecurity Defense Strategy/Policy. (43.0404)		191	251
Total	279	1361	3013

[28] Rowles, E. (2023). When Bad News is Good News: Cyber Breaches Drive Demand for Cybersecurity Programs. Available online at https://www.graydi.us/blog/graydata/when-bad-news-is-good-news-cyber-breaches-drive-demand-for-cybersecurity-programs

[29] What is a CAE in cybersecurity. (2023). Available online at https://www.caecommunity.org/about-us/what-cae-cybersecurity.

Table 2 Enrollment in Cybersecurity Associate's Degree Programs in Virginia, 2017, 2020, 2023

	Fall 2017	Fall 2020	Fall 2023
Computer and Information Systems Security/Auditing/Information Assurance. (11.1003)	1280	2499	3363

Tables 3 and 4 show the job demand nationally and in Virginia for BS degrees and MS degrees related to cybersecurity. As indicated previously, the Commonwealth of Virginia has more cybersecurity job vacancies than any other state in the United States.

Table 3. Labor Market Information: Bureau of Labor Statistics, 2022 -2032 (10-Yr)

Occupation	Base Year Employment	Projected Employment	Total % Change and #s	Typical Entry Level Education
Information Security Analysts[30]	168,900	222,100	32% (53,200)	BS
Computer and Information Research Scientists[31]	36,500	44,800	23% (8,300)	MS

Table 4. Labor Market Information: Virginia Employment Commission, 2020-2030

Occupation	Base Year Employment	Projected Employment	Total % Change and #s	Annual Change #	Education
Information Security Analysts[32]	16,340	22,360	37% (5,980)	1,970	BS
Digital Forensics Analysts[33]	17,130	19,620	15% (2,490)	1,580	BS
Computer and Information Research Scientists[34]	3,760	4,320	13% (560)	320	MS

Job announcements are included in Appendix D.

[30] https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm
[31] https://www.bls.gov/ooh/computer-and-information-technology/computer-and-information-research-scientists.htm
[32] https://www.onetonline.org/link/summary/15-1212.00
[33] https://www.onetonline.org/link/localtrends/15-1299.06?st=VA
[34] https://www.onetonline.org/link/localtrends/15-1221.00?st=VA

Student Demand

Student demand for a PhD level program in cybersecurity is strong, as evidenced by three sets of data, as follows.

1. Enrollments in cybersecurity undergraduate and graduate programs, providing a pool of prospective graduate students in this program. Specifically, the Office of Institutional Research at ODU reports those enrollments—in cybersecurity, cybercrime, and enterprise cybersecurity majors—as follows:

Fall 2015	11
Fall 2016	69
Fall 2017	131
Fall 2018	370
Fall 2019	608
Fall 2020	843
Fall 2021	964
Fall 2022	1251
Fall 2023	1451

2. Results of a survey sent to undergraduate (junior and seniors) and graduate (master's) cybersecurity students at ODU. The survey was conducted February 19 to February 23, 2024. A total of 77 individuals responded to the survey about the proposed PhD in Cybersecurity. A large number of students reported being extremely interested (38), very interested (15), or interested (18) in the proposed program. When asked whether they would enroll in the proposed program at ODU, 71 students said they were somewhat likely (11), likely (13), very likely (22), or definitely (27) applying to the proposed program.

3. Unsolicited emails received from students inquiring about the availability of a PhD program in cybersecurity.

Student survey results are in Appendix E. The unsolicited emails may be found in Appendix F.

STATE COUNCIL OF HIGHER EDUCATION FOR VIRGINIA
SUMMARY OF PROJECTED ENROLLMENTS IN PROPOSED PROGRAM

Projected enrollment:

Year 1		Year 2		Year 3		Year 4 **Target Year (2-year institutions)**			Year 5 **Target Year (4-year institutions)**		
2025 - 2026		2026 - 2027		2027 - 2028		2028 - 2029			2029 - 2030		
HDCT	FTES	HDCT	FTES	HDCT	FTES	HDCT	FTES	GRAD	HDCT	FTES	GRAD
12	9	24	18	36	27	48	36		60	45	8

Assumptions
Retention: 90%
Part-time students: 25% / Full-time students: 75%
Full-time students credit hours per semester: 9
Part-time students credit hours per semester: 6
Full-time students graduate in 5 years
Part-time students graduate in 8 years

Duplication

No public institution in the Commonwealth of Virginia offers a PhD in Cybersecurity.

Projected Resource Needs for the Proposed Program

Resource Needs

Old Dominion University and the School of Cybersecurity have sufficient resources to launch and sustain the proposed program. Specifically, faculty, staff, equipment, space, and library resources are available to launch and maintain the proposed program. The proposed program will allocate 1.0 FTE of instructional effort for every 9.0 FTE of enrollment. During the 2025-2026, academic year when the program is launched, a total of .9 FTE of instructional effort will be required, and it will rise to 4.5 FTE by the target year, 2030-2031.

The provost has committed to adding four new cybersecurity faculty with appointments in affiliated departments between program initiation and the first three years of the program.

Full-Time Faculty
The Director of the School of Cybersecurity will teach in the program, in addition to serving as the program director. His instructional efforts will be 50% of his teaching load through the target years; thus, he is considered full time, at .5 FTE. In year 2, An additional cybersecurity faculty member will contribute 50% of effort to the proposed program, providing .5 FTE through the

target year. In year 3, a third cybersecurity faculty member will provide 50% of effort to the proposed program, providing .5 FTE through the target year. In year 4, a fourth cybersecurity faculty member will contribute 50% of effort to the proposed program, providing .5 FTE through the target year.

Full-time faculty from the School of Cybersecurity will contribute .5 FTE effort in the initiation year and 2.0 FTE effort by the target year, 2030-2031.

Part-Time Faculty

Ten additional faculty members at the university, who are affiliated with the School of Cybersecurity, will teach part-time loads in the proposed program. Combined, they will account for .4 FTE faculty when the program is launched. By the target year, the combined part-time faculty members will account for 2.5 FTE faculty.

In years one and two, one faculty member from the Department of Computer Science will contribute .2 FTE to the proposed program. In year three and four, two (2) computer science faculty will each contribute .2 FTE to the proposed program, for a total of .4 FTE. In the target year, two computer science faculty will contribute .25 FTE to the program, for a total of .5 FTE. In the initiation year, computer science will contribute .2 FTE to the proposed program, increasing to .5 FTE by the target year.

In years one and two, one faculty member from the Department of Electrical and Computer Engineering will contribute .2 FTE to the proposed program. In year three and four, two (2) computer engineering faculty will each contribute .2 FTE to the proposed program, for a total of .4 FTE. In the target year, two computer engineering faculty will contribute .25 FTE to the program, for a total of .5 FTE. In the initiation year, computer engineering will contribute .2 FTE to the proposed program, increasing to .5 FTE by the target year.

In year two, one faculty member from the Department Philosophy and Religious Studies will contribute .2 FTE to the proposed program. In year three and four, two (2) philosophy faculty will each contribute .2 FTE to the proposed program, for a total of .4 FTE. In the target year, two philosophy faculty will contribute .25 FTE to the program, for a total of .5 FTE. In the initiation year, philosophy faculty will contribute .2 FTE to the proposed program, increasing to .5 FTE by the target year.

In year two, one faculty member from the Department of Information Technology and Decision Sciences will contribute .2 FTE to the proposed program. In year three and four, two (2) information technology faculty will each contribute .2 FTE to the proposed program, for a total of .4 FTE. In the target year, two information technology faculty will contribute .25 FTE to the program, for a total of .5 FTE. In the initiation year, information technology faculty will contribute .2 FTE to the proposed program, increasing to .5 FTE by the target year.

Beginning in the target year, one faculty member from the Department of Engineering Management and Systems Engineering will contribute .1 FTE to the proposed program.

Beginning in the target year, one faculty member from the Department of English will contribute .1 FTE to the proposed program.

Beginning in the target year, one faculty member from the Department of Psychology will contribute .1 FTE to the proposed program.

Beginning in the target year, one faculty member from the Instructional Technology and Design program will contribute .1 FTE to the proposed program.

Adjunct Faculty
No adjunct faculty members are required to launch and sustain the proposed program.

Graduate Assistants
Four graduate assistants will be required to initiate the program. Each year, an additional four graduate students will be added through year 5 when 20 graduate assistants will be needed. The cost for the graduate assistants will be covered by the Coastal Virginia Center for Cyber Innovation. Each graduate assistant will be paid a stipend of $25,000, for a total of $500,000 during the target year.

Classified Positions
A classified person—administrative assistant—who supports the School of Cybersecurity will assist with this proposed program. This person will devote approximately .20 FTE to the program, or $7,500 in salary and $2,783 in fringe benefits.

Targeted Financial Aid
No targeted financial aid is required to launch and sustain the proposed program.

Library
No new library resources are required to launch and sustain the proposed program. The University Libraries have adequate resources to support this program, including journals such as IEEE Security & Privacy, IEEE Transactions on Information Forensics and Security, and IEEE Transactions on Dependable and Secure Computing through the online IEEExplore database. In addition, the ODU Libraries have additional resources, including open access titles, that are easily discoverable and accessible via the Libraries' tools.

Telecommunications
No new telecommunication equipment or software is needed to launch or sustain the proposed program.

Equipment (including computers)
No new equipment or related resources are needed to initiate and sustain this proposed program.

Space
No additional space is needed to initiate and sustain this proposed program.

Other Resources (specify)

No new resources will be required to launch or operate the proposed Doctor of Philosophy in Cybersecurity.

Funds to Initiate and Operate the Degree Program

Figures provided in the table below will be compared to SCHEV funding estimates using the current base adequacy model. This comparison will serve as a reference for the estimated costs. If there are large discrepancies, SCHEV may request additional clarification to ensure the institution's assumptions are correct, or require modifications as a condition of approval.

Note: Institutions must use the recommended student-faculty ratio when estimating FTE enrollments and required faculty FTEs.

Cost and Funding Sources to Initiate and Operate the Program			
Informational Category		**Program Initiation Year 2025 - 2026**	**Program Full Enrollment Year[1] 2030 - 2031**
1.	Projected Enrollment (Headcount)	12	60
2.	Projected Enrollment (FTE)	9	45
3.	Projected Enrollment Headcount of In-State Students	6	30
4.	Projected Enrollment Headcount of Out-of-State Students	6	30
5.	Estimated Annual Tuition and E&G Fees for In-state Students in the Proposed Program	$12,262	$13,793
6.	Estimated Annual Tuition and E&G Fees for Out-of-State Students in the Proposed Program	$32,662	$37,465
7.	Projected Total Revenue from Tuition and E&G Fees Due to the Proposed Program	$269,544	$1,537,740
8.	Other Funding Sources Dedicated to the Proposed Program (e.g., grant, business entity, private sources)	$500,000	$1,000,000

[1] For the "Full Enrollment Year" use: for associate degrees, initiation year plus 1; for baccalaureate degrees, initiation plus 3; for masters degrees, initiation plus 2; for doctoral degrees, initiation plus 3.

Resource Needs

Answer the following questions about general budget information.

• Has or will the institution submit an addendum budget request to cover one-time costs?	Yes		No	X
• Has or will the institution submit an addendum budget request to cover operating costs?	Yes		No	X
• Will there be any operating budget requests for this program that would exceed normal operating budget guidelines (for example, unusual faculty mix, faculty salaries, or resources)?	Yes		No	X
• Will each type of space for the proposed program be within projected guidelines?	Yes	X	No	
• Will a capital outlay request in support of this program be forthcoming?	Yes		No	X

Certification Statement(s)

The institution will require additional state funding to initiate and sustain this program.

_____ Yes _____
Signature of Chief Academic Officer

__X__ No _____
Signature of Chief Academic Officer

If "no," please complete Items 1, 2, and 3 below.

1. Estimated $$ and funding source to initiate and operate the program.

Funding Source	Program initiation year 2025 – 2026	Target enrollment year 2028 - 2029
Reallocation within the department *(Note below the impact this will have within the department.)*		
Reallocation within the school or college *(Note below the impact this will have within the school or college.)*	$100,000	$500,000
Reallocation within the institution *(Note below the impact this will have within the institution.)*		
Other funding sources *(Specify and note if these are currently available or anticipated.)*		

2. Statement of Impact/Other Funding Sources.

Reallocation within the School:
Funds used to support internal grants in the Coastal Virginia Center for Cyber Innovation will be reallocated to support graduate research assistants. Given that the doctoral students will be supporting faculty with research projects, there will be negligible impact from this reallocation. The only impact is the amount available for internal research grants will be reduced.

3. Secondary Certification.

If resources are reallocated from another unit to support this proposal, the institution will **not** subsequently request additional state funding to restore those resources for their original purpose.

X Agree _____

Signature of Chief Academic Officer

_____ Disagree _____

Signature of Chief Academic Officer

APPENDICES

APPENDIX A
PLAN OF STUDY

Sample Plan of Study for Full-Time Students from BS program

Course	Credits	Category
Fall I		
CYSE 600 Cybersecurity Principles	3	Core
Restricted Foundational Elective	3	Elective
CYSE 603 Advanced Cybersecurity Law and Policy	3	Core
TOTAL 9 credits		
Spring I		
CYSE 601 Advanced Cybersecurity Techniques and Operations	3	Core
CYSE 605 Leadership and Management in Cybersecurity	3	Core
Restricted Foundational Elective	3	Elective
TOTAL 9 credits		
Summer I		
Restricted Foundational Elective	3	Elective
TOTAL 3 credits		
Fall II		
CYSE 616 Cyber Defense Fundamentals	3	Core
CYSE 800 Research Methods in Cybersecurity	3	Elective
Restricted Foundational Elective	3	Elective
TOTAL 9 credits		
Spring II		
CYSE 802 Cybersecurity Seminar	3	Core
CYSE/ PHIL 803 Moral Reasoning for Emerging Technologies	3	Core
Restricted Foundational Elective	3	Elective
TOTAL 9 credits		
Summer II		
Advanced Elective	3	Elective
TOTAL 3 credits		
Fall III		
CYSE 801 Advanced Cybersecurity Techniques and Operations II	3	Core
Advanced Elective	3	Elective
Advanced Elective	3	Elective
Total 9 credits		
Spring III		
Advanced Elective	3	Elective
CYSE 868 Cybersecurity Practicum	3	Core
Advanced Elective	3	Elective
Total 9 credits		
Summer III		
CYSE 899 Doctoral Dissertation	1	Dissertation

Total 1 Credit		
Fall IV		
CYSE 899 Doctoral Dissertation	4	Dissertation
Total 4 Credit		
Spring IV		
CYSE 899 Doctoral Dissertation	4	Dissertation
Total 4 Credit		
Summer IV		
CYSE 899 Doctoral Dissertation	1	Dissertation
Total 1 Credit		
Fall V		
CYSE 899 Doctoral Dissertation	4	Dissertation
Total 4 Credit		
Spring V		
CYSE 899 Doctoral Dissertation	4	Dissertation
Total 4 Credits		

Total Required for Degree—78 credits

Sample Plan of Study for Part-Time Students from BS Program

Course	Credits	Category
Fall I		
CYSE 600 Cybersecurity Principles	3	Core
CYSE 603 Advanced Cybersecurity Law and Policy	3	Core
TOTAL 6 credits		
Spring I		
CYSE 601 Advanced Cybersecurity Techniques and Operations	3	Core
Restricted Foundational Elective	3	Elective
TOTAL 6 credits		
Fall II		
CYSE 605 Leadership and Management in Cybersecurity	3	Core
Restricted Foundational Elective	3	Elective
TOTAL 6 credits		
Spring II		
Restricted Foundational Elective	3	Elective
Restricted Foundational Elective	3	Elective
TOTAL 6 credits		
Fall III		
CYSE 616 Cyber Defense Fundamentals	3	Capstone
Restricted Foundational Elective	3	Elective
TOTAL 6 credits		
Spring III		
CYSE/ PHIL 803 Moral Reasoning for Emerging Technologies	3	Core

CYSE 800 Research Methods in Cybersecurity	3	Core
TOTAL 6 credits		
Fall IV		
CYSE 801 Advanced Cybersecurity Techniques and Operations II	3	Core
Advanced Elective	3	Elective
TOTAL 6 credits		
Spring IV		
CYSE 802 Cybersecurity Seminar	3	Core
Advanced Elective	3	Elective
TOTAL 6 credits		
Fall V		
Advanced Elective	3	Elective
Advanced Elective	3	Elective
TOTAL 6 credits		
Spring V		
CYSE 868 Cybersecurity Practicum	3	Core
Advanced Elective	3	Elective
TOTAL 6 credits		
Fall VI		
CYSE 899 Doctoral Dissertation	3	Dissertation
TOTAL 3 credits		
Spring VI		
CYSE 899 Doctoral Dissertation	3	Dissertation
TOTAL 3 credits		
Fall VII		
CYSE 899 Doctoral Dissertation	3	Dissertation
TOTAL 3 credits		
Spring VII		
CYSE 899 Doctoral Dissertation	3	Dissertation
TOTAL 3 credits		
Fall VIII		
CYSE 899 Doctoral Dissertation	3	Dissertation
TOTAL 3 credits		
Spring VIII		
CYSE 899 Doctoral Dissertation	3	Dissertation
Total 3 credits		

Total Required for Degree—78 credits

Sample Course Plan for Full-Time Students who are Admitted with an MS

Fall I		
CYSE 801 Advanced Cybersecurity Techniques and Operations	3	Core
CYSE 800 Research Methods in Cybersecurity	3	Core
Advanced Elective	3	Elective
TOTAL 9 credits		
Spring I		
CYSE 802 Cybersecurity Seminar	3	Core
CYSE/ PHIL 803 Moral Reasoning for Emerging Technologies	3	Core
Advanced Elective	3	Elective
TOTAL 9 credits		
Summer I		
CYSE 899 Doctoral Dissertation	1	Dissertation
TOTAL 1 credits		
Fall II		
CYSE 868 Cybersecurity Practicum	3	Core
Advanced Elective	3	Elective
Advanced Elective	3	Elective
Total 9 credits		
Spring II		
Advanced Elective	3	Elective
CYSE 899 Doctoral Dissertation	6	Dissertation
Total 9 credits		
Summer II		
CYSE 899 Doctoral Dissertation	1	Dissertation
Total 1 Credit		
Fall III		
CYSE 899 Doctoral Dissertation	2	Dissertation
Total 2 Credit		
Spring III		
CYSE 899 Doctoral Dissertation	1	Dissertation
Total 2 Credit		
Summer III		
CYSE 899 Doctoral Dissertation	1	Dissertation
Total 1 Credit		
Fall IV	2	Dissertation
CYSE 899 Doctoral Dissertation		
Total 2 Credit		
Spring IV	1	Dissertation
CYSE 899 Doctoral Dissertation		
Total 2 Credit		

Total Credit Hours: 48

APPENDIX B
COURSE DESCRIPTIONS

New courses are denoted with an asterisk.

Core Courses

CYSE 600 Cybersecurity Principles (3 credits)
This course provides an overview of the field of cybersecurity. It covers core cybersecurity topics including computer system architectures, critical infrastructures, cyber threats and vulnerabilities, cryptography, cryptographic protocol design, information assurance, network security, and risk assessment and management. Students are expected to become familiar with fundamental security concepts, technologies and practices, and develop a foundation for further study in cybersecurity.

CYSE 601 Advanced Cybersecurity Techniques and Operations (3 credits)
This course introduces tools and techniques used to secure and analyze large computer networks and systems. It will include significant hands-on lab work. Students will explore and map networks using a variety of diagnostic software tools, learn advanced packet analysis, configure firewalls, write intrusion detection rules, perform malware detection, forensic investigation, and practice techniques for penetration testing.

CYSE 603 Advanced Cybersecurity Law and Policy (3 credits)
This course addresses two major cyber law subject matters. The first part of the course examines various U.S. laws and legal considerations that impact the digital and cyberspace worlds from civil and criminal perspectives. The second part, which builds upon the first, will familiarize cyber operations professionals about the extent of and limitations on their authorities to ensure operations in cyberspace are in compliance with U.S. law, regulations, directives and policies.

CYSE 605 Leadership and Management in Cybersecurity (3 credits)
This course introduces skills to manage technical professionals and lead strategic change in their organization. Based on the basic operations and functionality of cybersecurity systems, students will learn the management of cybersecurity technical professionals, including how to effectively lead and manage teams, how to launch and assess organizational change initiatives, and how to work effectively within an interdependent group to achieve common goals.

CYSE 616 Cyber Defense Fundamentals (3 credits)
This course introduces students to cyber security and defense. The course will primarily focus on cybersecurity theory, information protection and assurance, and computer systems and networks security. This course provides the essentials for understanding the security threats to information systems, the methods to counter these threats, and the state-of-the-art implementations and applications of cybersecurity systems.

CYSE 800 Research Methods in Cybersecurity* (3 credits)
Students learn how to use multiple research methods to conduct cybersecurity research. Students will conduct a multi-method research project in interdisciplinary groups.

Prerequisite: CYSE 600.

CYSE 701/801 Advanced Cybersecurity Techniques and Operations II (3 credits)
Students apply the tools and techniques learned in Advanced Cybersecurity Techniques and Operations. Virtual laboratory work is conducted, and students produce scientific reports describing the results of their analyses, investigations, and diagnoses.
Prerequisite: CYSE 601.

CYSE 802 Cybersecurity Seminar* (3 credits)
Introduces new PhD students to the study of cybersecurity through an interdisciplinary lens interdisciplinary fields of study offered as doctoral programs at ODU. Students will read studies published by ODU scholars and discuss how interdisciplinary research informs society. Students will identify possible research agendas for their doctoral studies. Professional development will be included.

CYSE/ PHIL 803 Moral Reasoning for Emerging Technologies* (3 credits)

This course provides training in how to think critically and inclusively about moral and ethical concerns in the context of new, emerging, and developing technologies. In these contexts where ethical guidelines and practices have not been fully developed, it is necessary to have experience with flexible and adaptive training in identifying and thinking through moral concerns. Students will develop these skills through a study of philosophy of technology, history of technology, and Science and Technology Studies combined with active and creative forms of speculative application of these theories and methods.

CYSE 868 Cybersecurity Practicum* (3 credits)
Students work in a professional setting and apply their cybersecurity skills. The professional setting may include a higher education setting, industry, government agency, research laboratory, or other setting. Students complete an electronic portfolio, work journal, and professional paper highlighting the ethical, policy, and empirical connections between their work experience and their doctoral studies.

Foundational Elective Courses

CYSE 519 Cyber Physical Systems Security (3 credits)
This course will introduce the state-of-the-art Cyber Physical System (CPS) technologies, ranging from Internet-of-Things to clouds. The objectives are to learn the basic concepts, technologies and applications of CPS, understand the fundamental security challenges and practical countermeasures and attacks, and gain hands-on experience in CPS systems.

CYSE 520 Applied Machine Learning in Cybersecurity (3 Credit Hours)
This course introduces the concepts and technologies of machine learning with a focus on applications related to cybersecurity. The objectives are to learn fundamental knowledge and practical experience and identify the use case of machine learning techniques in cybersecurity.

The course will discuss traditional and advanced machine learning techniques, e.g., neural network, deep convolutional neural network, generative adversarial network, and transfer learning algorithms. Students will engage in oral and written communication by reporting and presenting the materials of the course project.

CYSE 525 Cybersecurity Strategy and Policy (3 Credit Hours)
This course explores cybersecurity policy and strategy and introduces students to the essentials of strategy development and policy making in cybersecurity. Topics considered include planning principles in cyber strategy; risk management and cybersecurity policy; the connections between cybersecurity policies, businesses, and governmental institutions; the knowledge, skills, and abilities needed to develop and implement cybersecurity policy; the social, political and ethical implications that arise in cybersecurity policies and strategies; strategies to assess cybersecurity policy; and the ties between national security and cybersecurity policy.

CYSE 526 Cyber War (3 Credit Hours)
This course explores the national security dimensions of cybersecurity and examines cyber war in international relations. Exploration of cyber war begins with an examination of cybersecurity as a component of national security and investigates the topics of U.S National Cybersecurity and other national approaches to cyber war. The topics of cyber deterrence, cyber as a military domain, the roles of international organizations in cyber war, cyber terrorism, the role of social media, and information warfare will be discussed. The international dimension of cybersecurity is also discussed.

CYSE 595 Topics in Cybersecurity (3 Credit Hours)
The advanced study of selected cybersecurity topics designed to permit small groups of qualified students to work on subjects of mutual interest. These courses will appear in the course schedule and will be more fully described in information distributed to academic advisors.
Prerequisites: permission of the instructor

CYSE 607 Advanced Digital Forensics (3 credits)
This course introduces the concepts and technologies of digital forensics. Students will learn the advanced techniques and tools utilized for collecting, processing, and preserving digital evidence on computers, mobile devices, networks, and cloud computing environments. Students will also engage in oral and written communication to report digital forensic findings and prepare court presentation materials.

CYSE 610 Advanced Cryptography (3 Credit Hours)
This course studies advanced topics in cryptography. It begins with an overview of necessary background in algebra and number theory, private- and public-key cryptosystems, and basic signature schemes. It then upgrades the design and analysis of modern cryptography, including how the security model is defined, how practical cryptographic algorithms work, and how to exploit flaws in the current models of cryptography.

CYSE 615 Mobile and Wireless Security (3 credits)

An overview of wireless and mobile security providing students with practical and theoretical experiences. Topics include smartphone security, mobile Internet security, mobile location privacy, and wireless ad hoc, mesh, and sensor network security.

CYSE 625 Advanced Ethical Hacking and Penetration Testing (3 credits)
This course teaches students the underlying principles and many of the techniques associated with the cybersecurity practice known as penetration testing or ethical hacking. The course covers planning, reconnaissance, scanning, exploitation, post-exploitation, and result reporting. Students will discover how system vulnerabilities can be exploited and learns to avoid such problems.

CYSE 635 AI Security and Privacy (3 Credit Hours)
This course focuses on Machine Learning (ML) security and privacy. Students will understand and explore the vulnerabilities of the ML models, learn how to develop and deploy defenses to mitigate possible attacks, and gain hands-on experience to protect private data during model training and testing.

CYSE 695 Advanced Topics in Cybersecurity (3 Credit Hours)
The advanced study of selected cybersecurity topics designed to permit small groups of qualified students to work on subjects of mutual interest. These courses will appear in the course schedule and will be more fully described by academic advisors.
Prerequisites: Permission of the instructor

CYSE 697 Independent Study in Cybersecurity (3 credits)
This course allows students to develop specialized expertise by independent study (supervised by a faculty member).

CS 564 Networked Systems Security (3 credits)
This course is focused on network security. It begins with a review of various forms of network attacks including scanning, exploits and denial-of-service attacks, as well as various cryptographic mechanisms. Then, it will cover different security tools and protocols at different layers of network stack such as Layer 3 (IPSEC), Layer 4 (SSL) and Layer 7 (kerberos). It will also teach intrusion detection systems, viruses, firewalls, VPNs, and wireless security.

CS 565 Information Assurance (3 credits)
Introduction to information assurance; metrics, planning and deployment; identity and trust technologies; verification and evaluation, incident response; human factors; regulation, policy languages, and enforcement; legal, ethical, and social implications; privacy and security trade-offs; system survivability; intrusion detection; fault and security management.

CS 566 Principles and Practice of Cyber Defense (3 Credit Hours)
This course is to help students gain a thorough understanding of vulnerabilities and attacks in systems and networks and learn cyber defense best practices. It covers fundamental security design principles and defense strategies and security tools used to mitigate various cyber attacks. The topics may include identification of Recon Ops, intrusion detection, identification of C2 Ops, data exfiltration detection, identifying malicious codes, network security techniques,

cryptography, malicious activity detection, system security architectures, defense in depth, distributed/cloud and virtualization. Laboratory work required.
Prerequisites: Basic knowledge of programming, computer architecture, computer networks and operating systems; no prior knowledge of computer security is necessary.

CS 567 Introduction to Reverse Software Engineering (3 Credit Hours)
Covers all the major components such as static analysis, dynamic analysis, Windows x86/64 Assembly, APIs, DLL/process injection, covert launching methods, behaviors, anti-disassembly, anti-VM, packing/unpacking, shell code, C++, buffer overflow attacks and various kinds of networking attacks; includes a final project that analyzes a piece of real malware.

CS 861 Malware Analysis and Reverse Engineering (3 Credit Hours)
Theory and practice in analysis and mitigation of malware in networked machines. Theoretical topics include methods of attack anatomy, identification, reverse and anti-reverse engineering. Practice entails learning tools and techniques used by malware attackers, defenders and analysts in lab-based projects conducted in a secure 'sandbox' mode.

CS 569 Data Analytics for Cybersecurity (3 Credit Hours)
The course introduces classical and advanced models and techniques in machine learning and deep learning. It applies these techniques in the cybersecurity domain including anomaly detection, network security, and malware detection and classification. Advanced applications such as self-driving cars and IoT systems are also discussed. In addition, cyber-attacks on machine learning techniques and AI systems and the possible consequences are also discussed.
Prerequisites: experience in cybersecurity.

CS 522 Introduction to Machine Learning (3 Credit Hours)
An introduction to machine learning with a focus on practical aspects of various learning techniques. Topics include supervised learning (linear models, probabilistic models, support vector machine, decision trees, neural networks, etc.), unsupervised learning (scaling, dimension reduction, clustering, etc.), reinforcement learning, and model evaluation. The course will also discuss applications on image analysis, text processing, and biomedical informatics.

CS 580 Introduction to Artificial Intelligence (3 Credit Hours)
Introduction to concepts, principles, challenges, and research in major areas of AI. Areas of discussion include natural language and vision processing, machine learning, machine logic and reasoning, robotics, expert and mundane systems.

CS 624 Data Analytics and Big Data (3 Credit Hours)
This course introduces the essential data science tools to work with different types of data including streaming data and big data, including static and streaming data using Python software packages; modeling and predictive analysis using basic machine learning techniques; work with real sample data sets from different disciplines, e.g., the health sciences and finance industry; and how to work with big data using emerging technology such as Apache Spark.

CS 822 Machine Learning (3 Credit Hours)

This course presents both the foundational and the practical aspects of modeling, analyzing, and mining of computerized data sets, including classification, regression, clustering, semi-supervised learning, structured sparsity learning, etc. The course assignments are designed to contain both theoretical and programming components in order to train students to gain hands-on-experience.

CS 833 Natural Language Processing (3 Credit Hours)
Natural language processing (NLP) techniques are the crux of many leading modern technologies. Advances in NLP are also critical in the pursuit of Artificial Intelligence. This course will discuss core problems in NLP and the state-of-the-art tools and techniques as well as advanced NLP research topics. The topics will include language models, part-of-speech tagging, syntactic parsing, word embedding, statistical machine translation, text summarization, question answering, and dialog interaction. At the end of the course, students will be familiar with many language-processing tasks and applications.

MSIM/ENMA 670 Cyber Systems Engineering (3 credits)
This course provides an overview of functioning of cyber systems including how a computer interacts with the outside world. The composition of critical infrastructure and functioning of different engineered systems that form critical infrastructure is discussed. Mutual dependence and interactions between cyber systems and other engineered and the resulting security risks are also explored.

Advanced Electives.

CRIM 832 Advanced Cybercriminology* (3 Credit Hours)
This course explores cybersecurity through criminological and sociological lenses. Students critique popular criminological theories and examine their application to cybercrime and the response to cybercrime. Methods used by cybercriminologists to study cybercrime are considered within the context of social science and tradition STEM research strategies. Students will develop a research proposal for a cybersecurity study that is grounded in criminological themes and uses social science research methods

CS 764 Blockchains and Cryptocurrencies: Fundamentals, Technologies, and Economics (3 Credit Hours)
This course covers different aspects of cryptocurrencies, including P2P networks, distributed consensus, Bitcoin and Ethereum, blockchain technologies, cryptographic techniques (secure hashing, encryption, decryption, digital signatures), privacy and anonymity, mining and mining puzzles, wallets, smart contracts, case studies, cryptocurrency ecosystem, legal aspects, implications and impact on economy and finance, and future of cryptocurrencies.
Prerequisites: CS 471, CS 455/CS 555 or equivalent experience

CS 865 Internet of Things Security (3 Credit Hours)
This course covers various topics in Internet of Things (IoT) security, including web security, network security, mobile app security and secure cryptocurrency. It provides an in-depth study of various attack techniques and methods to defend against them. The course adopts the 'learning by doing' principle. Students are supposed to learn the attacks by performing them in a networked

virtual machine environment. They will also play with a number of security tools to understand how they work and what security guarantee they provide. Laboratory work required. Prerequisites: basic knowledge of programming, computer networks and operating systems; no prior knowledge of computer security is necessary

CS 872 Advanced Computer and Network Security (3 Credit Hours)
This course is a research-oriented, graduate-level course, centering around basic protocols and technique, as well as advanced, state-of-the-art topics to secure computer and Internet services. Topics include System and Software Security, Cryptography and PKI, Internet Infrastructure and Network Security, Web and Browser Security, Cloud Security, and Online Privacy. Prerequisites: CS 455 or CS 555

CS 873 Data Mining and Security (3 Credit Hours)
Introduction to data mining; Algorithms including naive Bayes, Decision Trees and Rules, Association Rules, Linear classification, and Clustering; Cross validation, Lift charts, ROC Curves; SVM, Bayesian networks, K-means clustering; Data transformation; PCA; Ensemble Learning; Application of data mining to security and privacy including authentication, authorization, and intrusion detection; Privacy-preserving data mining.

CS 874 Distributed System Security with .Net (3 Credit Hours)
The course provides a detailed coverage of security aspects of ASP.Net. It examines distributed system architectures, ASP.Net security framework, cyber attacks, system vulnerabilities, C# and ADO.Net. It also discusses windows and forms authentication, authorization, impersonation, and code obfuscation, and advanced concepts, including secure web services, runtime security, operating system security, code access security, role-based access control, and attribute-based access control. Finally, cryptography, XACML and security policies as implemented in

CYSE 897. Independent Study (3 credit hours).
Student conducts an independent project under the supervision of a faculty member with expertise in cybersecurity. GPD approval required.

ENGL 830 The Digital Humanities (3 Credit Hours).
Taking historical, cultural, and theoretical views, this course bridges literary studies with new media. How has technology historically affected literature and culture? Can the democratization of information accelerate literary development? Topics will include digital archives, intellectual property in the information age, and electronic textuality.

ENMA 801 Digital Systems Engineering (3 Credit Hours)
Digital systems engineering applies digital technologies to the systems engineering processes and principles. This course provides students with knowledge and skills on necessary digital technologies, such as Artificial Intelligence and Machine Learning, Big Data, Blockchain, and computational modeling. The course covers: (1) preliminaries of digitalization and digital technologies; (2) data and knowledge modeling; (3) logical approach to MBSE (Model-Based Systems Engineering); (4) application of Big Data and Machine Learning in Systems

Engineering; and (5) digital mechanisms of trust and security for digital engineering. Prerequisites: ENMA 646

ENMA 824 Risk Analysis (3 Credit Hours)
Approaches to the management of risk; probability assessment methods; risk modeling; use of software packages; extensions of decision analysis, including stochastic dominance and multiattribute methods; applications to project management, scheduling, and cost estimation.

ENMA 825 System Risk and Failure Analysis (3 Credit Hours)
This course is about the modeling of system dependencies using functional dependency network analysis to support the design of new and failure analysis of existing engineering systems. At the end of this course, students will be able to model and measure the operability and performance of today's highly networked and richly interconnected systems.

ENMA 850 System of Systems Engineering (3 Credit Hours)
Comprehensive treatment of System of Systems Engineering (SoSE), including fundamental systems principles, concepts, and governing laws; complex and simple systems; underlying paradigms, methodologies, and essential methods for SoSE analysis, design, and transformation; complex system transformation; current state of SoSE research and application challenges. Explores the range of technological, human/social, organizational/managerial, policy, and political dimensions of the SoSE problem domain.

ENMA 855 Human System Engineering (3 Credit Hours)
This course introduces concepts of Human System Engineering, focusing on designing systems that include human components. Human System Integration and Human Factors Engineering are discussed, as well as other human centered design approaches. The role of human data in systems and systems of systems design is explored, and methods to capture and represent human data, including architecture frameworks, are presented. Modeling and analysis of human centered systems is done through hands-on projects.

ENMA 871 Risk and Vulnerability Management of Complex Interdependent Systems (3 Credit Hours)
Seminar discussions and team projects. A systematic approach to basic principles of design, economics, and management of critical infrastructure systems, including issues of risk, vulnerability, and risk governance. Development of advanced methodologies, e.g. system of systems, by use of complexity analysis, dynamic/chaotic behavior, threat analysis, resilient design, and management under normal and stress conditions. Adopting an agent-based modeling approach under conditions of uncertainty, dysfunctionality, malicious attacks and/or presence of natural perils. Prerequisites: Permission of the instructor

ECE 742 Computer Communication Networks (3 Credit Hours)
This is an advanced level course in data communications. A focus is placed on the analysis, modeling, and control of computer communication systems. Topics include packet switched networks, circuit switched networks, ATM networks, network programming, network control and performance analysis, network security, and wireless sensor networks.

IDT 830 Principles and Practices of Human Performance Technology (3 Credit Hours)
This course explores both the principles and practices of human performance technology, with roughly equal emphasis on both. Students will learn what HPT is, how it's applied in practice, and how and why instructional designers need to know about it. Particular emphasis is given to determining whether or not problems are best amenable to instructional solutions.

IS 721/821 New World Order: Chaos or Coherence? (3 Credit Hours)
This course explores ideas of order and how they apply to international politics over space and time. Using theories of international relations, students look at how states and other international actors shape the principles and practices on which order is built and how these actors navigate among the many challenges and disruptions that arise. Specifically, students study the international liberal order, power shifts, and technological innovations, including cyber, and the rise and demise of norms in the international system.

PSYC 870 Human Factors Psychology (3 Credit Hours)
The application and evaluation of psychological principles and research relating human behavior to the design of tools, technology, and the work environment. Theory, methods, and application are emphasized. Prerequisites: PSYC 731/PSYC 831 and PSYC 741/PSYC 841 or equivalents or permission of the instructor

PSYC 876 Human-Computer Interaction (3 Credit Hours)
Review of the physical, cognitive, and performance capabilities and limitations of humans as they interact with modern computer systems. Emphasis is placed on the tools, techniques and procedures for the assessment and effective design of computer hardware, software and displays of information.

APPENDIX C
FACULTY CURRICULUM VITAE (ABBREVIATED)

Core Faculty

Tababi, Daniel, PhD, 2013, Information Technology and Science, University of Pittsburgh, Batten Endowed Chair of Cybersecurity, Specialization: Cybersecurity and privacy: Trustworthy AI, computation on encrypted data, insider threat, privacy enhancing technologies, usable privacy and security, advance access control models, sociotechnical aspects of cybersecurity and privacy.

Xin, Chunsheng, PhD, 2002, Computer Science, State University of New York at Buffalo. Associate Professor of Electrical and Computer Engineering. Specialization areas: Cybersecurity, cognitive radio networks, wireless communications and networking, cyber-physical systems, and performance evaluation and modeling.

Diaz, Rafael, PhD, 2007, Modeling and Simulation, Old Dominion University, Professor of Cybersecurity and Engineering Management. Specialization: Cyber risk management, supply chain cybersecurity, digital security, homeland security.

Karahan, Saltuk, PhD, 2015, International Studies, Old Dominion University, Senior Lecturer of Cybersecurity. Specialization: strategy, cybersecurity policy, international security dimensions of cybersecurity, systems engineering.

Ghasemigol, Mohammad, PhD, 2016, Computer Engineering, Ferdowsi University of Mashhad, Research Assistant Professor of Cybersecurity. Specialization: network security, IoT security, IDS, alert management, IRS, and incident handling

Md Shirajum Munir, PhD, 2017, Computer Engineering, Kyung Hee University, Republic of Korea. Research Assistant Professor of Cybersecurity. Specialization: Intelligent cyber-physical systems; Cyber-security, risk, and privacy management; AI security and privacy; Trustworthy machine learning (ML); AI-driven network automation and optimization.

Md Masud Rana, PhD, 2017, Computer Science and Engineering, University of Technology Sydney, Australia Mar. Research Assistant Professor of Cybersecurity. Specialization: network security, IoT security, IDS, alert management, IRS, and incident handling

Peng Jiang, PhD, 2024, Electrical & Computer Engineering, Old Dominion University. Senior Lecturer of Cybersecurity. Specialization: cyber operations, cyber defense, IoT security.

Wittkower, D.E., PhD, 2006, Philosophy, Vanderbilt University. Professor of Philosophy. Specialization areas: Philosophy of technology, new media theory, social networks and social media, business ethics, internet studies.

Sanzo, Karen, EdD, 2006, Education Administration and Policy Studies, The George Washington University. Professor of Educational Leadership. Specialization areas: Design thinking, improvement science, education.

Foundation and Advanced Elective Faculty

Shetty, Sachin, PhD, 2007, Modeling and Simulation, Old Dominion University. Associate Professor of Modeling, Simulation and Visualization Engineering. Specialization areas: Cloud and mobile security, computer networking, network security and machine learning.

Ning, Rui, PhD, 2020, Electrical & Computer Engineering, Old Dominion University. Assistant Professor of Computer Science. Specialization areas: cybersecurity and secure & privacy-preserved AI.

Mukkamala, Ravi, PhD, 1987, Computer Science, University of Iowa. Professor of Computer Science. Specialization areas: Security and privacy in computer systems and networks, database security, access control, and key management.

Handley, Holly, Ph.D., Information Technology and Engineering, George Mason University, 1999, Professor. Specialization: Data Science, Human Systems Engineering

Payne, Brian K. PhD, 1993, Criminology, Indiana University of Pennsylvania, Professor of Cybersecurity, Specialization areas: Cybercrime, Cybercriminology.

Gheorghe, Adrian, PhD, 1975, Systems Engineering, System Science, City University (London). Professor of Engineering Management and Systems Engineering and Batten Endowed Chair on System of Systems Engineering. Specialization areas: Critical infrastructures security, emergency planning, vulnerability modeling, security of complex systems, and homeland security and safety.

Still, Jeremiah, PhD, 2009, Human Computer Interaction, Iowa State University. Associate Professor of Psychology. Specialization Area: Human Computer Interaction, Usable design.

Wu, Harris, PhD, 2005, Business Information Technology, University of Michigan. Associate Professor of Information Technology and Decision Sciences. Specialization areas: Cybersecurity, data analytics, social media, text mining, enterprise information systems, and system integration.

Karp, Regina, PhD, 1985, University of Lancaster. Associate Professor of International Studies. Areas of Specialization: Arms Control, Weapons Proliferation, International Security, European Security.

APPENDIX D - EMPLOYMENT DEMAND - JOB ANNOUNCEMENTS

Endowed Associate Director of Cybersecurity

University of Oklahoma
Tulsa, OK

Type: Full-Time
Posted: 10/19/2023
Category: Other Science Faculty

Position Title: Endowed Associate Director of Cybersecurity

Location: OU Polytechnic Institute in Tulsa

Department: Polytechnic Institute in Tulsa

Position Type: Faculty

Qualifications:

The successful candidate will be a thoughtful, dynamic, purposeful and collaborative leader with a desire to build a polytechnic for the 21st century. An outstanding record of scholarship, research, dedication to technological education and inclusive excellence is expected to serve in this inaugural role. Candidates must have the requisite record of research, scholarship, teaching and mentoring to hold the rank of associate or full professor in a cybersecurity related field. Candidates should also have a PhD in cybersecurity or a related field and a strong record of departmental, school or other appropriate leadership experience. In addition, qualified candidates should have a demonstrated record of positive accomplishments in nurturing and enhancement of faculty, undergraduates and graduates, and effective management of complex physical and human infrastructure. Additional weight will be given to candidates that have research programs that include industry sponsorships.

Application Instructions:

Applicants are invited to submit a CV or resume along with a cover letter that includes a summary of teaching, research, administrative responsibilities and service activities and a description of how their background and career goals will support the success of OUPI students and faculty. Finally, please include the contact information for at least four references with a statement of the relationship of each reference. Additional materials may be requested later. Documents should be uploaded to https://apply.interfolio.com/131713. Initial screening of applications will begin on October 1, 2023, and will continue until the position is filled. The start date is negotiable. Inquiries and nominations may be sent to the search committee chair at teri.reed@ou.edu.

Description:

The University of Oklahoma (OU) is embarking on a transformational endeavor to grow the newly established OU Polytechnic Institute (OUPI). The aims are to further strengthen the educational landscape of the state, provide students with a unique educational experience that will enable them to be successful throughout their careers and respond to industry's need for a well educated, highly skilled and adaptable workforce to meet current and future needs. The Institute will be in Tulsa at the OU-Tulsa Schusterman Center campus. Enrollment for the inaugural class began this August and classes will start in August 2024. This position is being posted now to allow hired faculty leaders time to develop curriculum, plan programming, hire faculty and initiate research.

OUPI invites applications for the inaugural Associate Director of Cybersecurity, a senior-level faculty appointment and leadership position at the associate/full professor level with an endowed George Kaiser Family Foundation Chair available. This 12-month administrative position offers the opportunity to shape a forward-looking and innovative new program in Cybersecurity contributing to teaching, advising, mentoring, curriculum design and implementation at the undergraduate and graduate levels.

This endowed faculty leadership position offers a unique opportunity to shape the future of OUPI and is aligned with the OU strategic plan. Individuals with a strong track record in leadership and collaboration in cybersecurity related fields are encouraged to apply. The OUPI will offer bachelor's degree completion (junior and senior level classes only) and graduate degree programs

focused on innovation and advanced technology to meet growing workforce demands in areas including cybersecurity, software development and integration, artificial intelligence and advanced computing, health information systems and digital manufacturing. Threading through these areas are competencies in data science.

HigherEdJobs

Assistant Professor - Computer Science & Electrical Engineering - Cybersecurity

Type: Full-Time
Posted: 02/15/2024
Category: Computer Science; +1

Assistant Professor - Computer Science & Electrical Engineering - Cybersecurity

About Eastern Washington University:
Eastern Washington University, a regional, comprehensive public university with an enrollment of over 10,000 students, is one of six state-funded four-year institutions of higher education in Washington, each governed by its own board of trustees. EWUs 300-acre main campus is located in Cheney, a community of 12,000 residents 16 miles southwest of Washingtons second largest city, Spokane. Eastern also offers programs in downtown Spokane at the innovative, energy-efficient Catalyst building, the SIERR building which is a hub for research, development and advancement of health sciences, and at Riverpoint, a campus shared with Washington State University. In addition, EWU programs can be found at select locations throughout the state, aligned with the needs of the community. Eastern contributes to the vitality of the region and the state through its wide array of bachelors and masters degrees in over 100 fields of study, as well as applied doctorates in physical therapy and educational leadership, offering accessible pathways to career success and personal development to students of all socioeconomic and cultural backgrounds.

Eastern Washington University has been recognized for its commitment to helping undergraduate students learn, grow and succeed by **Colleges of Distinction**, a nationally trusted resource guide for college-bound students. The honor recognizes Eastern as a **22-23 College of Distinction** (CoD). *Money* magazine recently named **EWU as one of its Best Colleges in America 2023**.
Tribal Land Acknowledgement
Eastern Washington University resides within the traditional homelands of the Spokane People and other tribes who are connected through their shared history of this region. This land holds their cultural DNA and it is their Ancestors who are here and bring forth the knowledge of this place-the knowledge that comes from the land.

Job Summary:
Assistant Professor Tenure-Track, Cybersecurity College of Science, Technology, Engineering and MathematicsEastern Washington University
The Department of Computer Science and Electrical Engineering (CSEE) at Eastern Washington University (EWU) invites applications for an **assistant professor tenure-track position to begin September 2025.**
The Department of CSEE is one of two four-year NSA National Centers for Academic Excellence in Cyber Defense in the state of Washington, and offers academic programs leading to bachelor's and master's degrees: a Bachelor of Science in Computer Science Cyber Operations, a Bachelor of Science Cyber Operations, an ABET-accredited Bachelor of Science in Computer Science, a Bachelor of Computer Science, an ABET-accredited Bachelor of Science in Electrical and Computer Engineering, and a Master of Science in Computer Science. The program has recently received a significant investment by the state of Washington and is anticipating substantial growth in the coming years.
EWU's Cybersecurity Program is in the Department of Computer Science and Electrical Engineering. Cybersecurity/ Computer Science has 10 faculty members and approximately 400 undergraduate and 10 masters' students. The department resides in the Catalyst Building located in downtown Spokane's University District. This facility is a public-private partnership with the regional tech industry to create a high-tech hub for innovation and entrepreneurship. It offers our students and faculty outstanding opportunities for collaboration with regional industry and other universities.More information about life in Spokane: **https://www.visitspokane.com/**
All faculty are expected to actively participate in curriculum development, assessment of student learning and to engage in effective teaching including teaching practices and interactions with students with emphasis on student retention and a culture of belonging.
In addition to salary, the university offers a comprehensive benefits package including health insurance, life and disability insurance and retirement. In addition, EWU offers generous vacation and sick leave accruals, 12 paid holidays per year and fringe benefits, such as tuition waiver for employees, discounted EWU sports tickets, full access to our campus workout facilities at a minimum fee and free transportation through STA buses. For additional information regarding insurance benefits please see our Benefits page: **https://inside.ewu.ed u/hr/benefits/insurance/**.

Required Qualifications:

- A PhD in Cybersecurity, Computer Science, Computer Engineering, or closely related discipline is required at the time of appointment.

Type: Full-Time
Posted: 03/05/2024
Application Due: 03/31/2024
Category: Computer Science

Tenure Status: Tenure Track

Job Description

JOB SUMMARY:
The Department of Mathematics and Computer Science (MCS) at Coppin State University (CSU) seeks applications for one full time tenure-track Assistant/Associate Professor of Cybersecurity Engineering position with a Ph.D. in Cybersecurity, Computer Science. Digital Forensics or Computer Engineering related discipline.

Assistant Professor of Computer Science or Cybersecurity Engineering

Coppin State University in Baltimore, MD

Apply on Institution's Website

This position carries the CYSE and Computer Science program curriculum advancement and instructional content teaching and development, Cyber-lab supported advance CYSE R&D projects development and testing responsibilities, and participation in faculty and students training activities, and pursuing an engaging research grant writing agenda linking to NSA- CAE Cyber Operations Fundamental Knowledge Units, and seeking the ABET accreditation will be some of the areas MCS department is moving forward, and new faculty-hire will have the opportunity to play a leading role. Other desirable areas are AI/ML, Data Science, intelligent systems or quantum information science and computing.

It is imperative that all prospective applicants have experience and strong knowledge of developing software from object-oriented programming languages. Current primary languages taught in the MCS department include Java, C++, Python, and Ruby. The candidates must be familiar with one or more professional Integrated Development Environment, such as: Eclipse, MS Visual Studio Professional or a comparable IDEs. Secondary languages taught at CSU include R, C, JavaScript and Obj-C and the ability to run Jupyter notebooks and labs. Opportunities exist for collaborations with DoE, IBM, NSA and many other federal agencies in the nearby areas of Maryland, Washington DC and Virginia. The teaching requirement is 24 hrs./AY undergraduate CYSE and Computer Science courses during the day and/or evening. Candidates with established research agenda and advanced course-curriculum development interest in one or more of these areas will be given preference. Coppin State University (HBC/MI) is a member of University System of Maryland and was founded in 1900 (www.coppin.edu).

ESSENTIAL RESPONSIBILITIES:

- Twelve credits hours (4 courses) teaching at the undergraduate level. New advanced Cybersecurity Engineering and computer science courses and labs projects development.
- Development of face-to-face and Bb Ultra Online instructional materials, and Cyber-lab management and operation.
- Ability to work a flexible schedule that may include evening and weekend assignments.
- Research or scholarly activity involving publications and interest in grant-proposal writing.
- Collaborating with colleagues and or external university faculty.
- Assist department chair in coordinating and updating Computer Science and CYSE curricular, help update Computer Science and Cyber-labs' software and participate in MCS department's students outreach activities.
- Lead and support in developing Instructional and faculty workshops, labs, and materials reflecting culturally responsive and cultural intelligence learning thread.
- University-wide, College-wide, and Department-wide committee assignments.
- Student advising, student's support and Computer Science and Mathematics club activities.
- Participating in University-wide activities as assigned by the Chair.

Required Qualifications

EDUCATION:

- Applicants must have a PhD in Cybersecurity, Computer Science, Digital Forensics or Computer Engineering related discipline at the time of appointment and must have a commitment to quality teaching, a strong research and professional-service record.
- NIST certification is ideal.

Assistant/Associate Professor Cybersecurity

Job Class Code: 10031
FLSA: Exempt
Posting Number: FRGV1558
Location: Brownsville, Texas

Division/Organization: Provost - Academic Affairs
Appointment Period for Non-Tenure Position:
Tenure Status: Tenure Track
FTE: 1.0

Scope of Job:
The department of Informatics and Engineering Systems (IES) at The University of Texas Rio Grande Valley seeks applicants for one or more faculty positions in the broad area of Cybersecurity and Informatics. Successful candidates will be expected to teach and build research programs in the general area of informatics and cyber security.

The Department of Informatics and Engineering Systems currently has fourteen faculty members and offers several degree programs and research opportunities in the field of Informatics, Cyber Security, and Engineering Technology. The department offers a Bachelor of Science in Cybersecurity, a Bachelor of Science in Engineering Technology (automation), and a Master of Science in Informatics. The department offers research opportunities in informatics and engineering systems. Our programs prepare students for careers in industry and graduate study in informatics, engineering systems, and technology-related fields. We are actively pursuing program development at the undergraduate and graduate levels in the areas of informatics and engineering systems. The positions are for tenure track assistant professors; however, exceptional candidates may be considered for credit toward time on tenure track or for appointment as associate professor. Candidates are encouraged to highlight relevant expertise in these areas and interest to help in the development of such programs.

For further information regarding UTRGV and the Department of Informatics and Engineering Systems, please visit our websites at **www.utrgv.edu/cyberspace/**.

obs.chronicle.com/job/37582383/assistant-associate-professor-cybersecurity/

. 9:07 PM Assistant/Associate Professor Cybersecurity job with University of Texas - Rio Grande Valley | 37582383

Minimum Qualifications:
Applicants must have an earned Ph.D. in Cybersecurity, Informatics, Computer Science, or a related field from an accredited university.
Candidates at the Assistant Professor level will be considered based on demonstrated potential to enhance the teaching and research capabilities of the Cybersecurity program at UTRGV.

Associate Professor/Professor and Director of Cybersecurity (6761)

Employer
Northern Illinois University

Location
Illinois, United States

Salary
Salary Not Specified

Posted Date
Jan 19, 2024

View more

Apply on website

Save Send job

Position Summary

The Founding Director will provide vision and leadership to the university to create a nationally recognized program in cybersecurity. The Director will report to the Chair of the Computer Science department and is responsible for establishing and leading academic programs and outreach efforts to support cybersecurity workforce development. The Director will play a principal role in recruiting the first cohort of faculty expected to be hired in Fall 2025 in this

substantial and growing field.

Essential Duties and Responsibilities

- Lead efforts to create cutting-edge certificate and degree programs, including online programs, that are compliant with and recognized as part of national frameworks.
- Develop a robust vision and sustainable funding model for an agile cybersecurity workforce development program that includes strategies and plans to acquire external funds to support program development and outreach efforts.
- Identify opportunities for private- and public-sector partnerships that seek to develop cybersecurity solutions, particularly as those opportunities apply to employment for students as interns and career opportunities upon their graduation.
- Represent the department's cybersecurity programs by liaising and collaborating within the university and with external private- and public-sector cybersecurity groups.
- Promote the cybersecurity programs and recruit students.
- Recruit personnel in support of the cybersecurity programs.
- Monitor, maintain, and report on the quality and viability of the cybersecurity programs.
- Oversee and contribute to the development of new courses related to cybersecurity.
- Teach cybersecurity courses each academic year.

Minimum Required Qualifications

- Earned a doctorate in cybersecurity, computer science, or closely related field.
- Tenurable at the rank of associate or full professor.
- Five years of experience in cybersecurity in government, industry, or academia.

University Faculty Cybersecurity School of Computing

Requisition Number: F00389P:

Job Description:
Weber State University invites applications for a full-time tenure track faculty position or full time instructor (see required qualifications) in the School of Computing to begin in Fall 2024. The School of Computing houses three programs: Computer Science, Cybersecurity and Network Management, and Web & User Experience.

Job Duties:
Successful candidates will have duties that include teaching undergraduate

level courses, in a variety of modalities and campuses, including but not limited to: Face-to-Face, Virtual, and Online classes at the Ogden and Davis campus as well as some night classes, conducting some research and scholarship, participating in course and curriculum development, and providing service to the department, college, and the university.

Required Qualifications:
To be eligible for a tenure track appointment applicants must have a PhD or other terminal degree in Cybersecurity, Information Systems, Computer Science, or a related discipline or be on track to complete their terminal degree by the start of the 2024 Fall semester.

Cybersecurity Faculty

Job Location

1460 University Drive, Winchester, Virginia

Tracking Code

1367-306

Shenandoah University is seeking a dynamic and versatile individual with a pioneering spirit and a love of teaching to shape our nascent Cybersecurity Master's degree program. Post-docs are encouraged to apply. Candidates with exceptional academic and/or industry experience will be considered for appointment at the rank of Associate Professor.

The successful applicant will be an innovator who will help us design and deploy this new program to meet the needs of both students and industry as we improve our cyberdefenses in a rapidly evolving environment. Shenandoah University, located in the beautiful Shenandoah Valley, boasts a nimble and vibrant atmosphere where we value novel approaches and a diversity of ideas.

Required Skills

Qualifications:

Qualifications for this position include outstanding industry experience and/or an earned masters or Phd in Cybersecurity, Computer Science, Information Technology, or a related field. The ideal candidate will have experience with a variety of operating systems, cybersecurity tools, applicable laws, and modern best practices.

Assistant Professor of Cyber Threat Intelligence

Coastal Carolina University
Conway, SC

Type: Full-Time
Posted: 12/16/2023
Application Due: Open Until Filled
Category: Security Studies

Does this position require driving?: No

Job Details

Assistant Professor of Cyber Threat Intelligence

The Edwards College of Humanities and Fine Arts and the Gupta College of Science at Coastal Carolina University invite applications for a full-time assistant professor (tenure-track) position in Cyber Threat Intelligence (CTI). This is a joint position between the Departments of Intelligence and Security Studies and the Department of Computing Sciences. The Department of Intelligence and Security Studies will serve as the home department. For this position, CTI focuses on gathering, analyzing, and interpreting information about potential cybersecurity threats, enabling organizations to understand and mitigate risks.

The successful applicant will be appointed to a full-time, nine-month position beginning in August 2024.

Preference will be given to applicants with broad training and/or expertise in cyber security and intelligence topics who can spearhead the development of a new cyber threat intelligence focus within our university's curriculum. This effort will center on synthesizing the broad range of technical and human factors underlying computer networks and associated malign actors. As a result, the ability to offer courses in cybersecurity, programming, cyber threat intelligence, emerging technologies, and other areas of departmental needs is of particular interest. Professional experience in the field is welcome but not required.

Required Qualifications are an earned doctorate in cybersecurity, computer science, intelligence studies, or a closely related field (ABD will be considered if the defense is by August 2024).

Desired Qualifications:

- A record of excellence in university teaching, service, and consistent scholarly research;
- Potential for developing curriculum and other educational opportunities to support academic programming;
- A record of excellence in mentoring, supporting, and advising undergraduate students;
- Excellent oral and written communication skills;
- Experience in distance or online course delivery.

Information & Decision Sciences Department - Assistant Professor in Cybersecurity (2 Positions)
California State University, San Bernardino

Job No: 532043
Work type: Instructional Faculty - Tenured/Tenure-Track
Categories: Unit 3 - CFA - California Faculty Association, Tenured/Tenure-Track, Full Time, Faculty - Business/ManagementCalifornia State University, San Bernardino (CSUSB) is located in San Bernardino in the Inland Empire, 60 miles east of Los Angeles and operates a satellite campus in Palm Desert located in Coachella Valley. CSUSB serves approximately 20,000 students, of which 81% are first-generation college students and graduates about 5,000 students annually. As a designated Hispanic Serving Institution, CSUSB reflects the dynamic diversity of the region and has one of the most diverse student populations of any university in the Inland Empire, and the second highest Hispanic enrollment of all public universities in California. CSUSB employs 467 full-time faculty and offers 48 undergraduate, 35 graduate, and one doctoral degree programs and 14 academic programs with national accreditation.

At CSUSB, diversity, equity and inclusion are values central to our mission. We recognize that diversity and inclusion in all its forms are necessary for our institutional success. By fully leveraging our diverse experiences, backgrounds and insights, we inspire innovation, challenge the status quo and create better outcomes for our students and community. As part of CSUSB's commitment to hire, develop and retain a diverse faculty, we offer a variety of networking, mentoring and development programs for our junior faculty. We are committed to building and sustaining a CSUSB community that is supportive and inclusive of all individuals. Qualified applicants with experience in ethnically diverse settings and/or who demonstrate a commitment to serving diverse student populations are strongly encouraged to apply. CSUSB has received the Carnegie Community Engagement Classification, which recognizes CSUSB's ongoing commitment to service-learning, a high-impact practice that combines classroom instruction with meaningful volunteer service and correlates strongly to student success.

JOB SUMMARY

The IDS Department seeks two full-time assistant professors to join a growing and dynamic faculty team. CSUSB's cutting edge Cybersecurity program prepares students to address the cybersecurity issues and concerns faced today in many corporate and government environments. The foundation of our Cybersecurity program consists of imparting the skills required to succeed along with a combination of technical skills, policy, teamwork, ethics, and professionalism. In 2022, the Cyber program successfully renewed the NSA/DHS designation of Center of Academic Excellence in Cyber Defense (CAE-CD). Since receiving the CAE-CD designation, the program has secured a portfolio of $38m in grants and scholarships focused on cyber workforce.

The ideal candidate for this position must have knowledge, skill, and interest in teaching both undergraduate and graduate courses in Cybersecurity offered by the IDS Department at CSUSB main campus in San Bernardino and at Palm Desert. Candidates having a combination of both theory/research and applied/hands-on teaching experiences in the areas of Cybersecurity Management, Ethical hacking - SCADA/IOT, Forensics, Incident Response, and hold Industry recognized certifications such as Security+, CISSP, etc. are a plus.

The successful candidate will also be expected to advise students, serve on Department, College and University Committees, contribute to and participate in the life and strategic priorities of the IDS Department, and engage in the broader University disciplinary communities.

REQUIRED QUALIFICATIONS

- PhD in Cybersecurity or, a closely-related discipline by the time of appointment (ABD may be considered)
- Strong commitment to quality of student learning and program excellence
- Evidence of the ability or potential to work with a highly diverse student population.

Instructor or Assistant Professor of Cybersecurity, School of Computer Science & Information Systems

Employer
Northwest Missouri State University

Location
Maryville, Missouri (US)

Salary
Competitive

Posted Date
Feb 5, 2024

View more

Apply on website

Save Send job

Job Details Company

PRIMARY DUTY: A faculty position in the School of Computer Science and Information Systems at the Instructor level with the opportunity to lead or participate in Cybersecurity efforts for CAE-CD (Centers of Academic Excellent – Cyber Defense) for additional compensation.

ESSENTIAL FUNCTIONS:

1. Have a background in Cybersecurity or related field with the ability to teach cybersecurity undergraduate courses such as digital forensics, cryptography, secure systems administration, and ethical hacking
2. Participate in School activities including curriculum development and service activities
3. Work as a team on teaching and School activities
4. Deliver courses in traditional, as well as blended and online formats
5. Perform other duties as assigned

REQUIREMENTS for Instructor:

Education: Master's degree in Cybersecurity or related area

Experience: Experience in teaching in higher education at a regionally accredited institution or working full-time in cybersecurity-related field

Skills: Ability to teach undergraduate courses within the School; ability to conduct requisite service consistent with University practices

REQUIREMENTS for Assistant Professor (Tenure Track):

Education: Doctoral degree in Cybersecurity or related area

Experience: Experience in teaching in higher education at a regionally accredited institution or working full-time in cybersecurity-related field

Assistant Professor of Cybersecurity

Minnesota State University Moorhead
Moorhead, MN

Type: Full-Time
Posted: 07/06/2023
Category: Computer Science

Assistant Professor of Cybersecurity

Minnesota State University Moorhead

Hire Types: Faculty

Division: MSU Moorhead

Department: Academic Departments

Unit: College of Business, Analytics, and Communication209, IFO

Location: Moorhead, MN

FLSA: Exempt

Full/Part Time: Full Time

FTE: 1.0

Employment Condition: Limited

Work Shift:

Work Schedule/Hours/Days: This is a nine month fixed term position.

Posting Details: This position is covered by the IFO Master Agreement.

Salary Minimum: Please see page 36 of the agreement linked above

Salary Maximum: DOE

Salary Type: Annual

Bargaining Unit/Plan: 209, IFO

Job Description:

- Teach courses related to cybersecurity, computer science and Information Technology. The incumbent would be expected to teach courses that would include but are not limited to cybersecurity, computer science and Information Technology.
- Typical Teaching load is 24 credits (12 per semester)
- Instruct courses in varied locations, at varied times, and via various media commensurate with department and university needs.

- Provide evidence of continuing preparation and study in the field to enhance teaching abilities.
- Contribute to student growth and development including student advising.
- Support Minnesota State University Moorhead's strategic priority of creating a campus community that is diverse, inclusive, globally aware, and just.
- Other duties as defined by the collective bargaining agreement including:
  - Demonstrated ability to teach effectively and/or perform effectively in other current assignments.
  - Scholarly or creative achievement or research
  - Evidence of continuing preparation and study
  - Contributes to student growth and development
  - Service to the university and community

Required Qualifications:

- Earned doctorate in Cybersecurity/Computer Science or closely related field at the time of appointment or at least minimally the following ABD will be considered OR MS in Cybersecurity/Computer Science or closely related field at the time of appointment.
- Must meet Higher Learning Commission [HLC] faculty credentialing guidelines [e.g. have 18 graduate credit hours in the discipline the faculty is teaching].

Cybersecurity Center Director and Assistant

Harris-Stowe State University
Saint Louis, MO

Type: Full-Time
Posted: 12/11/2023
Category: IT Manager/Director

Job Title: Cybersecurity Center Director & Assistant Professor

Department: Anheuser-Busch School of Business

Reports To: Dean

Summary:

Harris-Stowe State University invites applications for the position of Cybersecurity Center Director & Assistant Professor. This is a unique opportunity for an experienced cybersecurity professional with a passion for academia to build and lead the university's Cybersecurity Center while contributing to the academic mission through teaching, research, and service.

Key Responsibilities:

Cybersecurity Center Leadership:

- Provide visionary leadership for the Cybersecurity Center, guiding its strategic direction and growth.
- Foster collaboration among faculty, students, and industry partners to enhance the center's impact on cybersecurity education, research, and outreach.
- Develop and maintain partnerships with industry, government agencies, and other academic institutions to advance the center's goals.

Teaching:

- Teach undergraduate courses in cybersecurity, ensuring high-quality instruction and student engagement.
- Contribute to curriculum development, staying abreast of industry trends and emerging technologies in cybersecurity.
- Mentor and advise students pursuing degrees and certifications in cybersecurity.

Research:

- Conduct and publish scholarly research in cybersecurity or related fields.
- Secure external funding through grants and partnerships to support research initiatives.
- Engage students in research activities and mentor them in research projects.

Service:

- Participate in departmental and university service activities, including committee work and academic program development.
- Contribute to the broader cybersecurity community through professional service and involvement in relevant organizations.
- Support the university's commitment to diversity, equity, and inclusion.

Cybersecurity Outreach:

- Organize and participate in outreach activities to promote cybersecurity awareness and education in the local community.
- Facilitate workshops, seminars, and conferences on cybersecurity topics.
- Serve as a resource and expert in cybersecurity for media inquiries and public engagements.

- PhD in Cybersecurity or related technical field preferred. Master's Degree in Cybersecurity, Computer Science, or a related field with industry certifications required.

Instructor of the Practice or Assistant Professor of Cybersecurity

Employer
Utah Tech University

Location
Utah, United States

Salary
Salary Not Specified

Start date
Nov 28, 2023

Apply on website

Save Send jo

View more

Position Announcement

The Department of Computing at Utah Tech University (UT) in St. George, Utah, invites applicants for a full-time professional-track Instructor of the Practice or tenure-track Assistant Professor of Cybersecurity, starting Fall Semester 2024. More information about the department, faculty, and its degree offerings can be found online at https://catalog.utahtech.edu/programs/computing/ .

Responsibilities

- Teach 24 credits (if tenure-track) or 30 credits (if professional-track) of lecture and laboratory courses in cybersecurity each academic year.
- Manage the cybersecurity club. Participate and encourage students to participate i hacking events and other related events.
- Participate in outreach events and help to build the program, recruit and retain students.
- Develop new courses in cybersecurity and help design new credentials and degree for students.
- Perform defined campus-wide duties including holding office hours, attending department, college, and division faculty meetings, and adhering to university polic and procedures.
- Perform institutional service and scholarship as defined by university policy and procedure (if tenure-track).
- Perform other duties as assigned.

Qualifications

- A bachelor's degree in Cybersecurity (or a closely related field) with industry experience will be considered for a one-year renewable appointment. A graduate degree will be required within 2 years of the start date in order to qualify for instructor status. Graduate degree preferred. PhD in cybersecurity (or related field) required for tenure-track professor appointment.
- Industry experience strongly preferred.
- Prior teaching experience preferred.
- Excellent communication and interpersonal skills, with a commitment to collegialit and teamwork.
- An interest in active learning, experiential learning and student engagement is desirable.

JOB DETAILS

Senior Cyber Security Analyst

Aditi Consulting • Contract • US, CA, Irvine • 11m ago

JOB DESCRIPTION:

Seeking a Senior Cyber Engineer to support our client in Irvine, CA. The contract is a comprehensive IT infrastructure initiative which aims to significantly improve the manner in which the Client's IT systems are operated, supported, and controlled. The Senior Cyber Engineer position is concerned with the Security Services Requirements section of this contract, providing technical leadership and oversight for the Security Operations Center (SOC). Services provided by the SOC are associated with (but not limited to) Security Information and Event Management (SIEM), incident response, Intrusion Detection and Prevention Systems (IDS/IPS), anti-virus and malware management, and firewall monitoring.

Duties and Responsibilities:

- Conducts research and evaluates technical and all-source intelligence with specific emphasis on network operations and cyber adversary tactics, techniques, and procedures.
- Conducts investigations into security incidents following defined Incident Response procedures, takes immediate measures to isolate the problem and minimize negative impact, follows escalation procedures as appropriate, creates post-incident reporting to include Root Cause Analysis.
- Analyzes network events to determine the impact on current operations.
- Correlates threat data from various sources.
- Develops and maintains analytical procedures to meet changing requirements and ensure maximum operational effectiveness.
- Implements secure operating systems, networks, security monitoring, tuning and management of IT security systems and applications, incident response, digital forensics, loss prevention, and eDiscovery actions.
- Performs risk and vulnerability assessments at the network, system, and application level.
- Develops and implements security controls and formulates operational risk mitigations along with assisting in security awareness programs.
- Involved in a wide range of security issues including architectures, firewalls, electronic data traffic, and network access.
- Utilizes COTS/GOTS and custom tools and processes/procedures to scan, identify, contain, mitigate, and remediate vulnerabilities, and intrusions.
- Performs analyses to validate established security requirements and recommends additional security requirements and safeguards.
- May support cyber metrics development and reporting.

Apply for this job

- BS in Cybersecurity or related technical field, 5+ years relevant industry experience.
- or MS in Cybersecurity or related technical field, 3+ years relevant industry experience.
- or PhD in Cybersecurity or related technical field with 0+ years relevant industry experience.

Apply on website

☆ Save ✉ Send

It's a great time to join Marymount University! We are looking for faculty and staff who are passionate about providing excellent service to ensure a high quality student experience and collaborative working environment.

Tenure-Track/Tenured Faculty Positions in the School of Technology in Computer Science,AI/Robotics, Information Technology or Related Fields (Assistant Professor, Associate Professor / Professor of Practice)

The Marymount University College of Business, Innovation, Leadership, and Technology (BILT) invites applications for two tenure-track positions within it School of Technology and Innovation to begin in Fall 2024. Positions are available at ranks of Assistant Professor –Tenure Track and Associate Professor/Professor of Practice in any of these areas: 1) Artificial Intelligence/Robotics, 2) Software Engineering, and 3) Cybersecurity. Successful candidates are expected to have a well developed research agen and a record of publishing in high quality journals. They will teach courses at

both graduate and undergraduate levels. Candidates should hold a Ph.D. in artificial intelligence/robotics, software engineering, cybersecurity, or other related fields. A candidate who is within the first year of achieving 'All but Dissertation' (ABD) status will be considered. Competitive salaries commensurate with experience will be offered to successful candidates.

George Mason University

research endeavors funded and associated with the NoVa Node of the Commonwealth Cyber Initiative and will collaborate with George Mason faculty as well as faculty from across the Commonwealth, especially those associated with the CCI Coastal Node and Old Dominion University. George Mason University and Old Dominion University have developed a strategic partnership and the incumbent will have access to faculty and facilities at both George Mason University and Old Dominion University to enable their success.

Research areas of specific interest to the CCI Nova Node include, but are not limited to, national defense, artificial intelligence (AI), quantum information processing and security, wireless communications, secure infrastructure e.g. transportation, smart buildings, Next G, power grid, security of manufacturing and supply chain, and impact of human behavior on cybersecurity among others. We are especially interested in faculty who conduct research in an interdisciplinary environment and who will collaborate with other CCI faculty, especially those in the NoVa and Coastal Nodes.

Responsibilities:

- Contribute to Mason's active cybersecurity research program, and laboratory and field portfolio of projects. Foster new and existing research collaborations with academic, industrial, and governmental institutions in Virginia and the greater Washington DC metropolitan area;
- Work collaboratively with faculty from across Virginia institutions to develop joint proposals and support research initiatives that advance Virginia's reputation as a global leader in cybersecurity; and
- Mentor students in cybersecurity and related disciplines and support the Department of Cybersecurity Engineering's educational initiatives.

Required Qualifications:

- Terminal degree (Computer Science, Computer Engineering, Cybersecurity, Information Technology, Systems Engineering, or a related field);

- Have an outstanding cybersecurity research record, as well as commitment to fostering interdisciplinary research/education; and
- Experience conducting cybersecurity research.

Type: Full-Time
Posted: 02/21/2024
Category: Computer Science

Job Number: REQ_0000052912

APPLICATION INSTRUCTIONS:

- **CURRENT PENN STATE EMPLOYEE (faculty, staff, technical service, or student), please** login to Workday **to complete the** internal application process**. Please do not apply here, apply internally through Workday.**
- **CURRENT PENN STATE STUDENT (not employed previously at the university) and seeking employment with Penn State, please** login to Workday **to complete the** student application process. **Please do not apply here, apply internally through Workday.**
- **If you are NOT a current employee or student, please click "Apply" and complete** the application process for external applicants**.**

JOB DESCRIPTION AND POSITION REQUIREMENTS:

Lecturer or Assistant Teaching Professor of Cybersecurity

Penn State Harrisburg in Harrisburg, PA

Apply on Institution's Website

inclusive learning environment for students and engage in scholarly and service activities supporting institutional goals. The School of Business is AACSB accredited. For more information about the technology programs at the business school please visit our website at http://harrisburg.psu.edu/business-administration.

This position is a term position and has a strong likelihood of renewal.

Responsibilities: The primary responsibilities of the Lecturer or Assistant Teaching Professor of Cybersecurity include:

Teaching: Specific job responsibilities include teaching undergraduate courses in cybersecurity, security, and risk analysis. Primary teaching areas include the following: digital networking and network security, cybersecurity and cyber forensics, security and malware analytics, and risk management. Secondary teaching areas could include th following: static and dynamic malware analysis, cyber defensive techniques, cybersecurity-related machine learning, programming skills (Java & Python), and database technology.

Research/Scholarship: Faculty are expected to maintain a high level of professional activity through scholarship and service.

Service: All faculty are expected to undertake committee work, community engagement, and mentorship, and make other contributions to the campus, to DEIB goals and initiatives, and to the broader academic community.

Qualifications: Preferred candidates will hold a doctorate in cybersecurity, Information Technology, or a related field with specialization in cybersecurity and network security. Candidates with a master's degree in cybersecurity Information Technology, or related field and security-related certifications (CISSP, CISM, CEH, OSCP, CCNA, etc.) are strongly encouraged to apply.

Director - Cybersecurity Center of Academic Excellence

Talladega College
Talladega, AL

Type: Full-Time
Posted: 11/28/2023
Category: Computer Science

Director - Cybersecurity Center of Academic Excellence
Department:Academic Affairs
Type:Full Time
Contact Name:Talladega College Office of Human Resources
Contact Email:hr@talladega.edu

Summary

Talladega College is seeking a Director for the Center of Academic Excellence in Cybersecurity. The Director acts as a primary liaison for building a strong partnership with industry, local communities, government agencies, and other Center of Academic Excellence (CAE) communities while providing oversight for grant writing, coordination of cyber trainings, and boot camps. This is an on-site position and will report to the Department Chair for Mathematics/Computer Science.

Essential Job Functions

- Oversee the operation of the cybersecurity center in collaboration with computer science faculty
- Provide oversight of the National Center of Academic Excellence in Cybersecurity (NCAE-C) designation requirements and summer programming
- Build relationships with external applicable industry businesses, clients and partners
- Work with other institutional colleagues to identify, write, and implement grants
- Collaborate with colleagues through strategic planning for the cybersecurity center including alignment of all cyber-related initiatives
- Plan and implement summer cyber camps and/or trainings (external and internal)
- Support faculty in the delivery of cybersecurity program
- Assist with necessary cybersecurity center upgrades
- Attend applicable external conferences and trainings, as needed
- Work with faculty and external partners in the development of departmental symposiums
- Work with faculty and students on institution-sponsored student competitions
- Assist in the preparation and monitoring of department budget and NCAE-C budget
- Teach undergraduate and graduate courses in cybersecurity and related field
- Perform other duties as assigned

Required Qualifications

- Earned doctorate from a regionally accredited institution
- Minimum three years of professional experience working in network systems or other related experience in cybersecurity
- Demonstrated experience or ability to effectively work with a wide range of individuals and constituencies in a diverse collegiate community and to cultivate an inclusive environment for students
- Excellent organizational, management, interpersonal, and communication skills

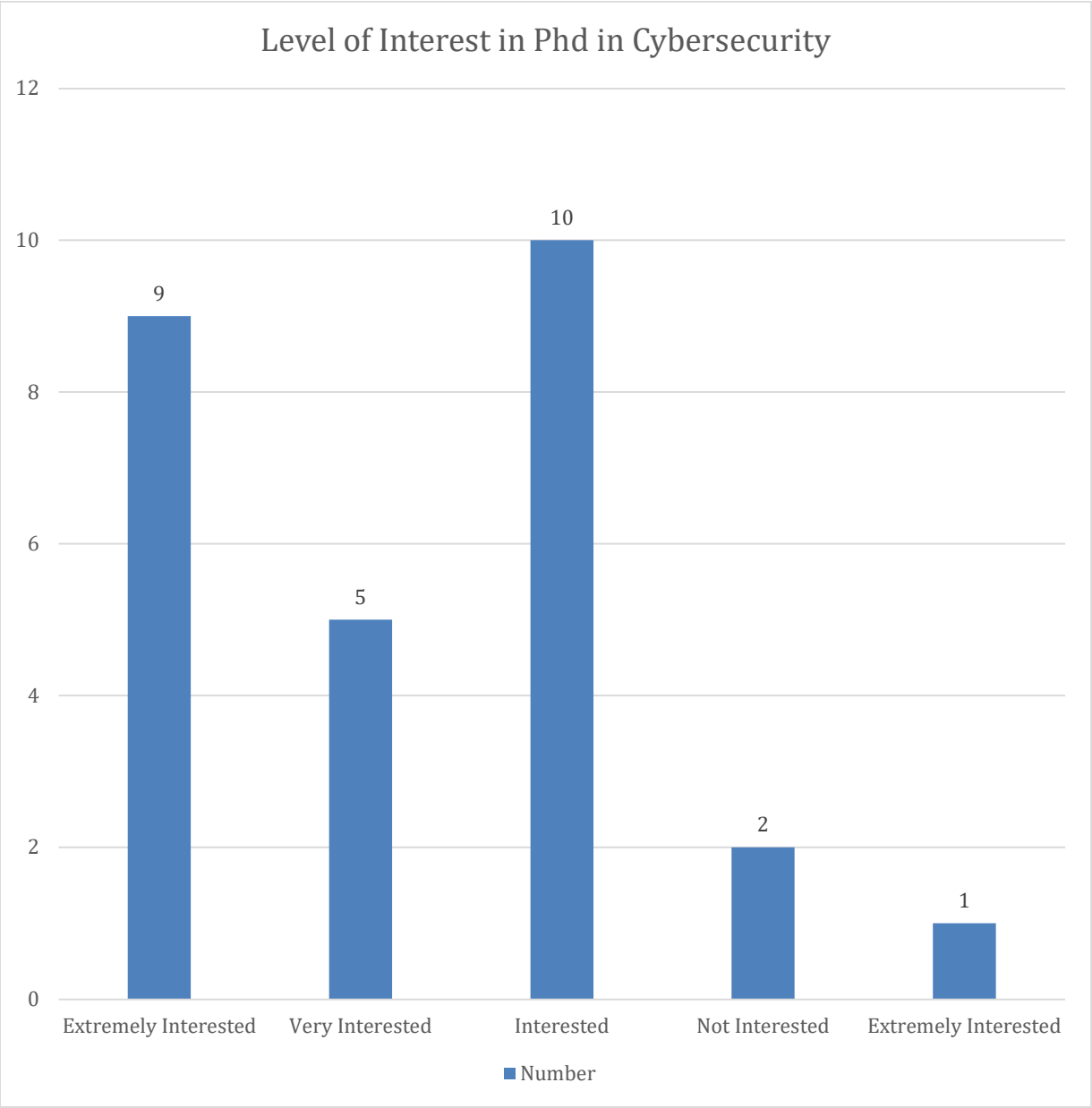
Preferred Qualifications

- Earned doctorate in cybersecurity/computer science or a related field of study

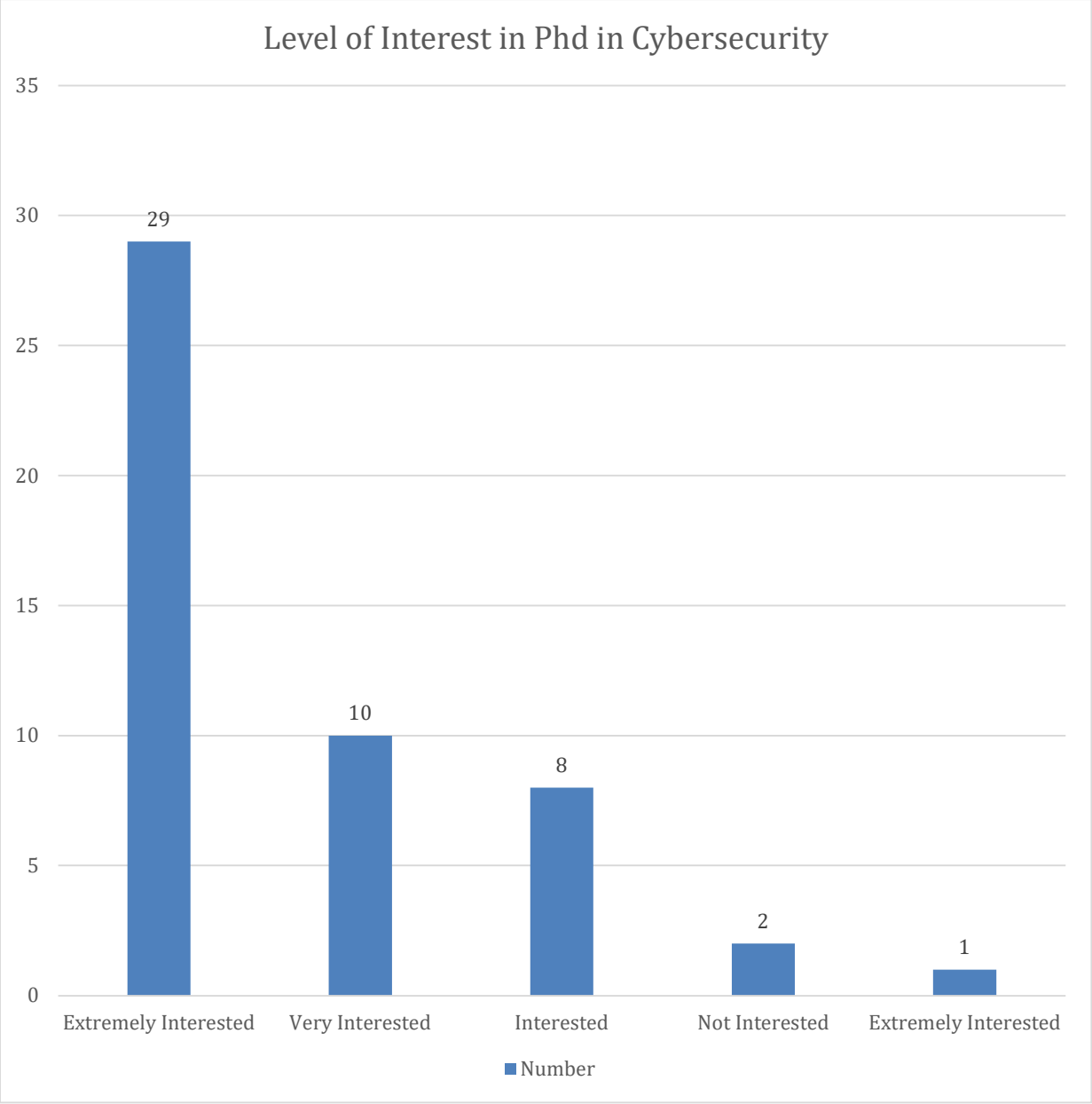
APPENDIX E - STUDENT DEMAND-STUDENT SURVEY

Demand Survey Results

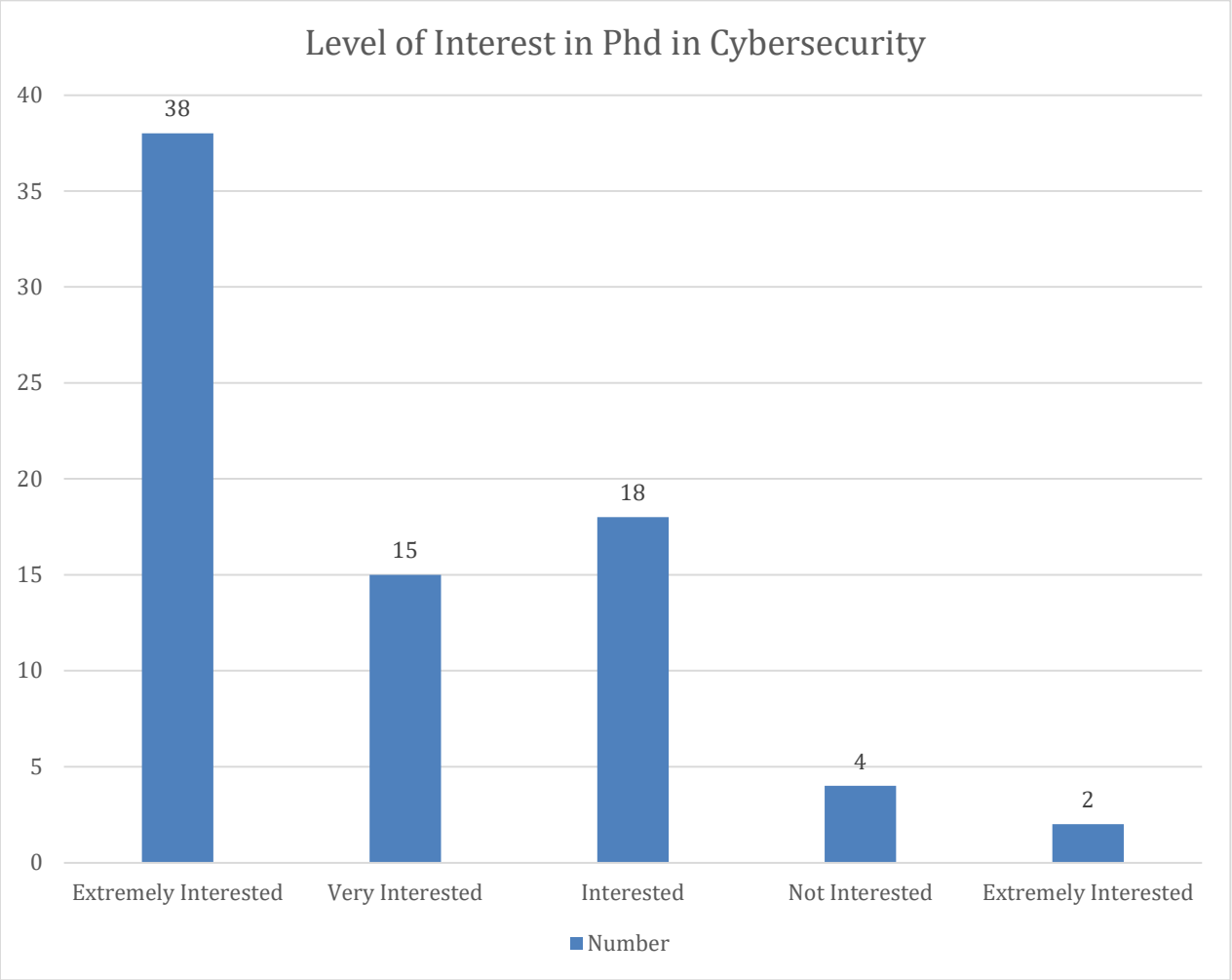
What is you level of interest in pursuing a Doctor of Philosophy in Cybersecurity degree? (Responses from cybersecurity seniors, n=27)



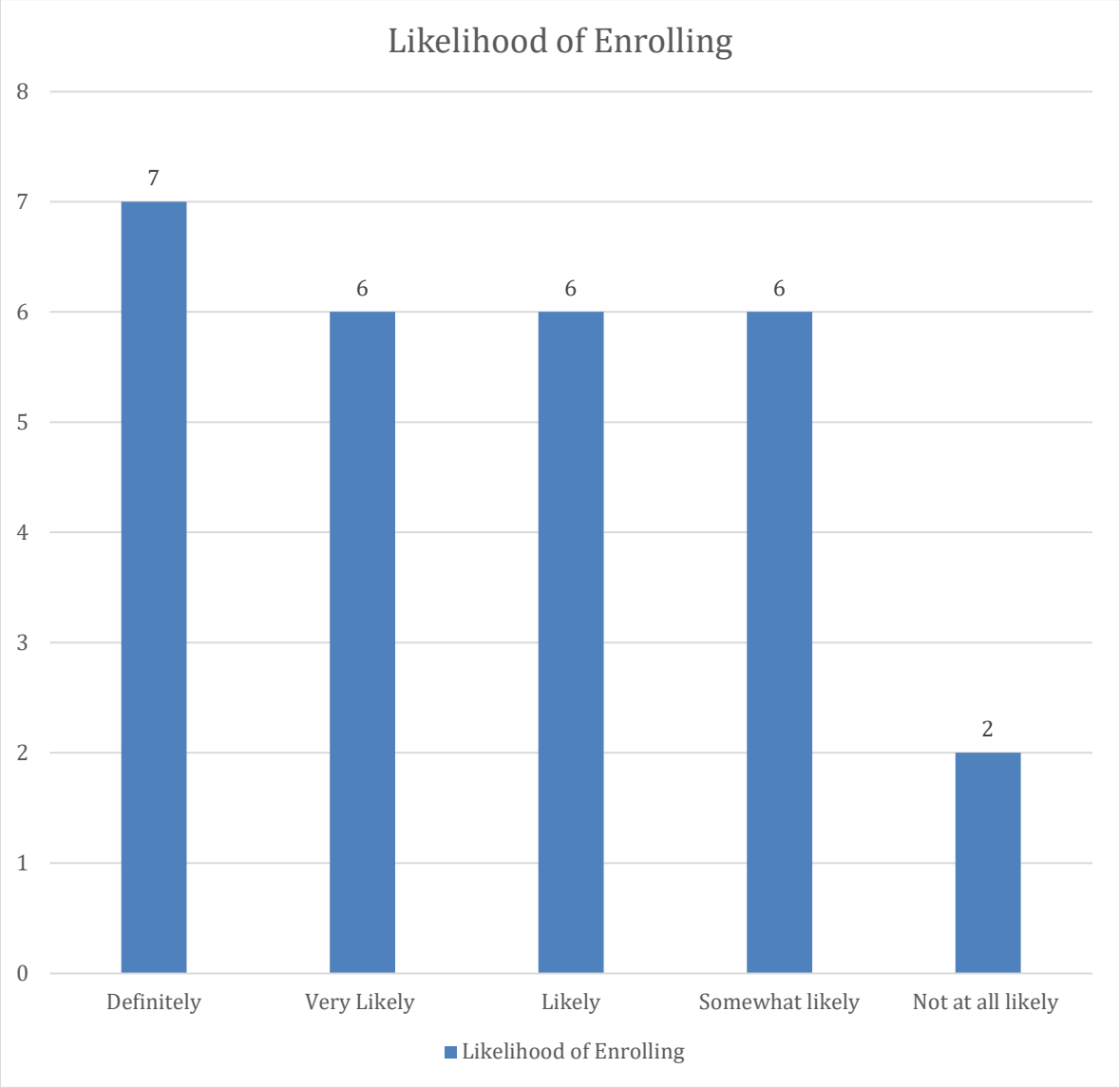
What is you level of interest in pursuing a Doctor of Philosophy in Cybersecurity degree? (Responses from Cybersecurity Masters students, n=50)



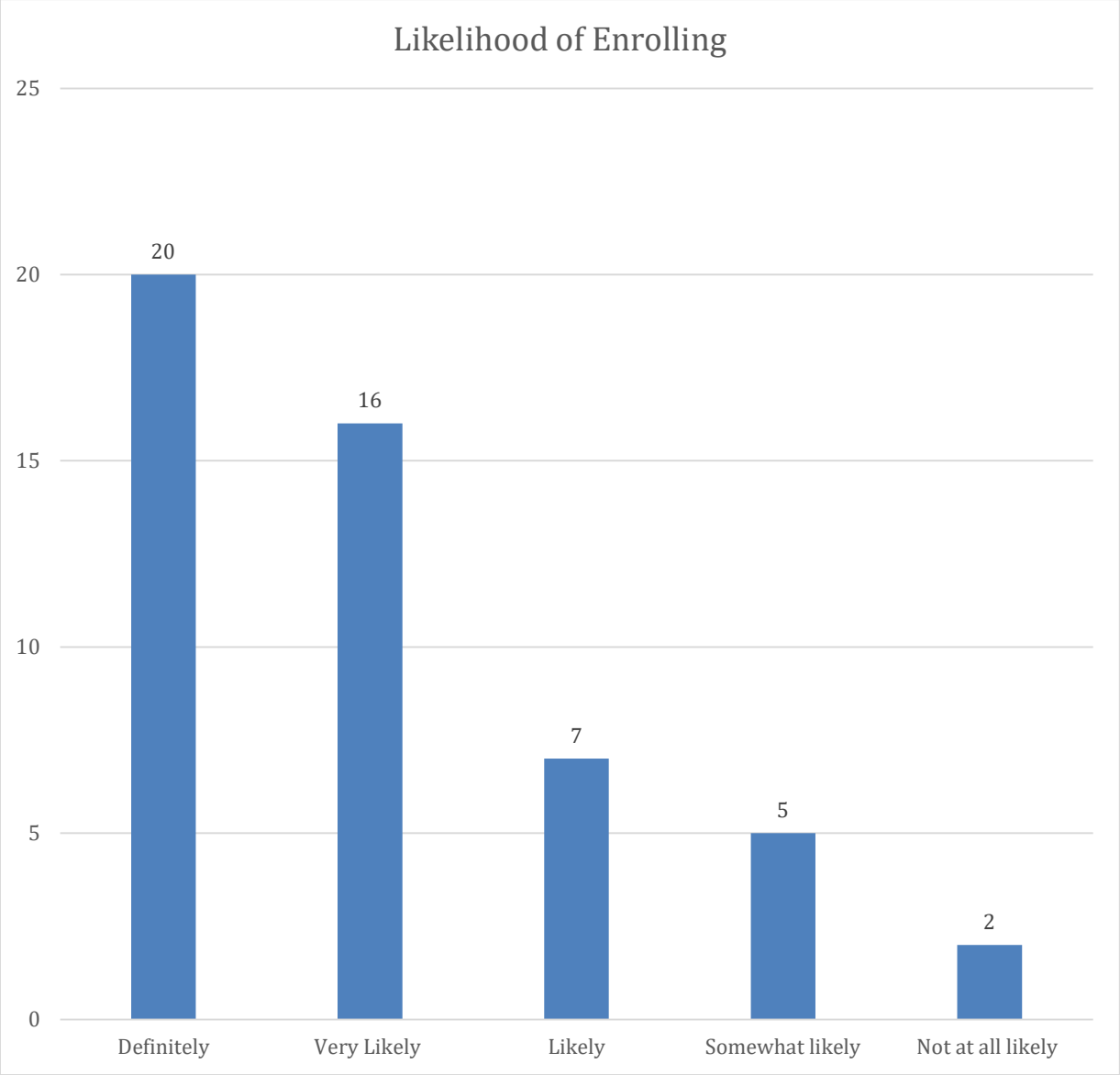
What is you level of interest in pursuing a Doctor of Philosophy in Cybersecurity degree? (Responses from all respondents, n = 77)



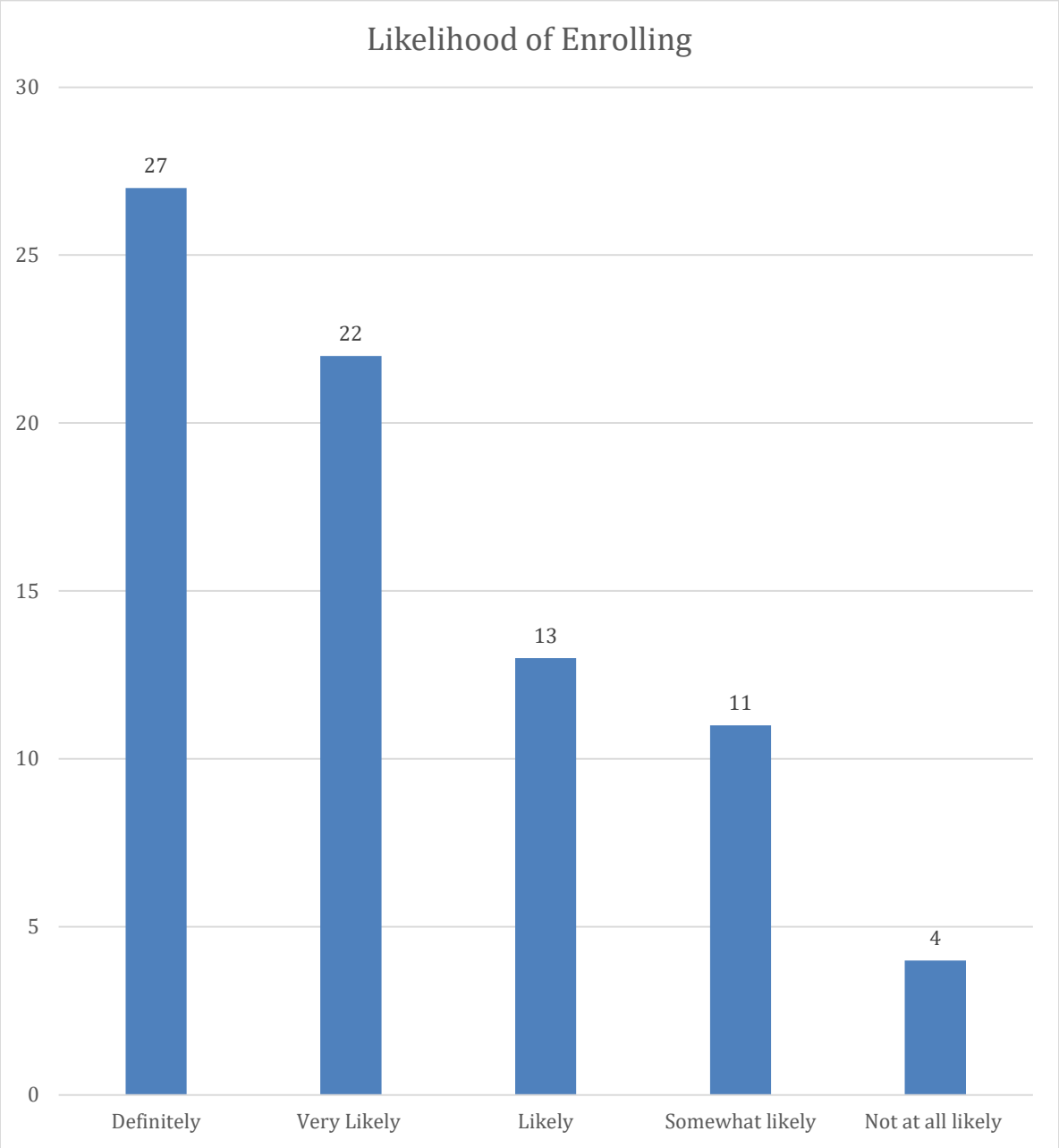
If ODU were to offer a Doctor of Philosophy in Cybersecurity, would you enroll? (cybersecurity seniors, n=27).



If ODU were to offer a Doctor of Philosophy in Cybersecurity, would you enroll? (cybersecurity Master's students, n=50).



If ODU were to offer a Doctor of Philosophy in Cybersecurity, would you enroll? (all cybersecurity respondents, n=77).



Summary Responses.

Q1 - What is your level of interest in pursuing a Doctor of Philosophy in Cybersecurity degree?

Field	Extremely interested	Very interested	Interested	Not interested	Extremely uninterested	Total
Undergrad	33% 9	19% 5	37% 10	7% 2	4% 1	27
Grad	58% 29	20% 10	16% 8	4% 2	2% 1	50
Total	49% 38	19% 15	23% 18	5% 4	3% 2	77

Q2 - If ODU were to offer a Doctor in Philosophy in Cybersecurity, would you enroll?

Field	Definitely	Very likely	Likely	Somewhat likely	Not at all likely	Total
Undergrad	26% 7	22% 6	22% 6	22% 6	7% 2	27
Grad	40% 20	32% 16	14% 7	10% 5	4% 2	50
Total	35% 27	29% 22	17% 13	14% 11	5% 4	77

Could you please comment on how this Doctor of Philosophy degree in Cybersecurity would fit with your current career or future career goals?

I am reaching retirement age, and I would like to teach at university after I retire from my current role.

I would love to continue to do Cybersecurity research and eventually have my own cybersecurity research company in which to be a reputable research company you need a PhD.

This doctorate degree would satisfy my goal of viewing cybersecurity from a multidisciplinary lens and the ability to apply what I learn to help solve problems using diverse perspectives/knowledge.

Having a Doctor of Philosophy degree in cybersecurity will make me more competitive when applying for jobs and give me an opportunity to teach cybersecurity as well.

I have a bachelors and masters degree completed already. I have also started a doctoral degree in a field that I am no longer sure I would like to finish the PhD within as I have become much more interested in cybersecurity in recent years, specifically due to salary, work-from-home/hybrid work options, and availability of advancement opportunities compared to my original field of study. I would love to earn my PhD in cybersecurity now and would appreciate if some of my 600-700-800 level coursework that I completed at ODU already would be considered towards this PhD, in order to shorten my timeline to graduation as well as cost of tuition.

The PHD program would help me as I gain more valuable knowledge in cybersecurity research, but also allow me the opportunity to work towards my goal as becoming a professor.

I'm currently working towards my bachelors in cybersecurity. I want to obtain higher education to open more doors and provide more opportunities for my future career.

I currently work of Lockheed Martin as a system admin for their F-22s. I plan on eventually moving up towards a position with homeland security or even NATO if the opportunity ever arose. Having a PHD in cyber would certainly help give me a much more in-depth perspective of cyber and slow me to stand out on a resume if compared to others applying to the same position I am.

I am currently enrolled in the MS in Cybersecurity program and graduated with a BS in cybersecurity from ODU as well. I currently work in the public sector as a cybersecurity analyst with hopes of transitioning to the private sector in the near future. I would love to continue my education at ODU, fostering newer relationships as well as building upon ones I have already created. Obtaining a PhD degree would provide an avenue to teach at a university after I have completed years of working in the industry to bring real world experience and connections to an institute of higher education.

Adding higher research and hands on skills to my resume in different sectors employers are seeking.

My ultimate career goal is to become a professor within the cybersecurity realm.

I really enjoyed the MS cyber program at ODU. Although, I want to continue my education in cybersecurity rather than computer science for phd. This will allow me further research opportunities and teaching opportunities. I also hope to work for CISA one day.

I have achieved a masters in cybersecurity and a bachelors in cybersecurity, I believe more research is necessary a essential to the field. I would love to contribute more research to the field.

A Doctor of Philosophy (Ph.D.) degree in Cybersecurity would greatly complement and enhance my current and future career goals in several ways:

- Expertise and Specialization: A Ph.D. in Cybersecurity would provide me with an in-depth understanding of advanced concepts, theories, and methodologies in the field. This specialized knowledge would allow me to become an expert in specific areas of cybersecurity, such as cryptography, network security, or digital forensics, aligning with my career aspirations.
- Research Skills: Pursuing a Ph.D. involves conducting original research and contributing new knowledge to the field. This experience would enhance my research skills, including problem-solving, critical thinking, and data analysis, which are highly valuable in any career related to cybersecurity. These skills would enable me to address complex security challenges and innovate solutions in both current and future roles.
- Leadership and Management: Completing a Ph.D. program requires leadership and project management skills to oversee research projects, collaborate with peers and faculty, and meet deadlines. These skills are transferable to leadership roles in cybersecurity, such as Chief Information Security Officer (CISO) or cybersecurity consultant, where the ability to manage teams and projects effectively is essential.
- Networking Opportunities: Engaging in a Ph.D. program would provide opportunities to network with leading researchers, industry professionals, and fellow students in cybersecurity. Building a strong professional network can open doors to collaboration, career opportunities, and knowledge exchange, enhancing both my current and future career prospects.
- Credential and Credibility: Earning a Ph.D. in Cybersecurity would enhance my credibility and establish me as a thought leader and subject matter expert in the field. This credential would differentiate me from other professionals and increase my value to employers, clients, and colleagues, facilitating career advancement and opportunities for growth.

APPENDIX F - UNSOLICITED EMAILS DEMONSTRATING DEMAND

From: [redacted] sabbe002@odu.edu
Date: Thursday, December 21, 2023 at 9:16 AM
To: Diaz, Rafael <RDiaz@odu.edu>
Subject: Cybersecurity Doctoral Program

Hello Mr. Diaz,

I would like to inquire and ask if there's a doctorate program for cybersecurity at Old Dominion University. I have searched through the website, and I don't see the option. Please let me know if there's a phd program for cybersecurity. I would very much like to take it.

Thank you!

From: [redacted] bmill026@odu.edu
Sent: Saturday, December 16, 2023 7:52 PM
To: Whitten, Jessica <jwhitten@odu.edu>
Subject: Question About PhD

Ms. Whitten,

Could you tell me if there is an online PhD program at ODU that I could do after completing my MS in Cybersecurity? I am currently looking at one at Dakota State University (Cyber Defense) and one at University of the Cumberlands (Information Technology). I'm leaning towards the latter, but I wouldn't mind continuing at ODU if there was an option that would fit.

Thank you! Hope you have a Merry Christmas!

--

[redacted] Bryon Miller

Cybersecurity Risk Management Certificate Student

From: [redacted] twood010@odu.edu
Date: Saturday, January 6, 2024 at 4:01 PM
To: Diaz, Rafael <RDiaz@odu.edu>
Subject: Cybersecurity Masters 2024 [redacted] Inquiry

Good afternoon Dr. Diaz!

I hope you're doing well! I am so excited to kick off this semester in my Masters program at ODU!

I wanted to let you know that I am thinking of continuing my education at ODU to obtain my P.hD degree in Cybersecurity.

For this reason, I have a few questions when you have a moment if you can answer, please.

Is there a p.hD at ODU for cybersecurity? If so, what is the duration of the degree?

Is the P.hD degree able to be accelerated? If so, what is the duration?

When do I apply for my p.hD at ODU? Regarding this, what are the requirements needed for me to apply to continue my education to obtain a p.hD?

What are the typical classes like such as syllabuses and the content that will be available?

Are all the Cybersecurity classes offered virtual?

Is there internship, or a project due to graduate with the P.hD?

I appreciate you taking time helping me during this process! I truly appreciate you & I cannot wait to continue my education and learn more!

I hope you're well and have a great day!

[redacted]

From: [redacted]
Sent: Monday, January 29, 2024 7:19 PM
To: Payne, Brian K. <bpayne@odu.edu>
Subject: Cybersecurity Doctoral Degree

Good evening, Mr. Payne:

It was a pleasure speaking with you and Ms. Pearson today. I've been speaking with an academic advisor about the doctorate of engineering with a concentration in cybersecurity. I know that would come later in my educational career, but I wanted to ask if you could provide an overview of the program. I know cybersecurity is constantly changing and evolving, and having a degree specializing in research and innovation would serve me well in the long run. In addition, I was informed by a faculty member that there have been talks about the possibility of adding a PhD program specifically for cybersecurity. Could you provide me an overview of what that program would look like should those plans come to fruition? I look forward to hearing from you!

Respectfully,
[redacted]