Issue AY17-01-C

FACULTY SENATE ISSUE FORM
Date Submitted: August 25, 2017
Title of Issue (a short descriptive title by which the issue may be referenced)
Proposed M.S. degree in cybersecurity
Description of Issue: The proposed M.S. program in cybersecurity is proposed to begin in fall 2018 and would be administered by the Center for Cyber Security Education and Research (CCSER) and the Graduate School. The CCSER also oversees an interdisciplinary undergraduate major in Cybersecurity, an undergraduate major in Cyber Operations, an undergraduate major in Cybercrime, as well as an undergraduate minor in Cybersecurity.
Rational for Submission: Within the region, ODU serves the professional educational needs of the: • Port of Virginia - the fastest growing port on the east coast with a vibrant and economically robust maritime industry; • Two major railroads; • One hundred and sixty four international businesses representing 28 countries; • Numerous federal facilities and military bases. This significant infrastructure represents a mosaic of assets and makes Hampton Roads particularly vulnerable to malicious cyber attacks. ODU is ideally and strategically located for hosting the MS cybersecurity program and is poised to train the next generation of cybersecurity professionals. To facilitate the mission of developing a pipeline of industry-ready cyber talent, the university has recently made substantial investments in the area of cybersecurity. The Center for Cyber Security Education and Research (CCSER) was established in March 2015. It reports directly to the Office of Academic Affairs and consists of about 30 affiliated faculty and staff from across the university, including four colleges (Arts & Letters, Sciences, Engineering and Technology, and Business) and the Virginia Modeling, Analysis and Simulation Center (VMASC). These entities and faculty possess significant expertise in cybersecurity education and research. Moreover, the CCSER has recently hired four full-time tenured/tenure-track faculty and a post-doctoral research associate who teach cybersecurity courses and conduct fundamental cybersecurity research.

Senate issue 17-01: Proposed MS program in Cyber Security

Committee C recommends approval of the revised proposal to establish a new MS in Cyber Security. Faculty to support the program as well as many of the required courses are in place and the Graduate School is lending support to ensure its success.

Name: Judy Bowman, submitted on behalf of Austin Agho
Department: Academic Affairs
Date: August 25, 2017
Signature:
For Faculty Senate Use Only
Assigned to Committee:
Date Assigned:

OLD DOMINION
UNIVERSITY
IDEA FUSION

August 18, 2017

Dr. Monica Osei
Assistant Director for Academic Affairs and Student Programs
State Council of Higher Education for Virginia
101N. 14th Street, 10th Floor, James Monroe Building
Richmond, VA 23219

Dear Dr. Osei:

Enclosed is a draft proposal for a Master of Science in Cybersecurity. I'm happy to answer any questions you may have about this program.

I look forward to hearing back from you about the proposal.

Sincerely,

Jeanie Kline, Ed.D.
Office of Academic Affairs

Office of Graduate Studies
2019 Koch Hall, Norfolk, VA 23529
Phone: 757/683-4885 • Fax: 757/683-5499 • www.odu.edu/graduatestudies • officeofgradstudies@odu.edu

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 Master of Science	6. Term and year of initiation Fall 2018
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 Fall 2019	9. Date approved by Board of Visitors
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 The Center for Cyber Security Education and Research School(s) or college(s) of The Graduate School Campus(es) or off-campus site(s) _____ Mode(s) of delivery: face-to-face _____ distance (51% or more web-based) ___X___ hybrid (both face-to-face and distance) _____	
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. Jeanie Kline, Ed.D., SCHEV Liaison, 757.683.3261, jkline@odu.edu	

PROPOSAL FOR
THE MASTER OF SCIENCE IN CYBERSECURITY
TABLE OF CONTENTS

Description of the Proposed Program

Program Background

Old Dominion University (ODU) seeks approval to initiate a Master of Science in Cybersecurity, scheduled to begin fall 2018 in Norfolk, Virginia. This proposed program will be administered by the Center for Cyber Security Education and Research (CCSER) and the Graduate School. The CCSER also oversees an interdisciplinary undergraduate major in Cybersecurity, an undergraduate major in Cyber Operations, an undergraduate major in Cybercrime, as well as an undergraduate minor in Cybersecurity.

Cybersecurity focuses on protecting computers, networks, programs, and data from attack, destruction or unauthorized access. It is of growing importance due to the increasing reliance on computer systems and networks. The information technology revolution is transforming every facet of society, empowering people to embrace new ways of completing daily tasks and transforming how they network, create social identities, build relationships and stay informed.[1] Approximately 87% of the U.S. population uses the Internet daily.[2] According to surveys by Accenture, 82% of executives believe digital technologies are erasing industry limitations and allowing paradigms to emerge.[3] Moreover, there is a remarkable proliferation of networked intelligent devices - collectively known as the Internet of Things (IoT). The IoT is a digitization of the physical world that has come about through embedding physical devices with electronics, sensors, actuators, and network connectivity that enable them to collect and exchange data and be controlled remotely. It presents vast opportunities for organizations to improve efficiencies, gain a competitive advantage, and build new business models. More IoT devices are coming online each and every day. Experts estimate that the IoT will grow to more than 50 billion devices by 2020.[4]

While the computer and network technologies, including the Internet, wireless networks, data centers, personal computers, smart phones, and the emerging Internet-of-Things, are embraced as important tools for efficiency and productivity, a wide spectrum of organizations, ranging from government and military agencies to financial and medical corporations, collect, process, store, and transmit across networks unprecedented amounts of sensitive data, which are becoming an increasingly attractive target for cybercriminals. In the recent years, cyber-attacks are becoming 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 surging demand for a well-trained cybersecurity workforce to safeguard information relating to national security, health and financial records, and various sensitive business and personnel data.

---

[1] "Digital Adoption", Accenture, https://www.accenture.com/t20170203T031808_w_/us-en/_acnmedia/PDF-42/Accenture-Digital-Adoption-Report.pdf.

[2] "13% of Americans don't use the internet. Who are they?", Pew Research, 2016, http://www.pewresearch.org/fact-tank/2016/09/07/some-americans-dont-use-the-internet-who-are-they/

[3] Accenture Technology Vision, 2016, https://www.accenture.com/us-en/insight-technology-trends-2016

[4] CISCO, "Cisco IoT System Security: Mitigate Risk, Simplify Compliance, and Build Trust," 2015.

This proposed MS in Cybersecurity program is designed to help prepare technology leaders who will fill the demand for highly skilled cyber security specialists and practitioners. It will prepare its graduates for high-level positions, working in a wide variety of capacities to protect the information systems of different types of organizations and to secure the nation's cyber infrastructure. Students will be educated to develop skills and competencies in the technical aspects of cyber security with proficiency in a diversity of current and emerging cyber security technologies, and will be prepared to assume responsibility for the management of cybersecurity systems and coordination of cyber operation teams.

Rationale for the Program at Old Dominion University

Old Dominion University is strategically located for many of its traditional undergraduate and graduate degrees in computer science, computer engineering, information technology, and modeling, simulation and visualization. The city of Norfolk, within Hampton Roads, is home to the largest natural deep-water harbor in the world. Norfolk is also home to the world's largest naval station, supporting 75 ships and 134 aircraft alongside 14 piers and 11 aircraft hangars. Within the region, ODU serves the professional educational needs of the:

- Port of Virginia - the fastest growing port on the east coast with a vibrant and economically robust maritime industry;
- Two major railroads;
- One hundred and sixty four international businesses representing 28 countries;
- Numerous federal facilities and military bases.

This significant infrastructure represents a mosaic of assets and makes Hampton Roads particularly vulnerable to malicious cyber attacks. ODU is ideally and strategically located for hosting the MS cybersecurity program and is poised to train the next generation of cybersecurity professionals. To facilitate the mission of developing a pipeline of industry-ready cyber talent, the university has recently made substantial investments in the area of cybersecurity. The Center for Cyber Security Education and Research (CCSER) was established in March 2015. It reports directly to the Office of Academic Affairs and consists of about 30 affiliated faculty and staff from across the university, including four colleges (arts & letters, sciences, engineering and business) and the Virginia Modeling, Simulation and Analysis Center (VMASC). These entities and faculty possess significant expertise in cybersecurity education and research.

Moreover, the CCSER has recently hired four full-time tenured/tenure-track faculty and a post-doctoral research associate who teach cybersecurity courses and conduct fundamental cybersecurity research. In addition, ODU is the lead on a Regional Alliances and Multi-stakeholder Partnerships to Stimulate (RAMPS) grant from the National Institute for Standards and Technology (NIST). The funded project, HRCyber, brings together more than two dozen partners to coordinate the development of cyber workforce that responds to the needs of the Hampton Roads region. Thus, the proposed Master of Science in Cybersecurity will effectively complement the cybersecurity programs at ODU by offering an advanced degree to meet the surging demand for well-trained professionals who can fill senior cybersecurity positions.

Mission

The Master of Science in Cybersecurity is supportive of the mission of Old Dominion University in that it "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 degree aligns with this mission by: (1) expanding the pipeline for a cybersecurity workforce and providing students with the expertise to perform senior cybersecurity jobs in the U.S. and around the world; (2) offering educational opportunities to early- and mid-career professionals in cybersecurity fields; (3) providing advanced students with the background necessary to continue their graduate studies for a doctoral degree that focuses on cybersecurity; (4) strengthening ODU's commitment to contributing to the economy and workforce of the Hampton Roads region and the Commonwealth of Virginia; and (5) enhancing the brand awareness of ODU's cybersecurity program worldwide.

Online Delivery

Students who are enrolled in master's degrees are often simultaneously holding down a full-time job and juggling personal responsibilities. The proposed master's degree program would be online, offering students the flexibility to complete coursework on their own time.

Students enrolled in the MS in Cybersecurity will be able to access course materials utilizing Blackboard, the University's course management system. All assignment submissions and other course management actions take place in Blackboard. Further, faculty-student interaction is available via email, phone, in-person meetings, and WebEx-interface meetings.

Faculty members who teach in the web-based format are trained in course development and delivery through the Center for Learning and Teaching (CLT). 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. 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 24 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. Online students can remotely connect to the lab facility to conduct various real-world cybersecurity experiments. It will effectively enrich 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.

Old Dominion University has a thirty-year history of delivering robust academic programming through a variety of technologies. In 2014, the University shifted the vast majority of distance learning programs and courses from a satellite and site-based delivery to a fully online delivery. Over 14,000 degrees have been conferred to students who have been enrolled in ODU's distance learning programs. According to the 2015-2016 Senior Student Satisfaction Survey, 96% of these distance learning students reported that they were satisfied or very satisfied with their ODU experience. It is ranked #2 among Online Colleges in Virginia, according to College Affordability Guide, 2017.[5]

Advisory Board

An advisory board consisting of industry leaders and employers will be formed to advise faculty and to ensure the proposed program is aligned with emerging cybersecurity areas that are relevant to career growth among students.

Old Dominion University will leverage the Hampton Roads Cybersecurity Education, Workforce and Economic Development Alliance (HRCyber) in establishing the board. HRCyber is a partnership among educational institutions, government agencies, nonprofit organizations, and private employers focused on developing educational pathways to provide a capable and fully trained cybersecurity workforce for the region. HRCyber aligns regional educational and skills development offerings with the workforce practices and activities of business and nonprofit organizations within the Hampton Roads region, with the specific goal of supporting local economic development and job growth via establishment of a multi-stakeholder alliance. The alliance focuses on leveraging the National Initiative for Cybersecurity Education (NICE) Framework, addressing cyber workforce needs, training providers conforming to the NICE Framework, and increasing the pipeline of students pursuing cybersecurity careers.

Current membership on HRCyber is available in Appendix A. Several of them have written in support of the proposed program, and will be asked to join the advisory board at ODU.

Admissions Criteria

Criteria for acceptance into the Master of Science in Cybersecurity include the following:

- Online graduate 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 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
- GRE scores, with a 50% or better attainment on quantitative reasoning

[5] http://www.collegeaffordabilityguide.org/

- Current scores on the Test of English as a Foreign Language (TOEFL) of at least 550 from applicants whose native language is not English (waived if an applicant has earned a college degree from an institution in an English-speaking country)

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

The primary candidates for the Master of Science in Cybersecurity are those with managerial career goals in the cybersecurity industry. Other candidates will be those in the U.S. Army, Navy, Air Force, and other branches of the military, individuals working for federal, state, or local government or for government contractors, and international and U.S. students who wish to gain advanced expertise in cybersecurity. Ultimately, the proposed program is designed to produce professionals with the knowledge and experiences necessary to handle the daily challenges in protecting critical cyber infrastructure and assets, and the leadership skills to fill senior cybersecurity positions.

In addition, Old Dominion students enrolled in the interdisciplinary undergraduate major in cybersecurity, the undergraduate major in cyber operations, the undergraduate major in cybercrime, as well as students in undergraduate computer science, computer engineering, information technology, and criminal justice programs who enrolled in the minor in cybersecurity may be keenly interested in the link between their undergraduate program and this proposed program. For many, it will represent a natural progression, particularly if they are currently working in, or have plans to work in, the cybersecurity field.

Curriculum

The M.S. in Cybersecurity is a 30-credit hour program that has been designed to address the advanced educational needs of students and employers in the area of cybersecurity. It will educate students about the theory, technologies, skills, and practices necessary to handle the daily challenges in protecting critical cyber infrastructure and assets. Students will be introduced to many advanced topics of cybersecurity, including information assurance, networked systems security, software reverse engineering, digital forensics, mobile and wireless security, ethical hacking and penetration testing, threat modeling and risk analysis, cybersecurity law and policy, and leadership and management in cybersecurity.

The curriculum will feature emerging topics in the field, and will include many opportunities for students to interact with potential employers through recruitment and networking events. Students will learn how to identify problems, gather information, analyze data, define hypotheses, develop solutions, establish contingencies, and effectively articulate and communicate results. This advanced knowledge will build upon the basic cybersecurity foundation acquired at the undergraduate level or in experiences gained in the industry.

Moreover, extensive studies have revealed the value of interdisciplinary underpinnings of cybersecurity. The field covers more than technical issues; it covers an interdisciplinary approach to cybersecurity matters by incorporating aspects of economics, human psychology, law, policy, and other disciplines. Generally, cybersecurity professionals are interdisciplinary in nature. They typically go through diverse education and career pathways. Few of them have ever earned a cybersecurity degree. To this end, the proposed master's program would have an interdisciplinary curriculum and be administered by the interdisciplinary Center for Cyber Security Education and Research (CCSER). An array of restricted elective courses across multiple disciplines will be offered such that students could choose elective courses based on their different backgrounds, interests, current employment, and future career goals.

This proposed program consists of four core courses (12 credit hours), five electives (15 credit hours), and one capstone course (3 credit hours). The four core courses 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.

The five electives provide students with opportunities to learn about different aspects of cybersecurity, e.g., in information systems, network systems, mobile and wireless systems, operating systems, and cyber-physical systems. Courses are also offered to address such important cybersecurity topics as reverse software engineering, digital forensics, thread modeling, and ethical hacking and penetration testing.

The capstone course, in students' final semester of study, provides opportunities to synthesize knowledge from their previous coursework and apply it to solve real-world cybersecurity problems. The faculty member who teaches the capstone course will work with industrial and academic partners who will serve as external mentors of the capstone course. Each student in the capstone course will discuss—with both faculty member and mentor—development of her/his master's project that aims to solve a cybersecurity problem in a real-world business setting. Students will learn how to quickly gather information, understand the business system, identify problems, define hypotheses, develop solutions, analyze data, and effectively articulate and communicate ideas and results. The capstone course also offers the chance for students to develop design thinking in cyber security and exercise leadership in a team environment.

The project counts 40% of the total grade of the capstone course. The faculty member who teaches the capstone course will be responsible for grading the project. If a student fails the project, he/she may still pass the course by working with the faculty member to improve selected aspects of the project. Requirements for the Master of Science in Cybersecurity include:

*New course

<u>Foundational Core Courses (12 hours)</u>

*CYSE 600	Cybersecurity Principles	(3 credits)
*CYSE 601	Advanced Cybersecurity Techniques and Operations	(3 credits)
*CRJS/CYSE 603	Advanced Cybersecurity Law and Policy	(3 credits)
*CYSE 605	Leadership and Management in Cybersecurity	(3 credits)

Restricted Elective Courses (15 hours), to be selected in consultation with program advisor. Up to three courses can be selected at 500 level.

CS 565	Information Assurance	(3 credits)
CS 564	Networked Systems Security	(3 credits)
CS/*CYSE 595	Software Reverse Engineering	(3 credits)
*CYSE 607	Advanced Digital Forensics	(3 credits)
*CYSE 615	Mobile and Wireless Security	(3 credits)
*CYSE 625	Advanced Ethical Hacking and Penetration Testing	(3 credits)
ECE 516	Cyber Defense Fundamentals	(3 credits)
ECE 519	Cyber Physical Systems Security	(3 credits)
ENMA 517	Secure and Trusted Operating Systems	(3 credits)
ENMA 670	Foundations of Cyber Security	(3 credits)
IT 649	Information Systems and Network Security	(3 credits)
MSIM 670	Cyber Systems Engineering	(3 credits)
MSIM 673	Threat Modeling and Risk Analysis	(3 credits)
*CYSE 697	Independent Study in Cybersecurity	(3 credits)
MSIM 773	Networked System Security	(3 credits)

Capstone Core Course (3 hours)

*CYSE 698	Master's Project	(3 credits)

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

Student Retention and Continuation Plan

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

- Requiring an orientation session for all new students, which introduces the program, curriculum, requirements, expectations, faculty, facility, and other relevant resources that are online or remotely accessible through the myODU portal;
- Publishing an up-to-date curriculum and a long-range course schedule to help students plan their enrollment and time to completion;
- Holding advising sessions each semester and providing personalized advising throughout students' program of study;
- Teaming with faculty and industrial partners to mentor students in subject matter and career direction; and
- Encouraging students to join ODU's Cybersecurity Student Association, which hosts meetings regularly for students to share success stories, talk about strategies to complete the program and discuss future career pathways.

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

- Additional advising and mentoring of the student;
- Connecting to a successful local cybersecurity professional as role-model;
- Involvement in state-of-the-art cybersecurity projects to stimulate student's interest; and
- Creating a cohort to increase interactions and peer learning.

To remain in good standing after admission to the program, students must maintain a minimum, cumulative grade point average of 3.0 in all graduate course work attempted at the University. Students who fall below this minimum standard will have 12 credit hours to remedy this deficiency. The graduate program director will work with such students to success, to the degree possible.

Faculty

Ten faculty members affiliated with CCSER hold credentials to teach in the Master of Science in Cybersecurity. They hold tenure or tenure-track positions in four colleges, including the College of Arts and Letters (Sociology and Criminal Justice; Philosophy and Religious Studies), Strome College of Business (Information Technology & Decision Science), Batten College of Engineering and Technology (Electrical and Computer Engineering; Engineering Management and Systems Engineering; Modeling, Simulation and Visualization Engineering), and College of Sciences (Computer Science).

The group includes 3 professors, one of whom serves as the director of CCSER, 4 associate professors and 3 assistant professors. Three of them were recruited recently through ODU's cybersecurity cluster hiring.

The faculty offer a diversity of cybersecurity expertise, 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 90 recent publications (during the past three years) in peer-reviewed journals and conferences in cybersecurity fields. They currently have 15 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, and Department of Energy.

The faculty will work collaboratively to teach the core courses and to mentor students in the proposed program. Brief CVs for existing full time faculty members can be found in Appendix D. Appendix E provides data on grant funding faculty have successfully obtained in this field.

Program Administration

This proposed program would be administered by the Center for Cybersecurity Education and Research (CCSER) and the Graduate School. CCSER was established under the Office of Academic Affairs to weave together disparate threads of programmatic and facility resources at

ODU to create a strong education and research program focusing on cybersecurity. It represents an interdisciplinary effort bringing together faculty, staff, degree programs, certificates, and research initiatives from four colleges, eight academic departments, the Office of Research, the Office of Information Technology Services, and the Virginia Modeling, Analysis and Simulation Center. It consists of about 30 affiliated faculty and staff from across the university. The CCSER also oversees an interdisciplinary undergraduate major in cybersecurity, an undergraduate major in cyber operations, an undergraduate major in cybercrime, as well as an undergraduate minor in cybersecurity.

A tenured CCSER faculty would be appointed as the graduate program director (GPD). She or he will assume responsibility for setting class schedules, coordinating student meetings and activities, gathering students' input, handling students' concerns, providing admission and enrollment information to the Graduate School, and meeting with the faculty, the CCSER director, and dean or associate dean of Graduate School to discuss program matters. He or she will also have teaching responsibilities in the program. A graduate committee, to include the graduate program director and other faculty members at CCSER, will be formed to review applicants for admission, evaluate curriculum in meeting student and employer needs, and conduct regular program assessments.

The administrative assistant in CCSER will support faculty and students in this program.

Student Assessment

Students will be evaluated throughout the program using formative assessments, such as quizzes, tests, cases studies, papers, research project, and presentations. Student learning outcomes cover many of the technical and management competencies that are required for the area of cybersecurity. Specifically, graduates will be able to:

1. Analyze ethical and social issues in the area of cybersecurity to clearly understand ethical standards and rules for cybersecurity professionals and to promote social responsibility;
2. Communicate in writing their understanding of cybersecurity problems and decisions about cyber defense and operations in a cohesive and well-structured manner;
3. Integrate principles and methods from a variety of disciplines to develop and implement best practices to solve cybersecurity complexities;
4. Analyze global cybersecurity problems and make decisions that enhance the effectiveness of cyber defense and operation solutions based on these analyses; and
5. 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.

Map of MS in 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 clearly understand ethical standards and rules for cybersecurity professionals and to promote social responsibility	CYSE 600. Cybersecurity Principles CRJS/CYSE 603. Advanced Cybersecurity Law and Policy	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) CRJS/CYSE 603 • 80% of students will successfully present and debate on alternative methods to accomplish ethics in the cybersecurity industry. (Presentation)
2. **Written Communication** Communicate in writing their understanding of cybersecurity problems and decisions about cyber defense and operations in a cohesive and well-structured manner.	CYSE 600. Cybersecurity Principles CYSE 601. Advanced Cybersecurity Techniques and Operations	CYSE 600 • 80% of students will design a cyber defense plan for a campus network (Research paper) • 90% of students will use cybersecurity principles to analyze vulnerabilities of a given computer system (Exam) 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)

3. Analytical Problem Solving Integrate principles and methods from a variety of disciplines to develop and implement best practices to solve cybersecurity complexities	CYSE 601. Advanced Cybersecurity Techniques and Operations CYSE 698. Master's Project	CYSE 601 • 80% of students will perform a thorough analysis of cybersecurity vulnerabilities in mobile wireless networks. (Group project, presentation, paper) CYSE 698 • 90% of students will solve a cybersecurity problem in a real-world business setting: gather information, understand business systems, analyze data, identify problems, define hypotheses, develop solutions, and articulate and communicate results. (Project, presentation, and report).
4. Global Perspective Analyze global cybersecurity problems and make decisions that enhance the effectiveness of cyber defense and operation solutions based on these analyses	CYSE 600. Cybersecurity Principles CYSE 605. Leadership and Management in Cybersecurity	CYSE 600 • 80% of students will conduct a thorough case study of the global impact of a cyber attack. (Project, presentation and report) CYSE 605 • 90% of students will correctly answer questions about international cybersecurity management. (Exam)
5. Oral Communication Orally communicate their understanding of cybersecurity, and explain decisions in cohesive and well-structured presentations to both technical and non-technical audience	CYSE 605. Leadership and Management in Cybersecurity CYSE 698. Master's Project	CYSE 605 • 90% of students will design a cybersecurity management plan and present it as a group leader. (Presentation) CYSE 698 • 90% of students will articulate cybersecurity problems in a business setting, communicating next steps to technical and non-technical audiences (Project, oral communication and presentation)

Workplace Competencies and Employment Skills

Graduates of the Master of Science in Cybersecurity will have the skills and ability needed for employment and workplace competencies in the field of cybersecurity. Specifically, they will have the:

1. Ability to manage the security complexities present in a wide range of cyber systems, from clouds to the Internet-of-Things
2. Awareness and knowledge of contemporary cybersecurity standards, practices, procedures and methods
3. Understanding of vulnerabilities in common computer systems and networks
4. Strong analytical and diagnostic skills for cyber system risks and vulnerabilities and their economic impacts
5. Demonstrated skills in innovation and collaboration
6. Ability to clearly articulate complex cybersecurity concepts, problems and solutions both written and verbally
7. Presentation and communication skills to effectively communicate with colleagues, management and customers
8. Ability to examine security from a holistic view, including threat modeling, specifications, implementation, testing, vulnerability assessment, and human factors
9. Ability to lead teams for cyber defense and operations

Program Assessment

The program will be assessed by faculty and administrators in CCSER, the Graduate School, and the provost's office. The review will be completed annually in the fall starting from the second year after the program is approved, 2019, 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;
- Curriculum 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 Academic Affairs for review. The Vice Provost will offer guidance, as needed, for improvement, and will provide updates about the review to the Provost.

Old Dominion University maintains a robust program review process for graduate programs; as such, this master's program will have an internal review conducted by external faculty after five years (i.e., in fall of year 6 or 2023). This review will include a self-study, a visit from faculty external to the program, and an action plan developed in concert with the graduate program director, program faculty, and dean and associate dean of Graduate School.

Benchmarks of Success

Benchmarks of success for the Master of Science in Cybersecurity include the following student enrollment and graduate goals:

- 20-30 new students will be admitted each year
- The program will graduate a minimum of 12 students annually by the completion of the program's fourth 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 one year 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
- 80% of employers will be satisfied with the level of education and skill of graduates, as measured by an employer survey administered within one year of hire.

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

The proposed program does not represent an expansion of a concentration or focus area at the master's level at Old Dominion University.

Relationship to Existing ODU Degree Programs

Old Dominion University has no related degree offering in the area of this proposed program at the master's level.

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 fast-growing field creating new jobs over the next decade, as both government and industry make significant 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.

Former national intelligence director, James Clapper, noted that cyber attack ranks highest on worldwide threats to U.S. national security.[6] According to Department of Homeland Security, "The federal enterprise depends on information technology (IT) systems and computer networks for essential operations. These systems face large and diverse cyber threats that range from unsophisticated hackers to technically competent intruders using state-of-the-art intrusion techniques. Many malicious attacks are designed to steal information and disrupt, deny access to, degrade, or destroy critical information systems."[7]

[6] http://www.washingtontimes.com/news/2015/feb/26/james-clapper-intel-chief-cyber-ranks-highest-worl/
[7] https://www.dhs.gov/topic/securing-federal-networks

IBM Corporation's Chairman, CEO and President, Ginni Rometty, said that cybercrime may be the greatest threat to every company in the world.[8] According to an analysis conducted by Cybersecurity Ventures, the global annual cybercrime costs has been estimated at $3 trillion in 2015, and it could reach $6 trillion by 2021.[9] Global spending on cybersecurity products and services for defending against cybercrime is projected to exceed $1 trillion cumulatively over the next five years, from 2017 to 2021, according to the Cybersecurity Market Report, which is published quarterly by Cybersecurity Ventures.[9]

Cyber-attacks not only impact national security and the economy, but also affect individuals personally in their daily lives. For example, in July 2015, hackers stole social security numbers, health records, and other highly sensitive data from 21 million Americans through the Office of Personnel Management in what, at the time, was the largest data breach in U.S. history.[10] In 2017, malware WannaCry affected more than 230,000 users in some 150 countries.[11]

As the volume and sophistication of cyber-attacks grow, there is a surging demand for well-trained cybersecurity workforce to safeguard the cyber space. Dr. Ronald Dodge from the United States Military Academy and Drs. Costis Toregas and Lance Hoffman from The George Washington University noted in their article that "The cybersecurity workforce is one of the most critical employment sectors in the world."[12]

However, recent studies have shown that there is a serious shortage of talent to fill cybersecurity positions. According to a study conducted by Information Systems Audit and Control Association (ISACA), a global leader in cybersecurity, "82 percent of organizations expect to be attacked, but they are relying on a talent pool they view as largely unqualified and unable to handle complex threats or understand their business. More than one in three (35 percent) are unable to fill open positions."[13] According to International Information System Security Certification Consortium's, or (ISC)²'s, Global Information Security Workforce Study, which queried 19,000 cybersecurity professionals worldwide, 66% of survey respondents feel they do not have enough employees to address the increasing level of threats coming their way.[14]

Based on a global survey of 649 cybersecurity and IT managers or practitioners, only 16% feel at least half of their applicants are qualified; 53% say it can take as long as six months to find a

---

[8] https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#5f8e8fcb3a91

[9] http://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

[10] "U.S. Government Cybersecurity Report", 2016, SecurityScorecard R&D Department, https://cdn2.hubspot.net/hubfs/533449/SecurityScorecard_2016_Govt_Cybersecurity_Report.pdf

[11] "How the WannaCry Attack Will Impact Cyber Security", May 2017, http://knowledge.wharton.upenn.edu/article/massive-global-cyberattack/

[12] Ronald C Dodge, Costis Toregas and, Lance Hoffman, "Cybersecurity Workforce Development Directions", in Proceedings of The Sixth International Symposium on Human Aspects of Information Security & Assurance, 2012.

[13] "State of Cybersecurity: Implications for 2015", An ISACA and RSA Conference Survey, http://www.isaca.org/cyber/Documents/State-of-Cybersecurity_Res_Eng_0415.pdf

[14] "Cybersecurity Faces 1.8 Million Worker Shortfall By 2022", http://www.darkreading.com/careers-and-people/cybersecurity-faces-18-million-worker-shortfall-by-2022/d/d-id/1329084

qualified candidate; and more than a third are left with job openings they cannot fill.[15] According to ESG's annual IT spending intentions research based on 600 IT and cybersecurity professionals, cybersecurity has been identified as the number one "problematic shortage" area across all of IT for the past six years in a row. In 2017, 45% of organizations say they have a "problematic shortage" of cybersecurity skills.[16]

Given the high demand for this cybersecurity workforce and the serious shortage of cybersecurity talent, the proposed program is aimed at filling the gap. While a bachelor's degree in a related field is required for almost all cyber security positions from entry-level and higher, many cybersecurity positions require advanced education and experience. The proposed online interdisciplinary graduate program gives students additional technical, theoretical, leadership, managerial and business skills required in high-level cybersecurity positions. It is on the cutting edge of supporting the growing government and industry demand for qualified cybersecurity professionals. Specific justification related to the proposed graduate degree include the following:

- An advanced degree opens up career options. A report by Burning Glass Technologies showed that 23% of cyber security postings require at least a master's degree.[17] There are high-level job openings in almost every state and across almost every sector, both private and public. For example, right now, approximately 65% of large U.S. companies have a CISO (Chief Information Security Officer) position, up from 50% in 2016, according to the Information Systems Audit and Control Association (ISACA), an independent, nonprofit, global association. Cybersecurity Ventures predicts that 100% of large companies globally will have a CISO position by 2021.[18] The skills and experiences gained through the advanced degree in cybersecurity open up vast opportunities for long-term career advancement.
- Most cybersecurity bachelor's programs focus on fundamental technical knowledge. As part of the master's program, students will be exposed to advanced technologies and leadership skills, along with managerial training. They will learn how to lead and manage teams of IT professionals, including cybersecurity personnel. The proposed program will offer essential knowledge and skills for cybersecurity professionals to advance in their careers and land those senior positions.
- Cybersecurity professionals are well paid, with information assurance specialists averaging $75,000 annually. Further, those with a master's degree have the potential to earn more; for example, an information security manager averages $100,000 a year and a chief information security officer earns about $145,000 annually.[19]

Thus, obtaining a master's degree in cybersecurity is highly desired by professionals in the field. Faculty members at ODU anticipate that graduates of the program will be highly sought-after by employers across the nation and from local organizations and governments in Hampton Roads.

---

[15] http://www.isaca.org/About-ISACA/Press-room/News-Releases/2015/Pages/Study-82-percent-of-Organizations-Expect-a-Cyberattack-Yet-35-percent-Are-Unable-to-Fill-Open-Security-Jobs.aspx
[16] http://www.csoonline.com/article/3177374/security/cybersecurity-skills-shortage-holding-steady.html
[17] "Job Market Intelligence:Cybersecurity Jobs", http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf
[18] http://cybersecurityventures.com/jobs/
[19] https://news.clearancejobs.com/2016/02/01/8-reasons-to-get-your-masters-degree-in-cybersecurity/

Employment Demand

National/International Focus

The cybersecurity unemployment rate was 0% in 2016, and it is expected to remain there from 2017 to 2021. U.S. News and World Report ranked a career in information security analysis seventh on its list of the 10 best technology jobs for 2017.[20] Further, "The field of cyber security is the least populated of any field of technology," according to John McAfee, founder of McAfee, Inc. "There are two job openings for every qualified candidate."[21]

The high demand for cybersecurity talent has been reported by multiple sources:

- According to CyberSeek, a project supported by the National Initiative for Cybersecurity Education (NICE), a program of the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce, the U.S. employs nearly 780,000 people in cybersecurity positions in 2017, with approximately 350,000 current cybersecurity openings.[21]
- Burning Glass Technologies, an analytics software company powered by the world's largest and most sophisticated database of labor market data, reports that cybersecurity openings are growing three times faster than overall IT postings.[22]
- According to the Bureau of Labor Statistics, the rate of growth for jobs in information security is projected at 18% from 2014–2024, much faster than the average for all other occupations.[23]
- Michael Brown, CEO at Symantec, the world's largest security software vendor, estimates that the demand for cybersecurity professionals is estimated to reach 6 million globally by 2019.[24]
- The ISACA, a non-profit information security advocacy group, predicts there will be a global shortage of two million cyber security professionals by 2019.[8]
- Cybersecurity Ventures predicts there will be 3.5 million unfilled cybersecurity positions globally by 2021.[24]

Virginia Focus

Cybersecurity is among Governor McAuliffe's top priorities for building the New Virginia Economy. There are approximately 36,000 cybersecurity job openings in Virginia – the 2nd highest among all states and the highest in terms of demand concentration.[25]

---

[20] "Best Technology Jobs", U.S. News, https://money.usnews.com/careers/best-jobs/rankings/best-technology-jobs

[21] http://www.csoonline.com/article/3201974/it-careers/cybersecurity-job-market-statistics.html

[22] http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf

[23] https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

[24] http://www.csoonline.com/article/2953258/it-careers/cybersecurity-job-market-figures-2015-to-2019-indicate-severe-workforce-shortage.html

[25] http://cyberseek.org/heatmap.html

"At a time when Virginia is home to 36,000 open jobs in the cybersecurity sector, we must do everything we can to encourage students to enter this growing industry," said Governor Terry McAuliffe at an event to announce the recipients of the Commonwealth's first Cybersecurity Public Service Scholarship. "Our problem in Virginia, unlike other states, is we have too many open jobs, high-paying jobs we cannot fill in Virginia today. Standing here today I have 36,000 cyber jobs open. I tell (students) the starting pay is $88,000," McAuliffe said in another event, "We either fill these jobs or they go to other states."

In May, 2015 over 7,500 job openings for cyber-security related occupations were advertised through the Virginia Employment Commission. The number of persons employed in this occupational group in the Commonwealth is expected to increase by 25% from 2012 through 2022. [26]

In May, 2015 over 7,500 job openings for cyber-security related occupations were advertised through the Virginia Employment Commission (VEC). The number of persons employed in this occupational group in the Commonwealth is expected to increase by 25% from 2012 through 2022.[27] The VEC indicated that jobs in this field, such as Information Security Analysts, are abundant. As of August 16, 2017, there were 519 openings for Information Security Analysts and fewer than 100 candidates seeking these positions.[28]

Hampton Roads Focus

The Hampton Roads area includes organizations that are keenly interested in this program. Letters of support from several of these employers may be found in Appendix F.

A survey will be conducted among employers with results of the survey are found in Appendix G.

Appendix H contains current job descriptions and position announcements demonstrating a need for prospective employees with the knowledge that this degree program would provide.

Student Demand

A student/alumni survey will be conducted with results of the survey available in Appendix I.

Following the administration of this survey, xx students offered unsolicited letters of interest in the program. Their letters may be found in Appendix J.

---

[26]http://www.yesvirginia.org/Content/pdf/Industry%20Profiles/VA%20Cybersecurity%20Summary%202016.pdf

[27]http://www.yesvirginia.org/Content/pdf/Industry%20Profiles/VA%20Cybersecurity%20Summary%202016.pdf

[28]https://data.virginialmi.com/vosnet/lmi/occ/occsummary.aspx?enc=Vdx1uREThVt4ZXZqIde02x70XpslwN0fJQZHOtORsY0Kpt0r4ot0R85Y5htQjKgPOWJFjC/JGcHVA5YNAJtky6oiKJcV2AzDM0wrIEHXLQ=

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)**		
2018 - 2019		2019 - 2020		2020 - 2021		2021 - 2022			2022 - 2023		
HDCT	FTES	HDCT	FTES	HDCT	FTES	HDCT	FTES	GRAD	HDCT	FTES	GRAD
15	10	25	15	34	28	45	34		50	35	12

Assumptions
Retention: 90%
Part-time students: 60% / Full-time students: 40%
Full-time students credit hours per semester: 12
Part-time students credit hours per semester: 6
Full-time students graduate in 1.5 years
Part-time students graduate in 2.5 years

Duplication

Several master's degree programs are offered in the Commonwealth of Virginia that cover areas similar to the proposed program.

George Mason University (GMU)
George Mason University (GMU) offers a Master of Science in Information Security and Assurance.

Similarities to ODU
One of the three required core courses of the Master of Science in Information Security and Assurance at GMU is ISA 562, Information Security Theory and Practice. The content of the course includes some areas covered in an ODU's core course, CYSE 600, Cybersecurity Principles.

Differences from ODU
The other two core courses in the GMU program are heavily network related, including a course about computer communications and another course about network security. In contrast, the ODU program includes a broad coverage of cybersecurity ranging from cyber operations to cyber laws, policies, and leadership skills. It covers both technical aspects and human factors in cybersecurity.

The GMU program is computer science oriented, housed in the Department of Computer Science, whereas the ODU program takes an interdisciplinary approach, with the courses taught by interdisciplinary faculty from four different colleges.

The GMU program does not include a capstone course, while the ODU program requires a capstone that will focus on a master's project to solve a cybersecurity problem in a real-world business setting. Finally, the GMU program is offered in a traditional format, whereas the ODU program will be available in an online format, with the option for local students to attend classes on campus.

George Mason University also offers a Master of Science in Management of Secure Information Systems and an Executive Master of Business Administration (EMBA) in Critical Infrastructure Protection and Management, through the School of Business. The former focuses on business management aspect of information security. It is run as a cohort with no electives. The entire program has a duration of 16 months including about seven days of study abroad. The latter addresses the analysis and management within critical infrastructure sectors. Its curriculum includes 17 required EMBA courses.

Similarities with GMU M.S. in Management of Secure Information Systems
The GMU program includes a 2-credit course, Foundations of Cyber Security (MSEC 510). The content of the course is partially covered in an ODU's core course, CYSE 600, Cybersecurity Principles. It also includes a 2-credit course, Leadership and Change Management, which includes some areas covered in the ODU's core course, CYSE 605, Leadership and Management in Cybersecurity.

Differences from GMU M.S. in Management of Secure Information Systems
The GMU program is business management oriented, including a variety of courses that focus on enterprise, finance, and management. The proposed M.S. in Cybersecurity has a different goal and target population. It focuses on cybersecurity technologies, covering advanced cybersecurity principles, techniques, and operations, as well as various important cybersecurity topics such as reverse software engineering, digital forensics, thread modeling, and ethical hacking and penetration testing. It aims to produce technical leaders who can take senior cybersecurity positions in a wide range of federal, state and local governments, military agencies, and the private sector, including various senior engineering positions such as cyber security engineers, cyber security architects, and cyber security analysts, that need different skill sets than those taught in the M.S. in Management of Secure Information Systems offered by the School of Business at George Mason University.

Similarities with GMU EMBA in Critical Infrastructure Protection and Management
The content of EMBA 718, Leadership & Change Management, is partially covered in an ODU's core course, CYSE 605, Leadership and Management in Cybersecurity.

Differences from GMU EMBA in Critical Infrastructure Protection and Management
This GMU EMBA program emphasizes business/government coordination to achieve business efficiency, ensure business continuity, and develop capacities to create resilience and

competitive advantage. The program includes 7 modules of EMBA courses. None of them focus on cybersecurity technologies. On the other hand, the ODU program aims to prepare students with deep understanding of cybersecurity technologies and become technical leaders in the field. It covers advanced cybersecurity principles, techniques, and operations, and provides students with opportunities to learn about a diversity of cybersecurity topics such as reverse software engineering, digital forensics, thread modeling, mobile wireless security, and ethical hacking and penetration testing.

Norfolk State University (NSU)
Norfolk State University (NSU) offers a Master of Science in Cybersecurity through the Department of Computer Science.

Similarities with NSU program
The NSU program includes 11 foundation courses, which are all required. One of the courses is CSC 535, Computer Security I. The content of the course is partially covered in an ODU's core course, CYSE 600, Cybersecurity Principles. In addition, the NSU program includes CSC 555, Management of Information Security, which has some areas covered in the ODU's core course, CYSE 605, Leadership and Management in Cybersecurity.

Differences with NSU program
The NSU program has no electives, whereas the proposed ODU program offers 5 elective courses that allow students to learn different aspects of cybersecurity, e.g., in information systems, network systems, mobile and wireless systems, and cyber-physical systems. The elective courses also cover important cybersecurity topics such as reverse software engineering, digital forensics, thread modeling, and ethical hacking and penetration testing.

The ODU program stresses real-world hands-on experience. It includes a lab-based class CYSE 601, Advanced Cybersecurity Techniques and Operations. Moreover, every course in the curriculum involves extensive hands-on activities.

The ODU program emphasizes leadership in cybersecurity, aiming to educate the next generation of technical leaders in the field. The NSU program does not include a course for leadership skills, which is essential for cybersecurity professionals to advance in their careers.

The NSU program is housed in the Computer Science Department, whereas the ODU program takes an interdisciplinary approach. It would be administrated by the interdisciplinary Center for Cybersecurity Education and Research, and the courses would be taught by faculty from four different colleges.

Virginia Commonwealth University (VCU)
Virginia Commonwealth University (VCU) offers a Master of Science in Computer and Information Systems Security through the Department of Computer Science.

Similarities with VCU program
One of the six required core courses of the Master of Science in Computer and Information Systems Security at VCU is CISS/INFO 644, Principles of Computer and Information Systems

Security. The content of the course is partially covered in an ODU's core course, CYSE 600, Cybersecurity Principles. Another VCU core course CISS 634, Ethical, Social and Legal Issues in Computer and Information Systems Security, is similar to an ODU core course CRJS/CYSE 603, Advanced Cybersecurity Law and Policy.

Differences with VCU program

The VCU program has no capstone course, whereas the proposed ODU program includes a required capstone, i.e., a master's project that focuses on solving real-world cybersecurity problems. The faculty member who teaches the capstone course will work with industrial and academic partners who will serve as external mentors of the capstone course. Students will learn how to gather information, understand the business system, identify problems, define hypotheses, develop solutions, analyze data, and effectively articulate and communicate ideas and results.

The VCU program does not include a course about leadership skills, which is essential for cybersecurity professionals to advance in their careers and take senior technical positions. The ODU program emphasizes leadership. It includes a core course CYSE 605, Leadership and Management in Cybersecurity, in order to train the next generation of technical leaders in the field of cybersecurity.

The VCU program is computer science oriented, offered by the Department of Computer Science, whereas the ODU program is based on an interdisciplinary framework. It would be administrated and taught by faculty from different colleges and departments.

Finally, the VCU program is offered in a traditional format, whereas the ODU program will be available online and at the same time allow local students to attend classes on campus.

It is also worth pointing out that the combined graduates of these relevant programs are far behind the workforce demand, which is estimated about 36,000 in the Commonwealth of Virginia.

Enrollment and number of graduates for these programs include the following:[29,30]

GMU	2012-13	2013-14	2014-15	2015-16	2016-17
-MS Info Security and Assurance Enrollments	98	73	78	66	54
-MS Info Security and Assurance Graduates	41	24	32	26	
-MS Mgmt of Secure Information Enrollments	27	19	18	32	21
-MS Mgmt of Secure Information Graduates	27	16	19	29	

[29] http://research.schev.edu/enrollment/E16_report.asp
[30] http://research.schev.edu/Completions/C1Level2_Report.asp

-EMBA Enrollments	86	95	72	72	69
EMBA Graduates	32	39	25	27	
NSU					
-MS Cybersecurity Enrollments				14	49
-MS Cybersecurity Graduates					
VCU					
-MS Computer and IT Sys Security Enrollments	12	12	14	21	16
-MS Computer and IT Sys Security Graduates	6	3	5	5	

Projected Resource Needs for the Proposed Program

Projected Resource Needs

The Center for Cyber Security Education and Research (CCSER) and Old Dominion University have sufficient resources to launch and sustain the proposed program. Specifically, faculty members who have expertise in cybersecurity have been teaching both graduate and undergraduate courses for a number of years. This program successfully presents a graduate degree that provides robust information to students who wish to obtain a credential focused on cybersecurity. It will not compromise existing programs; in fact, it is designed to enhance the breadth of programs in the university.

Full-Time Faculty
No faculty member at the university will have a teaching load that is solely devoted to the proposed program. Each faculty member teaches in undergraduate and graduate programs, as well as general education assignments for their respective departments.

Part-Time Faculty
Ten faculty members at the university, who are affiliated with the CCSER, will teach part-time loads in the proposed program. Combined, they will account for 1.5 FTE faculty when the program is launched. By the target year, the combined part-time faculty members will account for 4.0 FTE faculty. The average salary among these faculty members for 1 FTE is $110,000 plus fringes of $40,810.

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

Graduate Assistants
Two part-time graduate assistants will be required to launch and sustain the program. The cost of each position is $16,000 in salary for two semesters, a total of $32,000 plus FICA in the amount of $2,448.

Classified Positions
A classified person—administrative assistant—who supports CCSER will assist with this program. This person will devote approximately ¼ time to the program, or $7,500 in salary and $2,783 in fringe benefits.

Targeted Financial Aid
No targeted financial aid is projected in launching and operating the program.

Library
No new library resources are required to launch and sustain the program. The University Libraries have adequate resources to support this program from the time it is launched to the target year. Appendix L provides details related to these holdings.

Telecommunications
No new telecommunication equipment or software is needed to launch or sustain the program. With one new faculty member to be hired, an office with a computer and phone are in place.

Equipment (including computers)
No new equipment or related resources are needed to initiate and sustain this proposed program. Computer and peripherals, in addition to a phone, are in place.

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

Other Resources (specify)
No resources other than those described above will be required to launch or operate the proposed Master of Science in Cybersecurity.

PROJECTED RESOURCE NEEDS FOR PROPOSED PROGRAM

Part A: 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

Part B: Fill in the number of FTE and other positions needed for the program

	Program Initiation Year 2018-2019		Expected by Target Enrollment Year 2022-2023	
	On-going and reallocated	**Added (New)**	**Added (New)*** **	**Total FTE positions**
Full-time faculty FTE*				0.00
Part-time faculty FTE**	1.50		2.50	4.00
Adjunct faculty				0.00
Graduate assistants (HDCT)	2.00			2.00
Classified positions	0.25			0.25
TOTAL	3.75	0.00	2.50	6.25

*Faculty dedicated to the program. **Faculty effort can be in the department or split with another unit.

*** Added **after** initiation year

Part C: Estimated resources to initiate and operate the program

	Program Initiation Year 2018- 2019		Expected by Target Enrollment Year 2022- 2023	
Full-time faculty	0.00	0.00	0.00	0.00
salaries				$0
fringe benefits				$0
Part-time faculty (faculty FTE split with unit(s))	1.50	0.00	2.50	4.00
salaries	$165,000		$275,000	$440,000
fringe benefits	$61,215		$102,025	$163,240
Adjunct faculty	0.00	0.00	0.00	0.00
salaries				$0
fringe benefits				$0
Graduate assistants	2.00	0.00	0.00	2.00
salaries	$32,000			$32,000
fringe benefits	$2,448			$2,448
Classified Positions	0.25	0.00	0.00	0.25
salaries	$7,500			$7,500
fringe benefits	$2,783			$2,783
Personnel cost				
salaries	$204,500	$0	$275,000	$479,500
fringe benefits	$66,446	$0	$102,025	$168,471
Total personnel cost	$270,946	$0	$377,025	$647,971
Equipment				$0
Library				$0
Telecommunication costs				$0
Other costs				$0
TOTAL	**$270,946**	**$0**	**$377,025**	**$647,971**

Part D: 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 2018 – 2019	Target enrollment year 2022 - 2023
Reallocation within the department *(Note below the impact this will have within the department.)*	$75,405	$75,405
Reallocation within the school or college *(Note below the impact this will have within the school or college.)*		
Reallocation within the institution *(Note below the impact this will have within the institution.)*	$195,541	$572,566
Other funding sources *(Specify and note if these are currently available or anticipated.)*		

2. Statement of Impact/Other Funding Sources.

Reallocation within the Department:
The Center for Cyber Security Education and Research (CCSER), in collaboration with the Graduate School, will administer the proposed program. The Director of the CCSER will oversee the program and teach a minimum of one course in the program. Funds from the CCSER will be available at the program's launch and through the target year. In addition, two graduate assistants will assist with this program. The faculty and administration anticipate no negative impact from the implementation of this program.

Reallocation within the Institution:
Most courses in this interdisciplinary program will be taught by faculty from four colleges across the institution. No negative impact is anticipated for any of the colleges or from any other areas of the University.

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

The Hampton Roads Cybersecurity Education, Workforce and Economic Development Alliance (HRCyber)

Members of The Hampton Roads Cybersecurity Education, Workforce and Economic Development Alliance (HRCyber)

Anuswith, Chris
VP Risk Management
ABNB FCU

Armistead, Leigh
President
Peregine Technical Solutions

Bouchard, Joe
Principle
VNA Consulting

Bowden, Dan
VP & CISO
Sentara Healthcare

Burke, Diana
Executive Director
Va Beach Hotel Association

Cook, Steve
Vice President of Workforce Innovation
Opportunity Inc. of Hampton Roads

Crisler, Kane
Director, Technical Operations
Packet Forensics

Dabbs, Derek
CIO
Sera-Brynn

Escobar, Katherine
President
ISSA-HR

Francis, Adrian
Vice President
ISSA-HR

Gracia, Johnny
Founder/CEO
SIMIS Inc

Hegedus, Rob
CEO
Sera-Brynn

Johann, Joe
Senior VP & ISO
Towne Bank

Johnson, Richard
CEO
Rileen Innovation Technologies, Ince

Jones, Gray
Strategic Business Consultant
Klett Consulting

Joseph, Martin
President and CEO
360 IT Partners

Kelly, Patrick
President
CMIT Solutions

Klett, Mark
President and CEO
Klett Consulting

Longe, Mark
Vice President, Business Development
C5BDI

Morgan, Penny
President
AERMOR

Morrozoff, Natalie
Senior Associate
Booz Allen Hamilton

Oppleman, Sasha
Vice President & FSO
Vostrom Holdings, Inc

Page, Grant
Founder & President
MI Systems

Pizzini, Robert
CEO
iFLY

Prevette, Thom
Director of Advocacy and Community Relations
Bon SeCours Health System

Quinn, Joseph
Vice President Navy Fleet Programs
SAIC

Reece, Terry
CISSP-ISSMP Principal
Sera-Brynn

Richmond, Domonick
Manager
Alvarez & Marsal

Rose, Matt
Account Director
Lumos Networks

Runyan, Darich
Senior Director, Terminal Technology
Port of Virginia

Severinghaus, Richard
President and CEO
CRTN Solutions

Spino, Romeo
Co-founder & Executive VP
StratasCorp Technologies

Tomchick, Greg
Security Strategy Analyst
Klett Consulting

Upchurch, Justin
Computer Security Engineer
Hunting Ingalls, NNSY

Villanueva, Ron
President and CEO
StratasCorp Technologies

Watkins, Stephen
VP and Chief Security Strategist
G2 Ops

Weatherly, Michael
Owner
C5BDI

Zeliaman, Steven
Cybersecurity Solutions Architect
SAIC

APPENDIX B

PLANS OF STUDY

Sample Schedule for Full-Time Students

Course	Credits	Category
Fall I		
CYSE 600 Cybersecurity Principles	3	Core
Restricted Elective	3	Elective
Restricted Elective	3	Elective
CRJS/CYSE 603 Advanced Cybersecurity Law and Policy	3	Core
TOTAL 12 credits		
Spring I		
CYSE 601 Advanced Cybersecurity Techniques and Operations	3	Core
CYSE 605 Leadership and Management in Cybersecurity	3	Core
Restricted Elective	3	Elective
Restricted Elective	3	Elective
TOTAL 12 credits		
Fall II		
CYSE 698 Master's Project	3	Capstone
Restricted Elective	3	Elective
TOTAL 6 credits		

Total Required for Degree—30 credits

Sample Schedule for Part-Time Students

Course	Credits	Category
Fall I		
CYSE 600 Cybersecurity Principles	3	Core
CRJS/CYSE 603 Advanced Cybersecurity Law and Policy	3	Core
TOTAL 6 credits		
Spring I		
CYSE 601 Advanced Cybersecurity Techniques and Operations	3	Core
Restricted Elective	3	Elective
TOTAL 6 credits		
Fall II		
CYSE 605 Leadership and Management in Cybersecurity	3	Core
Restricted Elective	3	Elective
TOTAL 6 credits		
Spring II		
Restricted Elective	3	Elective
Restricted Elective	3	Elective
TOTAL 6 credits		
Fall III		
CYSE 698 Master's Project	3	Capstone
Restricted Elective	3	Elective
TOTAL 6 credits		

Total Required for Degree—30 credits

APPENDIX C

COURSE DESCRIPTIONS

Foundational 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, 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 forensic investigation, and practice techniques for penetration testing.

CRJS/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.

Restricted Elective Courses

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 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/CYSE 595 Software Reverse Engineering (3 credits)
This course provides students with the understanding and practice to perform analysis on malware, deduce its design, determine how malware works, and to aid the analysis via disassembly. Students will be able to use a combination of tools (IDAPro, OllyDbg) to safely perform static and dynamic analysis of malware, including encoded, packed, obfuscated ones. Students are expected to have extensive hands-on exercises through in-class practice, homework and projects.

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 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 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.

ECE 516 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.

ECE 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.

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.

IT 624 Information Technology Assurance Services (3 credits)
Standards, ethics, and practice of information technology assurance services particularly as it concerns the governance and control of information systems.

IT 664 Project Management in Information Technology (3 credits)
This course provides basic knowledge of project management including tools to manage scope, time, cost, quality, risk, team, communications and procurement. Special issues in the IT context are emphasized.

IT 685 Introduction to Information Security (3 credits)
Introduction to technical and administrative aspects of information security. Topics include identification and authentication, access control, security models, computer intrusion detection, trust management, cryptography, PKI, fire walls, network security, web security, and secure e-commerce and e-business.

MSIM 673 Threat Modeling and Risk Analysis (3 credits)
This course discusses how to develop cyber threat models using attack graphs/trees, STRIDE, Universal Modeling Language (UML), attack graphs/trees and common of risk analysis tools. Course also discusses the need for quantitative security analysis and formal validation of security models and basic principles of formal model validation.

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

MSIM 773 Networked System Security (3 credits)
Course presents an overview of theory, techniques and protocols that are used to ensure that networks are able to defend themselves and the end-systems that use networks for data and information communication. Modeling of threats to networked systems, attack modeling with attack trees/graphs, cyber physical systems survivability to attacks, and behavior modeling of malware are explored.

Capstone Course

CYSE 698 Master's Project (3 credits)
Individual project directed by the student's professor in major area of study.

APPENDIX D

ABBREVIATED CVs FOR CORE FACULTY

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.

Graham, Rod, PhD, 2009, Sociology, City University of New York. Assistant Professor of Sociology and Criminal Justice. Specialization areas: African American digital practices, digital practice of mobile phones, the role of digital literacy in reducing phishing victimization, exploring the characteristics of Darknet—an anonymous space online.

Haines, Russel, PhD, 2002, Management Information Systems, University of Houston. Associate Professor of Information Technology and Decision Sciences. Specialization areas: Cybersecurity, application development, communication and collaboration systems.

He, Wu, PhD, 2006, Information Science, University of Missouri. Associate Professor of Information Technology and Decision Sciences. Specialization areas: Cyber security, social media, data mining, computational thinking, case-based reasoning, and computing education.

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.

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.

Wang, Cong, PhD, 2017, Electrical and Computer Engineering, State University of New York at Stony Brook. Assistant Professor of Computer Science. Specialization areas: cybersecurity, mobile computing, machine learning, network optimizations and energy-efficiency.

Wu, Hongyi, PhD, 2002, Computer Science, State University of New York at Buffalo. Professor of Electrical and Computer Engineering and Batten Chair of Cybersecurity. Specialization areas: Networked cyber-physical systems for security, safety, and emergency management applications.

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.

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.

APPENDIX E

FUNDED SCHOLARSHIP

Recent research projects funded by federal grants (within 2 years):

- "REU Site: Cybersecurity Research in a Multidisciplinary Environment", NSF, $360,000, March 2017 – Feb. 2020, ChunSheng Xin and Khan Iftekharuddin.
- "On-Demand Spectrum Access: Application-Oriented Dynamic Spectrum Access," NSF, 12/2013 – 08/2017, $498,000, Chunsheng Xin.
- "Enhancing Spectral Access via Directional Spectrum Sensing Employing 3D Cone Filterbanks: Interdisciplinary Algorithms and Prototypes," 12/2013–08/2017, $157K, Chunsheng Xin.
- "Data provenance Assurance in Cloud using Blockchain", AFRL, 08/2016- 3/2017, $100,000, Sachin Shetty.
- "Analyzing and Supporting the Development of the Cyber-insurance Market as a Market-Based Solution for Cyber Resiliency Project", DHS Critical Infrastructure Resilience Institute, 07/2016 - 12/2016, $80,000, Sachin Shetty.
- "Cyber Resilient Energy Delivery Consortium", DOE, 07/2016 - 7/2020, $740,000, Sachin Shetty.
- "Center of Excellence in Cyber Security", DOD OASD, 07/2016 - 3/2020, $480,000, Sachin Shetty.
- "Large-Scale Opportunistic Data Crowdsourcing and Dissemination in Device-to-Device (D2D) Networks", NSF, 08/2015-08/2018, $385,024, Hongyi Wu.
- "Distributed In-network Data Storage and Retrieval in 3D Wireless Sensor Networks", NSF, 09/2013-08/2017, $372,513, Miao Jin and Hongyi Wu.
- "Enhancing Cybersecurity Education Using POGIL", NSF, 09/2016-8/2019, $140,696, Wu He and Xu Li.
- "GenCyber: Preparing Tomorrow's Heroes to Secure the Cyberspace", NSF and NSA, 04/2016-04/2017, $93,061, Wu He, Chunsheng Xin, Dylan Wittkower, Tammi Milliken and Melva Grant.
- "Improving Security Behavior of Employees in Cyberspace through Evidence-based Malware Reports and E-Learning Materials", NSF SaTC, 09/2013-08/2016, $245,460, Wu He, Li Xu, Ling Li, and Ivan Ash.
- "The Effectiveness of Pair Programming for Students with Learning Disabilities" $299,999, NSF, 08/15/2017 – 07/31/2020, Wu He.

Recent publications:

- W. He, X. Tian, and M. Anwar, "Developing and Using Evidence-based E-learning Videos for Cybersecurity Education". KSU Conference on Cybersecurity Education, Research and Practice. October 29-30, 2016. Paper 3.
- M. Anwar, W. He, and X. Yuan, "Employment Status and Cybersecurity Behaviors", The 3rd International Conference on Behavioral, Economic, and Socio-Cultural Computing (BESC), South Point, Durham, NC, USA, November 11-13, 2016.
- X. Yuan, W. He, L. Simpkins, and Y. Liu, "Teaching Security Management for Mobile Devices", The 17th Annual Conference on Information Tech. Education (SIGITE), Boston, 9/28-10/1, 2016.

- D. Brill, A. Dinh, Y. Li, and W. He, "Malware Sequence Alignment", in Proceedings of the 6th IEEE International Conference on Big Data and Cloud Computing, Atlanta, GA, USA, October 8-10, 2016.
- W. He, M. Anwar, I. Ash, X. Yuan, L. Li, and L. Xu, "A Study of Employees' Self-Reported Cybersecurity Behaviors", in Proceedings of the 22nd Americas Conference on Information Systems (AMCIS), San Diego, USA, August 11-13, 2016.
- W. He, X. Tian, J. Shen, and Y. Li, "Understanding Mobile Banking Applications' Security risks through Blog Mining and the Workflow Technology", in Proceedings of the International Conference on Information Systems 2015, Fort Worth, Texas, December 13-16. 2015.
- W. He and X. Yuan, "Behavioral Information Security Research with Emerging Technologies", Journal of Information Privacy and Security, 10(4), 157-159, 2014.
- W. He, A. Kshirsagar, and A. Nwala, "Teaching Information Security with Workflow Technology – A Case Study Approach", Journal of Information Systems Education, 25(3), pp. 201-210, 2014.
- W. He, X. Yuan, and L. Yang, "Supporting Case-based Learning in Information Security with Web-based Technology", Journal of Information Systems Education, 24(1), 31-40, 2013.
- A. Sharah, T. Oyedare, and S. Shetty, "Detecting and Mitigating Smart Insider Jamming Attacks in MANETs Using Reputation-Based Coalition Game", Journal Comp. Network and Communications, 2016.
- P. McNeil, S. Shetty, D. Guntu, and G. Barve, "CREDENT: Scalable Real-time Anomalies Detection and Notification of Targeted Malware in Mobile Devices", in proceedings of The 7th International Conference on Ambient Systems, Networks and Tech., pp. 1219-1225, 2016.
- W. Chen, L. Hong, S. Shetty, D. Lo, R. Cooper, "Cross-Layered Security Approach with Compromised Nodes Detection in Cooperative Sensor Networks", in IPDPS Workshops, pp. 499-508, 2016.
- X. Yuchi and S. Shetty, "Enabling security-aware virtual machine placement in IaaS clouds", in proceedings of MILCOM, pp. 1554-1559, 2015.
- B. Ban, M. Jin, and H. Wu, "Optimal Marching of Autonomous Networked Robots", in *IEEE International Conference on Distributed Computing Systems (ICDCS)*, 2016.
- U. Tatar, B. Bahsi, and A. Gheorghe, "Impact Assessment of Cyber Attacks: A Quantification Study on Power Generation Systems", System of Systems Engineering Conference (SoSE), 2016.
- U. Tatar, B. Karabacak, and A. Gheorghe, "An Assessment Model of Improving National Cyber Security Governance", 11th International Conference on Cyber Warfare and Security, 2016.
- V. Ashok and R. Mukkamala, ``Data Mining Without Data: A Novel Approach to Privacy-preserving Collaborative Data Mining," Workshop on Privacy in the Electromic Society (WEPS 2011), CCS 2011, Chicago, IL, October 2011.

- T. Sayi, R.K.N. Sai Krishna, R. Mukkamala, and P.K. Baruah, ``Privacy Preserving Distribution in Outsourced Environments," HiPC 18th International Conference on High-performance Computing: Student Research Symposium, Bangalore, India, December 2011.
- M. R. Gorai, K.S. Sridharan, T. Aditya, R. Mukkamala, and S. Nukavarapu, ``Employing Bloom Filters for Privacy Preserving Distributed Collaborative kNN Classification," World Congress on Information and Communication Technologies, WICT 2011, Mumbai, India, December 2011.
- S. Tummalapalli, R.K.N. Sai Krishna, R. Mukkamala, P.K. Baruah, "Data outsourcing in cloud environments: A privacy preserving approach," 9th Int. Conf. Information technology: New Generations, April 16-18, Las Vegas, 2012.
- S. Tummalapalli, R.K.N. Sai Krishna, R. Mukkamala, P.K. Baruah, "Privacy Preserving Data Distribution in Outsourced Environments," HiPC 2011, December 18-21, 2011.
- S. Tummalapalli, R.K.N. Sai Krishna, R. Mukkamala, P.K. Baruah, "Privacy Preserving Data Management in Mobile Environments: A partial encryption approach,"13th Intl. Conf. Mobile data Management, MDM 2012, July 23-26, 2012.
- R.K.N. Sai Krishna, S. Tummalapalli, R. Mukkamala, P.K. Baruah, "Efficient Privacy-preserving Data Distribution in Outsourced Environments: A Fragmentation-based Approach," International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2012.
- R.K.N. Sai Krishna, S. Tummalapalli, R. Mukkamala, P.K. Baruah, "Preserving Privacy of Outsourced Data: A Cluster-Based Approach," 2012 IEEE International Workshop on Data Integration and Mining (DIM-2012), August 8-10, 2012.
- S. Tummalapalli, R.K.N. Sai Krishna, R. Mukkamala, P.K. Baruah, "Data Outsourcing in Cloud Environments: A Privacy Preserving Approach," ITNG 2012, April 16-18, 2012.
- R. Krishna Prasanth, R. Mukkamala, and P.K. Baruah, "Employing GPU accelerators for efficient enforcement of data integrity in outsourced data," IEEE 19th Intl. Conf. High performance Computing, HiPC 2012, 18-21 Dec, 2012.
- R. Sairam, N. Ramachandran, M. Gorai, R. Mukkamala, and P.K. Baruah, "A computationally efficient and scalable approach for privacy preserving kNN classification," IEEE 19th Intl. Conf. High performance Computing, HiPC 2012, 18-21 Dec, 2012.
- V. Ashok and R. Mukkamala, "A Scalable and Efficient Privacy Preserving Global Itemset Support Approximation using Bloom Filters,"DBSec 2014 : 28th Annual IFIP WG 11.3 Working Conference on Data and Applications Security and Privacy, Vienna, Austria, July 14-16, 2014.
- R. K. Dhandhania, P. K. Baruah, and R. Mukkamala, "Privacy-Preserving Mining of Decision Trees Using Data Negation Approach," International Conference on Contemporary Computing and Informatics (IC3I), Mysore,India, November 2014.
- V. Ashok, K. Navuluri, A. Alhafdhi, and R. Mukkamala, "Dataless Data Mining: Association Rules-based Distributed Privacy-preserving Data Mining," 12th International

Conference on Information Technology: New Generations (ITNG 2015), Las Vegas, NV, April 2015.

- C. Iyer, P. K. Baruah, and R. Mukkamala, "Privacy-preserving frequent itemset mining in outsourced transaction databases," Fourth International Conference on Advances in Computing, Communications, and Informatics," August 10-13, 2015.
- K. Navuluri, R. Mukkamala, and A. Ahmad, "Privacy-aware Big Data Warehouse Architecture," 2016 IEEE International Congress on Big Data (BigData Congress), pp. 341-344, 2016.
- K. Navuluri and R. Mukkamala, "Effect of threat modeling on Identity System Management design," pp. 183-189, 10th MSVESCC, Modeling, Simulation, Visualization Conference, 2016.
- A. Ahmad A. Ahmad and R. Mukkamala, "A Novel Information Privacy Metric," ITNG 2017, April 2017, Springer-Verlag.
- A. Ahmad and R. Mukkamala, "A Layered Model for Understanding and Enforcing Data Privacy," ITNG 2017, April 2017, Springer-Verlag.
- A. Rezaei, D. Zhao, M. Daneshtalab, and H. Wu, "Shift Sprinting: Fine-Grained NoC-based MCSoC Architecture in Dark Silicon Age", in *ACM/IEEE Design Automation Conference (DAC)*, 2016.
- T. Luo, S. Kanhere, H-P. Tan, F. Wu, and H. Wu, "Crowdsourcing with Tullock Contests: A New Perspective", in *IEEE International Conference on Computer Communications (INFOCOM)*, HongKong, China, April 26-May 1, 2015. (Best Paper Award nominee)
- S. Xia, H. Wu, and M. Jin, "Trace-Routing in 3D Wireless Sensor Networks: A Deterministic Approach with Constant Overhead", in *ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, pp. 357-366, Philadelphia, PA, August 11-14, 2014.
- Y. Yang, M. Jin, and H. Wu, "3D Surface Localization with Terrain Model", in *IEEE International Conference on Computer Communications (INFOCOM)*, pp. 46-54, 2014.
- H. Zhou, S. Xia, M. Jin and H. Wu, "Localized and Precise Boundary Detection in 3D Wire- less Sensor Networks", in *IEEE/ACM Trans. on Networking*, Vol. 23, No. 6, pp. 1742-1754, 2015.
- Y. Yang, M. Jin, Y. Zhao, and H. Wu, "Distributed Information Storage and Retrieval in 3D Sensor Networks with General Topologies", in *IEEE/ACM Transactions on Networking*, Vol. 23, No. 4, pp. 1149-1162, 2015.
- J. Backens, C. Xin, M. Song, "A Novel Protocol for Transparent and Simultaneous Spectrum Access between the Secondary User and the Primary User in Cognitive Radio Networks," Elsevier Computer Communications, vol. 69(9), p. 98-106, Sep. 2015.
- C. Xin and M. Song, "An Application-Oriented Spectrum Sharing Architecture," IEEE Transactions on Wireless Communications, vol. 14(5), p. 2394-2401, May 2015.

- J. Backens, C. Xin, M. Song, and C. Cheng, "DSCA: Dynamic Spectrum Co-Access between the Primary Users and the Secondary Users," IEEE Transactions on Vehicular Technology, vol. 64(2), p. 668-676, Feb. 2015.
- C. Cheng, M. Song, and C. Xin, "CoPD: A Conjugate Prior based Detection Scheme to Countermeasure Spectrum Sensing Data Falsification Attacks in Cognitive Radio Networks," Springer Wireless Networks, vol. 20(8), p. 2521-2528, Nov. 2014.
- C. Xin and M. Song, "Detection of PUE Attacks in Cognitive Radio Networks based on Signal Activity Pattern," IEEE Transactions on Mobile Computing, vol. 13(5), p. 1022 - 1034, May 2014.

APPENDIX F

SUPPORT LETTERS

APPENDIX G

EMPLOYER SURVEY

APPENDIX H

JOB ANNOUNCEMENTS

Security Engineer

BCMC 3 reviews - Oakton, VA

Security Engineer

Top Secret Clearance is required

BCMC has an immediate opening for a Cyber Systems Engineer. This position provides an opportunity to further advance the cutting-edge technology that supports some of our nation's core defense/intelligence services and systems. Employee will work closely with esteemed customers to develop solutions that allow them to carry out high-stakes national security missions.

The candidate will function with general direction, and will have frequent inter-organizational interactions. Specific responsibilities include:

REPRESENTATIVE DUTIES AND TASKS:

- Leads security requirements analysis, security requirements definition, system security design, security architecture generation, security trade studies, and security verification and validation with little or no supervision
- Leads security planning, cost and risk analyses for the program security activities
- Leads customer security requirements analysis, develops system security requirements and defines allocations to lower levels (subsystem, elements and components)
- Develops detailed security analyses at the system of system (SOS) level
- Synthesizes security solutions within the context of the system to meet customer expectations while staying within schedule and cost constraints
- Recognizes various security architectural patterns, applies them appropriately, understands strengths/weaknesses within those security architectures, is

able to perform/lead system-level security architecture effort
- Researches and analyzes data, such as vendor products, COTS components, GFE/CFE, specifications, and manuals to determine security of design
- Effectively chooses the appropriate standards, processes, procedures, and tools throughout the system development life cycle to support the generation of the security engineering products
- Contributes to the system level required security documentation, including items such as security controls assessment report and security tests plans and procedures in compliance with the IA policy
- Leads or executes the security testing and evaluation to ensure the correct implementation of security requirements
- Assesses and mitigates system security threats and risks throughout the program life cycle
- Leads technical security tasks for large and medium projects
- Mentors less experienced engineers internal and external to the department on IA/cyber principles, practices, and processes

KNOWLEDGE SKILLS AND ABILITIES:

- Demonstrated use and understanding of systems engineering concepts, principles, and theories
- Demonstrated understanding of cyber security specifications such as Risk Management Framework (RMF), DIACAP, STIGs and other government security specifications and guidelines
- Demonstrated understanding of cyber security technology and trends
- Contributes to the achievement of business objectives
- Recognizes and incorporates various security designs and lessons learned
- Demonstrated ability in communicating issues, impacts, and corrective actions as they affect the cyber design and implementation
- Demonstrated ability in reporting relevant cyber systems engineering design
- Regular contact with senior levels of security work groups internally and externally
- Ability to lead security work groups within the project

- Serves as consultant to senior management and customers on long-range security planning and security issues
- May serve as company technical spokesperson in cyber security
- Recognized and trusted as a cyber leader in the customer community
- Recognized internally and externally as an expert in cyber security
- Contact with project leaders, the customer program leadership, and professionals within the Engineering department and with project teams
- Frequent contact with the external customers' security professionals
- Creative thinker, good multi-tasker

BASIC QUALIFICATIONS:

Bachelor's of Science degree in Engineering, a related specialized area or field is required (or equivalent experience) plus a minimum of 10 years of relevant experience; or Master's degree plus a minimum of 8 years of relevant experience

CLEARANCE REQUIREMENTS:

Department of Defense TS/SCI security clearance is required at time of hire. Must be able to obtain a DHS Suitability. Applicants selected will be subject to a U.S. Government security investigation and must meet eligibility requirements for access to classified information. Due to the nature of work performed within our facilities, U.S. citizenship is required.

PREFERRED DEGREE TYPES AND EXPERIENCE:

Work with the following security tools: Nessus, Foundstone, Retina, Fortify, App Scan, Brakemen, JIRA and SharePoint.

Our Company Overview:

Business Computers Management Consulting Group, LLC (BCMC) is an 8(a) Small Disadvantaged Business specializing in Information Technology (IT), Cybersecurity, Information Assurance (IA), SOA, Big Data Management, Program Management, and more for Federal, State, and Local agencies. We are appraised at CMMI Level 3 and ISO 9001:2008 certified and registered promising highest quality to all of our clients.

- https://bcmcgroup.com/

- https://www.linkedin.com/company/bcmc-llc
- http://www.indeed.com/cmp/Bcmc

Job Type: Full-time

Job Location:

- Oakton, VA

Required education:

- Bachelor's

Required experience:

- security engineering: 8 years

Required license or certification:

- active Top Secret clearance

5 days ago - save job

» Apply Now

Please review all application instructions before applying to BCMC.

Apply Now

Senior Logistics Specialist

Metrica, Inc. - Arlington, VA 22209

Metrica Inc. is a small business leader in Global Mobility, Cybersecurity Modernization, and International Logistics. Metrica's core values include providing our clients with strong service, continuous improvement, and quick response and giving our employees responsibility, trust, and ownership of their positions. Metrica requires all of its employees to understand and embrace these values as they form the foundation on which the corporation undertakes its endeavors.

Metrica is seeking to fill the Deputy Program Manager/Senior Logistics Specialist positon based in Arlington, VA. In this position, you will administer program efforts providing Staffing Support, Freight Forwarding, Logistical Support, Security, and Business Process Services to U.S. Government and private sector clients. Candidates should have sound grounding in the acquisition and delivery of goods and services across the supply chain.

Key Responsibilities:

- Focus on customer relationships and stakeholder management to provide excellent customer service and exceptionally high-quality deliverables
- Manage tasks by coordinating the required services according to standard operating policies and procedures
- Work in partnership with the client throughout the Task Management and Execution Process
- Assist in identifying new overseas partners, managing tasks in over 25 countries and developing effective business improvement processes
- Conduct data collection and financial analysis and reporting including trend analysis, budgeting, cost projection, burn-rate, best-value, and basic earned-value management
- Prepare and review invoices and cost projections
- Identify and develop solutions to complex logistical problems between the client and Metrica's overseas partners and/or local authorities and address and resolve host country legal and compliance issues
- Assist in the management of service contracts and be familiar with varying contract, country-specific and customer requirements

- Coordinate logistical efforts in assigned countries or regions, and/or functional areas such as technical advisor support and conference/event management
- Demonstrate effective communications with the ability to translate raw data and extraneous information into applicable products to inform internal and external decisions
- Review task requests and identify resources required for each task
- Provide guidance and support to logistics specialists and other team members

Experience & Skills Required:

- Minimum 10-15 years of professional experience in international operations or similar field
- BA in business, finance, public administration, international relations or related field required; Master's degree preferred
- Project Management Professional (PMP) certification desired
- Exceptional analytical and problem-solving abilities
- Proficient in use of personal computers and MS Office Products and general office equipment
- Strong oral and written communications, including creating and delivering presentations
- Experience living or working overseas is a benefit, but not a requirement
- Self-starter who displays initiative and can work independently is a must. The attention to detail and the ability to work effectively under tight timelines is also critical to this position

Metrica offers an excellent starting salary and outstanding fringe benefits, including Medical, Dental, Tuition Assistance, and 401(k) Retirement Plan to name a few.

Interested Applicants should submit their resume & cover letter to Metica's H/R Office by noon CST Friday, August 11, 2017.

Metrica is an Equal Opportunity Employer, M/F/D/V.

Job Type: Full-time

Required education:

- Master's

18 days ago - save job

Careers | Information Assurance Professional (VM Ware) - Springfield, VA

Share This Job

0Share

Apply Now

Information Assurance Professional (VM Ware)

Req #: 133000
Location: Springfield, VA US
Job Category: Information Systems
Security Clearance: TS/SCI
Clearance Status: Must be Current

Job Description:
At CACI, we don't just hire you for a job; we hire you for a career. CACI recruits, retains, and develops a diverse range of talent to create an environment that fuels innovation and fosters continuous improvement and success. We empower you to forge your path while providing you with the tools, guidance, and flexibility needed to accomplish your career goals. CACI has a clear, defined strategy that has guided our success for over fifty years.

Consider a career with CACI, where you will have the opportunity to make an immediate impact by providing the information technology and consulting solutions America needs to defeat global terrorism, secure our homeland and improve government services.

Duties and RESPONSIBILITIES:

CACI has an immediate opening for an Information Assurance (IA) Professional to support a Government client. The candidate will provide ISSE services to information system owners as determined by the government cust er. IS urity inee consists of applying the best

practices and processes of capturing, refining, and assisting in prioritization of requirements based on risk, engineering principles, and mission requirements. ISSE produces purposeful security architecture, design development and a configuration information system that facilitate secure missions systems. The candidate will provide Information System Owners (ISOs) guidance, requirements understanding, and options to support technical security engineering and capability based security analysis of system security architectures, identify vulnerabilities, and provide suggested mitigation alternatives. They will participate in design, development, and implementation of information systems to ensure these systems are in compliance with required security features and safeguards.

The IA professional will propose categorization of information systems based on types of information processed, in conjunctions with DAO Representatives and ISOs. They will identify improved or equal security features and safeguards provided for system enhancements. The IA professional analyzes IA policies, procedures, and requirements and provides security recommendations for the operational functionality of systems or proposed capabilities in sufficient detail to support the development of interoperable, standard, and compatible systems. They will coordinate with appropriate Security Control Assessors (SCAs) early in engineering design phase for ongoing coordination, understating in development and application of security controls, and security tradeoffs and other decisions. The IA professional provides technical assistance to the government efforts to conduct cost/benefit analysis for security design decisions. They perform security engineering analysis and documentation reviews to validate government IA policies, procedures, and requirements are met. They provide technical guidance in security design reviews and analyze vendor documentation for government and commercial solutions. The IA professional oversees and reports compliance with system security plans on all government customer information stores, systems and networks on a regular (at least quarterly) basis and reviews audit logs for security significant issues and events and advises government PMs on a weekly basis. They provide network services engineering expertise in support of strategic defense of essential network infrastructures and operations against compromise by ensuring integrity and robustness of interconnections between networks of different security domains. They ensure information systems are designed, developed, and implemented with required security features and safeguards. They provide cross domain system security control guidance to developers.

Required Qualifications:

- Experience with demonstrated competency in engineering related functional or cross-functional security areas (e.g., security engineering, IT operations security design, cybersecurity)
- Experience in identifying technical gaps and providing solution recommendations
- Experience in providing and analyzing comprehensive security architecture artifacts

- Working knowledge and experience in security disciplines including but not limited to, information systems security, operations security, administrative security, personnel security, physical security and communications security
- Working knowledge of IA principles and organizational requirements that are relevant to confidentiality, integrity, availability, authentication, and non-repudiation
- Working knowledge of DCID 6/3. ICD 503, CNSSI 1253, NIST SP 800-53, NIST SP 800-53A, NIST SP 800-37, and security controls assessment criteria/procedures
- Working knowledge of DoD/IC system security control requirements, roles, missions, and operational enterprise architecture
- Working knowledge of IA architecture frameworks, including the IC IA Architecture Reference Model
- Working knowledge of network security architecture concepts, including topology, protocols, components, and principles
- Working knowledge of the System Development Lifecycle
- Working knowledge of information security systems engineering principles and virtual machine technology
- Working knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption)
- Working knowledge of network access, identity, and access management (e.g., PKI)
- Working knowledge, skills, and experience in Systems Engineering principles, requirements analysis, system development (software and hardware)
- Skill in designing countermeasures to identified security risks
- Skill in discerning the protection needs (i.e., security controls) of information systems and networks
- Ability to evaluate the adequacy of security designs
- Ability to develop and apply security system access controls
- Ability to conduct audits or reviews of technical systems
- Certified 8570 IAM or IAT level 3, CISSP, CISM, CASP, CISA or GSLC certification (CISSP preferred)

Desired Qualifications:

- Working knowledge of IT supply chain security/risk management policies, requirements, and procedures
- Working knowledge of system design tools, methods, and techniques, including automated system analysis and design tools
- Working knowledge of system software and organizational design standards, policies, and authorized approaches (e.g., International Organization for Standardization guidelines) relating to system design

- Working knowledge of Privacy Impact Assessments (PIA) and Personally Identifiable Information (PII)
- Working knowledge and experience with XACTA, including understanding workflow
- Skill in translating security requirements into functional requirements and options for developers
- Skill in security control inheritance from enterprise security services and communicating these to developers
- Skill in creating policies that reflect system security objectives
- Skill in designing security controls based on IA principles and tenets
- Skill in designing the integration of hardware and software solutions
- Ability to use design modeling (e.g., unified modeling language)
- Ability to conduct vulnerability scans and recognizing vulnerabilities in security systems
- Ability to establish working relationships internally and externally to the Agency
- Skill in identifying gaps in technical capabilities and in talking to others to convey information effectively
- Experience within the Intelligence Community

EDUCATION & EXPERIENCE:

Typically requires a bachelor's degree or equivalent and two to 15 years of related experience. Master's degree or doctorate in field mathematics, telecommunications, electrical engineering, computer engineering, or computer science is preferred.

PHYSICAL DEMANDS:

Normal demands associated with an office environment. Ability to work on computer for long periods, and communicate with individuals by telephone, email and face to face. Some travel may be required.

CACI employs a diverse range of talent to create an environment that fuels innovation and fosters continuous improvement and success. Join CACI, where you will have the opportunity to make an immediate impact by providing information solutions and services in support of national security missions and government transformation for Intelligence, Defense, and Federal Civilian customers. A Fortune magazine World's Most Admired Company in the IT Services industry, CACI is a member of the Fortune 1000 Largest Companies, the Russell 2000 Index, and the S&P SmallCap600 Index. CACI provides dynamic careers for over 20,000 employees worldwide. CACI is an Equal Opportunity Employer - Females/Minorities/Protected Veterans/Individuals with Disabilities.

Cybersecurity Info Assurance

Location: **Manassas, VA**

Job Code: **1651**

# of openings: **1**

Description

Job Qualifications:

The Cybersecurity System Engineer is responsible for ensuring the highest level of confidentiality, integrity, and availability in Aurora developed unmanned mission systems. This position has the responsibility to lead the assigned team of both internal staff and subcontractors to execute and mature the company's technical and operational cybersecurity capabilities. This position is expected to be a combination of technical delivery and team leadership. This position will develop cybersecurity plans and implement processes resulting in accredited hardware and software solutions deployed into operational unmanned aerial systems (UAS).

Technical responsibilities include, but are not limited to, requirements and CONOPS development, system design and analysis, and operations support.

Typical duties include:

- Providing technical analyses for information assurance (IA) support and integration efforts and performing analyses of authorization and accreditation (A&A) documentation for information security (INFOSEC) product evaluation and related documentation.
- Conducting risk assessments and risk mitigation analyses and developing contingency plans.
- Developing and maintaining Risk Management Framework (RMF) artifacts
- Analyzing the documentation, validation, and accreditation processes necessary to ensure compliance to security and privacy requirements.
- Direct interaction with federal government stakeholders and accrediting authorities
- Researching mission system standards, platforms and architectures and develop cost-effective, timely recommendations for implementation.
- Supporting aircraft and ground system architecture & interface design and capturing target functionality.
- Defining, analyzing and reviewing hardware and software requirements to meet defined and anticipated customer needs, system quality, and performance standards.

Required Qualifications and Experience:

- B.S. in Computer Science, IT or applicable engineering or science field, Master's degree preferred
- 5+ years of experience with operational information technology environments, including 3+ years in a DoD environment
- 5+ years of experience with system and network vulnerability analysis, risk assessment and risk mitigation analysis, security test and evaluation (ST&E), contingency planning, firewall policy, ports, and protocols
- Knowledge of Air Force Platform IT (PIT) Cybersecurity concepts and requirements
- Demonstrated proficiency in developing and implementing a Cybersecurity plan for a new operational system resulting in an ATO and/or ATC

- Knowledge of the DoD Authorization and Accreditation (A&A) process and standards as implemented in the NIST Risk Management Framework (RMF)
- Familiarity with the DoD Critical Program Protection (CPI) process
- Certifications equivalent to IAT Level II, including Security+ CE or above, or IAM Level II, including CISM, CISSP, or CAP Certification, or IA SAE II
- Current Active SECRET, Eligible for TS/SCI

Desired Qualifications and Experience:

- Proficiency in using a SysML modeling methods and tools
- Network design and implementation including IP addressing, firewall configuration, and multi-level security devices and systems
- Operating in a regulated development environment, like CMMI (level 3 or higher) or DO-178.
- Unified Ground Control Station or equivalent GCS for 24x7 mission operations.
- Experience with Federal Government DIACAP and RMF management systems, such as EITDR, eMASS, and ACAS.
- Experience integrating and fielding operational GOTS tools and systems such as DCGS, AIMES, SIRIS, and HBSS.
- Ability to meet DoD 8140/8570 Cybersecurity Workforce (CSWF) Certification requirements
- Active TS/SCI

Physical Requirements:

Candidate must be able to work within a hangar and enter and exit aircraft and other similar physical environments without restriction.

Aurora Flight Sciences is an Equal Opportunity Employer

APPLY FOR THIS POSITION SEND TO A FRIEND

Previous Applicants:

Returning Candidate?
Log back in!

Cyber Security Analyst

All times are in Eastern Daylight Time.

ID	2017-1071	**# of Openings**	1
Job Locations	US-VA-Dam Neck	**Posted Date**	7/24/2017
Category	Information Technology		

More information about this job

Overview

The Cyber Security Analyst will provide technical analysis for IA support and integration efforts. The Cyber Security Analyst will perform analysis of C&A documentation for DOD or Navy Research Development Testing & Evaluation (RDT&E) or operational systems, networks and applications, and Commercial Off-The-Shelf (COTS) INFOSEC product evaluation and related documentation.

Responsibilities

Must **have demonstrated experience in the following areas:**

- Demonstrated knowledge of IA / INFOSEC concepts and requirements.
- Knowledge of the DOD C&A process and standards.
- System / network vulnerability analysis.
- Risk assessment and risk mitigation analysis.
- Security Test and Evaluation (ST&E).
- Contingency planning.
- Firewall Policy
- Ports & Protocols

Qualifications

WORK EXPERIENCE
Minimum four (4) years' experience in IA / C&A analysis support in IA controls analysis, conducting risk assessments, risk mitigation analysis, developing contingency plans.
JOB LOCATION
Norfolk/Suffolk, VA
CERTIFICATIONS

- NQV Level II is required
- Preference for IAM III certified (i.e. CISSP (or Associate), GSLC, CISM, CASP) or Master's in Cyber Security

CLEARANCE
Secret Clearance with the ability to obtain a Top Secret Clearance

All qualified applicants will receive consideration for employment without regard to race, color, religion, sex, sexual orientation, gender identity, or national origin.

Options

Apply for this job online

Refer this job to a friend

Share on your newsfeed

Go back to the welcome page

Application FAQs

Cyber Systems Engineer

Spectrum Comm Inc 14 reviews -
Newport News, VA 23606
Newport News, VA

Job Responsibilities:
Work with Team to research and develops strategies, methodologies, and approaches to integrate new software application and services.

Lead prototyping and development projects

Provide planning and management for projects throughout the systems engineering lifecycle

Develop, review, and validate planning and design artifacts

Perform research in support of product and concept development

Develop and document new concepts

Develop test plans and perform tests of hardware, controls, and software components

Manage cost, schedule and performance of projects assigned

Provide support to business development activities

Interact directly with customers at senior technical and management levels

Required Skills and Experience:
5 years of relevant experience

Bachelor of Science degree in engineering, computer science, or related discipline

Desired Skills and Experience:
Master of Science degree

Spectrum is proud of our diverse workforce and diligently committed to remaining an Equal Opportunity Employer. Spectrum governs all employment-related decisions without regard to an individual's race, color, gender, gender identity, sexual orientation, religion, national origin, age, disability, veteran status or any other protected classification.

[Equal Opportunity/Affirmative Action Employer – minorities/females/veterans/individuals with disabilities/sexual orientation/gender identity]
7 days ago - save job - original job

» Apply Now

Please review all application instructions before applying to Spectrum Comm Inc .

☆ Cybersecurity Systems Engineer

Engineering | Full-time | Arlington, Texas, USA

Apply Now (https://l3com.taleo.net/careersec

Cybersecurity Systems Engineer -

Requisition ID

089840

USA-Texas-Arlington

Description

Description

L3 Link Simulation and Training is seeking an experienced Cybersecurity Expert to provide technical expertise for the design, development, qualification, integration and fielding of compliant systems solutions used in military flight and maintenance training systems.

Responsibilities

• Design and guide development of secure platform solutions for Link's simulation and training markets
• Interact with customers to define cybersecurity and requirements, trades, solutions, costs, implementation, system impacts, and effectiveness
• Assist programs and monitor program execution throughout product development lifecycle to ensure cyber objectives are met
• Lead, advise, and educate engineers on cybersecurity concepts and solutions
• Prepare briefings to obtain approvals by government agencies for contracted efforts

Qualifications

Qualifications

• Bachelor's degree or equivalent in a technical field, such as Electrical Engineering, Systems Engineering, Computer Science; Master's preferred
• Possess the CISSP certification Level II, or equivalent, in accordance with Information Assurance Workforce Improvement Certification (8570.01M)
• Possess an Active Clearance or be capable of obtaining a DoD Top Secret clearance as well as DoD Special Access Program clearance
• Risk Management Framework experience per DoDI 8510.01
• Experience with architecting Cybersecurity concepts into trusted communication and computing platforms for real-time application deployment in distributed network environments
• 8+ years of Cybersecurity engineering experience

Additional Desired Qualifications and Experience

• Experience with multi-threading, multi-process development, including virtualization (Type 1 Hypervisor, Type 2 Hypervisor, para-virtualization), inter-process communication, multi-platform distributed computing

• JSIG/JAFAN implementation experience

• Proficiency in and knowledge of tools and techniques for verification and protection of CPI per DoDI 5200.39

• Full lifecycle systems development experience

L3 Link Simulation & Training (L3 Link) is a division of L3 Technologies. Headquartered in Arlington, TX, L3 Link provides Total Training Solutions to government and commercial customers. Our Core capabilities include development of flight simulator devices, mission training for military pilots, commercial pilot training, and schoolhouse development and operation.

Headquartered in New York City, L3 Technologies employs approximately 38,000 people worldwide and is a leading provider of a broad range of communication and electronic systems and products used on military and commercial platforms. L3 is also a prime contractor in aerospace systems.

Equal Opportunity Employer – minorities / females / veterans / individuals with disabilities / sexual orientation / gender identity

US Security Clearance Required : Secret

Schedule : Full-time

Shift : Day - 1st

Travel : Yes, 10 % of the Time

Organization : Division - LINK Simulation & Training-21000004

Job Level : Individual Contributor

Job Posting : Jul 27, 2017, 10:05:37 PM

Job : Engineering-Systems

Job Description

Job Title: Cyber Security Engineer, Sr

Job ID: 24541

Location: VA - Portsmouth

Full/Part Time: Full-Time

Regular/Temporary: Regular

Email to Friend Save Job Apply Now Return to Previous Page

Responsibilities

Under limited supervision, design, test and implements state-of-the art secure operating systems, networks, and database products. Analyze a wide range of security issues at all levels including architectures, firewalls, electronic data traffic, and network access.

Will be a senior engineer in a team of personnel supporting Naval Undersea Warfare Center Division Newport. Provides cyber security expertise in support of projects to include concept development and system requirements management and review, design and analysis support, reliability and supportability analysis, platform-level inter-subsystem interface definition, integration, test and evaluation, obsolescence investigation, programmatic support, Fleet technical support, and detailed involvement with the subsystems that compose the Submarine combat systems.

Recognized within Alion as a senior level contributor in the field, and may have begun to acquire a similar reputation in the external scientific and client communities.

**** Duties and Responsibilities ****

Involved in the implementation of new security solutions, participation in the creation and or maintenance of policies, standards, baselines, guidelines and procedures as well as conducting vulnerability audits and assessments.

Designs vulnerability assessments, penetration tests and security audits and provides recommendations for application design.

Uses encryption technology, penetration and vulnerability analysis of various security technologies, and information technology security research.

Design and development new systems, applications, and solutions for external customer enterprise-wide cyber systems and networks.

Ensures the logical and systematic conversion of customer or product requirements into total systems solutions that acknowledge technical, schedule, and cost constraints.

Integrates new architectural features into existing infrastructures, designs cyber security architectural artifacts, provides architectural analysis and relates existing system to future needs and trends.

Embeds forensic tools and techniques for attack reconstruction, provides engineering recommendations, and resolves integration/testing issues.

Participates in the creation and enforcement of enterprise security documents (policies, standards, baselines, guidelines and procedures). Maintains documentation, procedures and working instructions in accordance with federal and departmental guidelines.

Analyze logs and reports and interprets the implications. Participates in investigations into problematic activity and assists with plans for appropriate resolution.

Assists with proposals, including gathering facts, analyzing data and preparing project overview which compares alternatives in terms of cost, time, availability of equipment and personnel, etc.
Performs additional duties and responsibilities as required.

Qualifications

Education and Experience

Bachelor¿s degree in Information Assurance, Computer Science, or a related field plus 5 to 7 years of directly related experience. Master¿s degree preferred. An Information Assurance certification in compliance with DoD 8570 (e.g. Security+) is required. Navy Validator certification desired

Additional experience and Operating System Certificates desired for:
1. Windows 7 and/or
2. Windows 10 and/or
3. Linux and/or
4. Windows Server 2008 or greater

In some cases, educational requirements may be adjusted or waived for comparable work experience. Work experience may be adjusted for highly specialized knowledge or uniquely applicable experience for positions involving new technology or labor market shortages as reflected by market survey data.

**** Knowledge, Skills, Abilities ****

Advanced analytical skills and attention to detail

Advanced knowledge of secure operating systems as well as data security.

Effective customer and organizational level communication, presentation and interpersonal skills.

Must be eligible for Secret clearance immediately upon employment.

Diversity Statement

Women, minorities, individuals with disabilities and veterans are encouraged to apply. Alion will provide a reasonable accommodation to individuals with disabilities and disabled veterans who need assistance to apply. Please visit the Alion Careers site for more information U.S. Citizenship Required.

Email to Friend Save Job Apply Now Return to Previous Page

Search by Keyword

Share this Job

Email similar jobs to me

MSC ITESS Information Systems Security Engineer (ISSE) Job

Date: Aug 10, 2017
Location: Virginia Beach, VA, US

MSC ITESS Information Systems Security Engineer (ISSE) (Job Number:429835)

Description:

SAIC has a contingent opening for an Information Systems Security Engineer (ISSE) supporting Military Sealift Command. This is contingent upon contract award and will be located in Virginia Beach, VA.

The Information Systems Security Engineer (ISSE) will establish an IA Program to implement and sustain appropriate IA management, operation, and technical controls and processes required to safeguard DoD non-public information resident on or transiting the contractor's unclassified information systems from unauthorized access and disclosure. The ISSE shall provide program specific input for the development of new application security documentation and the updating of existing application security documentation to facilitate the security accreditation of the system IAW the current C&A guidance.

Qualifications:
EDUCATION AND EXPERIENCE:

- Bachelors and five (5) years or more experience; Masters and three (3) years or more experience; PhD and 0 years related experience.

CLEARANCE REQUIREMENT:

- A minimum of a SECRET clearance is required for this position

REQUIRED EDUCATION AND EXPERIENCE:

- B.S. from an ABET Engineering Accreditation Commission (EAC) Accredited Institution or equivalent work experience.
- Experience with Defense Information Assurance Certification and Accreditation Process
- The ISSE shall have (5 years) experience managing and leading the successful capturing and refining of information protection requirements and ensuring their integration into IT systems through purposeful security design or configuration.

The ISSE shall have experience in the following areas:

- Information Assurance Vulnerability alerts and researching the IAVA/B/T occurrences within the following:
- Vulnerabilities and risks associated with Windows operating systems, and components
- Vulnerability incident reporting
- Cognizance of various DoD policies and regulations (e.g. 8500, 5200), and ability to interpret such policies and regulations as are provided to the Afloat community
- Develop, Review, & Provide feedback on DoD/MSC Information Assurance Packages, documents, orders and instructions
- Strong inter-personal and communication skills to carry out this assignment with the ability to lead and work as part of a team.

SAIC Overview:SAIC is a premier technology integrator providing full life cycle services and solutions in the technical, engineering, intelligence, and enterprise information technology markets. SAIC is Redefining Ingenuity through its deep customer and domain knowledge to enable the delivery of systems engineering and integration offerings for large, complex projects. SAIC has approximately 15,000 employees are driven by integrity and mission focus to serve customers in the U.S. federal government. Headquartered in Reston, Virginia, SAIC has annual revenues of approximately $4.5 billion. For more information, visit saic.com.

EOE AA M/F/Vet/Disability

Job Posting: Aug 10, 2017, 6:02:41 PM
Primary Location: United States-VA-VIRGINIA BEACH
Clearance Level Must Currently Possess: Secret
Clearance Level Must Be Able to Obtain: Secret
Potential for Teleworking: No
Travel: Yes, 10% of the time
Shift: Day Job
Schedule: Full-time

Nearest Major Market: Virginia Beach
Job Segment: Information Systems, Engineer, Systems Engineer, Secret Clearance, Technology, Engineering, Security, Government

Search by Keyword

Share this Job

Email similar jobs to me

Information Systems Security Manager Job

Date: Aug 5, 2017
Location: Hampton, VA, US

Information Systems Security Manager (Job Number:428412)

Description:

JOB DESCRIPTION:

SAIC has an opportunity for an Operational Security Specialist supporting the Air Force with Advanced Programs Support. The successful applicant will support the integration of advanced program concepts and technology as well as coordinate and integrate resource priorities across the Special Access Program (SAP) portfolio to shape Combat Air Forces (CAF) programming strategy to ensure warfighter future requirements are met. Key duties/responsibilities include, but are not limited to:

- Maintain a formal IS security program and policies for organization
- Develop and oversee operational information systems security implementation policy and guidelines
- Coordinate with Program Security Officer (PSO) or cognizant security official on approval of External Information Systems (e.g. guest systems, interconnected system with another organization)
- Maintain required IA certifications
- Monitor all available resources that provide warnings of system vulnerabilities or ongoing attacks
- Maintain a repository of all security authorizations for IS under their purview
- Facilitate IT requirements meetings VTCs, etc
- Conduct periodic testing to evaluate the security posture of IS by employing various intrusion/attack detections and monitoring tools
- Coordinate IS security inspections, tests, and reviews
- Guide implementation of an effective IS security education, training, and awareness program
- Participate in self-inspections; identify security discrepancies and report security incidents
- Confirm proper measures are taken when an IS incident or vulnerability is discovered
- Manage, maintain, and execute the information security continuous monitoring plan

Qualifications:
TYPICAL EDUCATION AND EXPERIENCE:

- Bachelors and five (5) years or more experience; Masters and three (3) years or more experience; PhD and 0 years related experience.

CLEARANCE REQUIREMENT:

- Clearance Level Must Currently Possess: TS/Sensitive Compartmented Information (SCI)
- Clearance Level To Obtain: TS/SCI with Poly

REQUIRED EDUCATION AND EXPERIENCE:

- Must meet position and certification requirements outlined in DoD Directive 8570.01-M for Information Assurance Manager Level 2
- Five (5) years of Information Systems Security management experience required
- Four (4) years of SAP experience within the last six (6) years required

SAIC Overview:SAIC is a premier technology integrator providing full life cycle services and solutions in the technical, engineering, intelligence, and enterprise information technology markets. SAIC provides systems engineering and integration offerings for large, complex projects. Headquartered in McLean, Virginia, SAIC has approximately 15,000 employees and annual revenues of about $4.3 billion.

EOE AA M/F/Vet/Disability

Job Posting: Jul 7, 2017, 12:07:44 PM
Primary Location: United States-VA-HAMPTON
Clearance Level Must Currently Possess: Top Secret/SCI
Clearance Level Must Be Able to Obtain: Top Secret/SCI with Polygraph
Potential for Teleworking: No
Travel: Yes, 10% of the time
Shift: Day Job
Schedule: Full-time

Nearest Major Market: Hampton Roads
Job Segment: Information Systems, Information Technology, IT Manager, Engineer, Technology, Engineering, Security

APPENDIX I

STUDENT DEMAND SURVEY

APPENDIX J

STUDENT LETTERS OF INTEREST

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 Master of Science	6. Term and year of initiation Fall 2018
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 Fall 2019	9. Date approved by Board of Visitors
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 The Center for Cyber Security Education and Research School(s) or college(s) of The Graduate School Campus(es) or off-campus site(s) Mode(s) of delivery: face-to-face _____ distance (51% or more web-based)___X__ hybrid (both face-to-face and distance) _____	
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. Jeanie Kline, Ed.D., SCHEV Liaison, 757.683.3261, jkline@odu.edu	

PROPOSAL FOR
THE MASTER OF SCIENCE IN CYBERSECURITY
TABLE OF CONTENTS

Description of the Proposed Program

Program Background

Old Dominion University (ODU) seeks approval to initiate a Master of Science in Cybersecurity, scheduled to begin fall 2018 in Norfolk, Virginia. This proposed program will be administered by the Center for Cyber Security Education and Research (CCSER) and the Graduate School. The CCSER also oversees an interdisciplinary undergraduate major in Cybersecurity, an undergraduate major in Cyber Operations, an undergraduate major in Cybercrime, as well as an undergraduate minor in Cybersecurity.

Cybersecurity focuses on protecting computers, networks, programs, and data from attack, destruction or unauthorized access. It is of growing importance due to the increasing reliance on computer systems and networks. The information technology revolution is transforming every facet of society, empowering people to embrace new ways of completing daily tasks and transforming how they network, create social identities, build relationships and stay informed.[1] Approximately 87% of the U.S. population uses the Internet daily.[2] According to surveys by Accenture, 82% of executives believe digital technologies are erasing industry limitations and allowing paradigms to emerge.[3] Moreover, there is a remarkable proliferation of networked intelligent devices - collectively known as the Internet of Things (IoT). The IoT is a digitization of the physical world that has come about through embedding physical devices with electronics, sensors, actuators, and network connectivity that enable them to collect and exchange data and be controlled remotely. It presents vast opportunities for organizations to improve efficiencies, gain a competitive advantage, and build new business models. More IoT devices are coming online each and every day. Experts estimate that the IoT will grow to more than 50 billion devices by 2020.[4]

While the computer and network technologies, including the Internet, wireless networks, data centers, personal computers, smart phones, and the emerging Internet-of-Things, are embraced as important tools for efficiency and productivity, a wide spectrum of organizations, ranging from government and military agencies to financial and medical corporations, collect, process, store, and transmit across networks unprecedented amounts of sensitive data, which are becoming an increasingly attractive target for cybercriminals. In the recent years, cyber-attacks are becoming 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 surging demand for a well-trained cybersecurity workforce to safeguard information relating to national security, health and financial records, and various sensitive business and personnel data.

[1] "Digital Adoption", Accenture, https://www.accenture.com/t20170203T031808_w_/us-en/_acnmedia/PDF-42/Accenture-Digital-Adoption-Report.pdf.
[2] "13% of Americans don't use the internet. Who are they?", Pew Research, 2016, http://www.pewresearch.org/fact-tank/2016/09/07/some-americans-dont-use-the-internet-who-are-they/
[3] Accenture Technology Vision, 2016, https://www.accenture.com/us-en/insight-technology-trends-2016
[4] CISCO, "Cisco IoT System Security: Mitigate Risk, Simplify Compliance, and Build Trust," 2015.

This proposed MS in Cybersecurity program is designed to help prepare technology leaders who will fill the demand for highly skilled cyber security specialists and practitioners. It will prepare its graduates for high-level positions, working in a wide variety of capacities to protect the information systems of different types of organizations and to secure the nation's cyber infrastructure. Students will be educated to develop skills and competencies in the technical aspects of cyber security with proficiency in a diversity of current and emerging cyber security technologies, and will be prepared to assume responsibility for the management of cybersecurity systems and coordination of cyber operation teams.

Rationale for the Program at Old Dominion University

Old Dominion University is strategically located for many of its traditional undergraduate and graduate degrees in computer science, computer engineering, information technology, and modeling, simulation and visualization. The city of Norfolk, within Hampton Roads, is home to the largest natural deep-water harbor in the world. Norfolk is also home to the world's largest naval station, supporting 75 ships and 134 aircraft alongside 14 piers and 11 aircraft hangars. Within the region, ODU serves the professional educational needs of the:

- Port of Virginia - the fastest growing port on the east coast with a vibrant and economically robust maritime industry;
- Two major railroads;
- One hundred and sixty four international businesses representing 28 countries;
- Numerous federal facilities and military bases.

This significant infrastructure represents a mosaic of assets and makes Hampton Roads particularly vulnerable to malicious cyber attacks. ODU is ideally and strategically located for hosting the MS cybersecurity program and is poised to train the next generation of cybersecurity professionals. To facilitate the mission of developing a pipeline of industry-ready cyber talent, the university has recently made substantial investments in the area of cybersecurity. The Center for Cyber Security Education and Research (CCSER) was established in March 2015. It reports directly to the Office of Academic Affairs and consists of about 30 affiliated faculty and staff from across the university, including four colleges (arts & letters, sciences, engineering and business) and the Virginia Modeling, Simulation and Analysis Center (VMASC). These entities and faculty possess significant expertise in cybersecurity education and research.

Moreover, the CCSER has recently hired four full-time tenured/tenure-track faculty and a post-doctoral research associate who teach cybersecurity courses and conduct fundamental cybersecurity research. In addition, ODU is the lead on a Regional Alliances and Multi-stakeholder Partnerships to Stimulate (RAMPS) grant from the National Institute for Standards and Technology (NIST). The funded project, HRCyber, brings together more than two dozen partners to coordinate the development of cyber workforce that responds to the needs of the Hampton Roads region. Thus, the proposed Master of Science in Cybersecurity will effectively complement the cybersecurity programs at ODU by offering an advanced degree to meet the surging demand for well-trained professionals who can fill senior cybersecurity positions.

Mission

The Master of Science in Cybersecurity is supportive of the mission of Old Dominion University in that it "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 degree aligns with this mission by: (1) expanding the pipeline for a cybersecurity workforce and providing students with the expertise to perform senior cybersecurity jobs in the U.S. and around the world; (2) offering educational opportunities to early- and mid-career professionals in cybersecurity fields; (3) providing advanced students with the background necessary to continue their graduate studies for a doctoral degree that focuses on cybersecurity; (4) strengthening ODU's commitment to contributing to the economy and workforce of the Hampton Roads region and the Commonwealth of Virginia; and (5) enhancing the brand awareness of ODU's cybersecurity program worldwide.

Online Delivery

Students who are enrolled in master's degrees are often simultaneously holding down a full-time job and juggling personal responsibilities. The proposed master's degree program would be online, offering students the flexibility to complete coursework on their own time. Students enrolled in the MS in Cybersecurity will be able to access course materials utilizing Blackboard, the University's course management system. All assignment submissions and other course management actions take place in Blackboard. Further, faculty-student interaction is available via email, phone, in-person meetings, and WebEx-interface meetings.

Faculty members who teach in the web-based format are trained in course development and delivery through the Center for Learning and Teaching (CLT). 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. 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 24 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. Online students can remotely connect to the lab facility to conduct various real-world cybersecurity experiments. It will effectively enrich 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.

Old Dominion University has a thirty-year history of delivering robust academic programming through a variety of technologies. In 2014, the University shifted the vast majority of distance learning programs and courses from a satellite and site-based delivery to a fully online delivery.

Over 14,000 degrees have been conferred to students who have been enrolled in ODU's distance learning programs. According to the 2015-2016 Senior Student Satisfaction Survey, 96% of these distance learning students reported that they were satisfied or very satisfied with their ODU experience. It is ranked #2 among Online Colleges in Virginia, according to College Affordability Guide, 2017.[5]

Advisory Board

An advisory board consisting of industry leaders and employers will be formed to advise faculty and to ensure the proposed program is aligned with emerging cybersecurity areas that are relevant to career growth among students.

Old Dominion University will leverage the Hampton Roads Cybersecurity Education, Workforce and Economic Development Alliance (HRCyber) in establishing the board. HRCyber is a partnership among educational institutions, government agencies, nonprofit organizations, and private employers focused on developing educational pathways to provide a capable and fully trained cybersecurity workforce for the region. HRCyber aligns regional educational and skills development offerings with the workforce practices and activities of business and nonprofit organizations within the Hampton Roads region, with the specific goal of supporting local economic development and job growth via establishment of a multi-stakeholder alliance. The alliance focuses on leveraging the National Initiative for Cybersecurity Education (NICE) Framework, addressing cyber workforce needs, training providers conforming to the NICE Framework, and increasing the pipeline of students pursuing cybersecurity careers.

Current membership on HRCyber is available in Appendix A. Several of them have written in support of the proposed program, and will be asked to join the advisory board at ODU.

Admissions Criteria

Criteria for acceptance into the Master of Science in Cybersecurity include the following:

- Online graduate 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 colleges and universities attended
- Undergraduate coursework or equivalent work experience in cybersecurity and/or related areas
- Two letters of recommendation from individuals familiar with the applicant's professional and/or academic background
- A current resume
- A statement of professional goals
- GRE scores, with a 50% or better attainment on quantitative reasoning

[5] http://www.collegeaffordabilityguide.org/

- Current scores on the Test of English as a Foreign Language (TOEFL) of at least 550 from applicants whose native language is not English (waived if an applicant has earned a college degree from an institution in an English-speaking country)

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

The primary candidates for the Master of Science in Cybersecurity are those with managerial career goals in the cybersecurity industry. Other candidates will be those in the U.S. Army, Navy, Air Force, and other branches of the military, individuals working for federal, state, or local government or for government contractors, and international and U.S. students who wish to gain advanced expertise in cybersecurity. Ultimately, the proposed program is designed to produce professionals with the knowledge and experiences necessary to handle the daily challenges in protecting critical cyber infrastructure and assets, and the leadership skills to fill senior cybersecurity positions.

In addition, Old Dominion students enrolled in the interdisciplinary undergraduate major in cybersecurity, the undergraduate major in cyber operations, the undergraduate major in cybercrime, as well as students in undergraduate computer science, computer engineering, information technology, and criminal justice programs who enrolled in the minor in cybersecurity may be keenly interested in the link between their undergraduate program and this proposed program. For many, it will represent a natural progression, particularly if they are currently working in, or have plans to work in, the cybersecurity field.

Curriculum

The M.S. in Cybersecurity is a 30-credit hour program that has been designed to address the advanced educational needs of students and employers in the area of cybersecurity. It will educate students about the theory, technologies, skills, and practices necessary to handle the daily challenges in protecting critical cyber infrastructure and assets. Students will be introduced to many advanced topics of cybersecurity, including information assurance, networked systems security, software reverse engineering, digital forensics, mobile and wireless security, ethical hacking and penetration testing, threat modeling and risk analysis, cybersecurity law and policy, and leadership and management in cybersecurity.

The curriculum will feature emerging topics in the field, and will include many opportunities for students to interact with potential employers through recruitment and networking events. Students will learn how to identify problems, gather information, analyze data, define hypotheses, develop solutions, establish contingencies, and effectively articulate and communicate results. This advanced knowledge will build upon the basic cybersecurity foundation acquired at the undergraduate level or in experiences gained in the industry.

Moreover, extensive studies have revealed the value of interdisciplinary underpinnings of cybersecurity. The field covers more than technical issues; it covers an interdisciplinary approach to cybersecurity matters by incorporating aspects of economics, human psychology, law, policy, and other disciplines. Generally, cybersecurity professionals are interdisciplinary in nature. They typically go through diverse education and career pathways. Few of them have ever earned a cybersecurity degree. To this end, the proposed master's program would have an interdisciplinary curriculum and be administered by the interdisciplinary Center for Cyber Security Education and Research (CCSER). An array of restricted elective courses across multiple disciplines will be offered such that students could choose elective courses based on their different backgrounds, interests, current employment, and future career goals.

This proposed program consists of four core courses (12 credit hours), five electives (15 credit hours), and one capstone course (3 credit hours). The four core courses 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.

The five electives provide students with opportunities to learn about different aspects of cybersecurity, e.g., in information systems, network systems, mobile and wireless systems, operating systems, and cyber-physical systems. Courses are also offered to address such important cybersecurity topics as reverse software engineering, digital forensics, thread modeling, and ethical hacking and penetration testing.

The capstone course, in students' final semester of study, provides opportunities to synthesize knowledge from their previous coursework and apply it to solve real-world cybersecurity problems. The faculty member who teaches the capstone course will work with industrial and academic partners who will serve as external mentors of the capstone course. Each student in the capstone course will discuss—with both faculty member and mentor—development of her/his master's project that aims to solve a cybersecurity problem in a real-world business setting. Students will learn how to quickly gather information, understand the business system, identify problems, define hypotheses, develop solutions, analyze data, and effectively articulate and communicate ideas and results. The capstone course also offers the chance for students to develop design thinking in cyber security and exercise leadership in a team environment.

The project counts as 40% of the total grade of the capstone course. The faculty member who teaches the capstone course will be responsible for grading the project. If a student fails the project, he/she may still pass the course by working with the faculty member to improve selected aspects of the project. Requirements for the Master of Science in Cybersecurity include:

*New course

<u>Foundational Core Courses (12 hours)</u>

*CYSE 600	Cybersecurity Principles	(3 credits)
*CYSE 601	Advanced Cybersecurity Techniques and Operations	(3 credits)
*CRJS/CYSE 603	Advanced Cybersecurity Law and Policy	(3 credits)
*CYSE 605	Leadership and Management in Cybersecurity	(3 credits)

Restricted Elective Courses (15 hours), to be selected in consultation with program advisor. Up to three courses can be selected at 500 level.

CS 565	Information Assurance	(3 credits)
CS 564	Networked Systems Security	(3 credits)
CS/*CYSE 595	Software Reverse Engineering	(3 credits)
*CYSE 607	Advanced Digital Forensics	(3 credits)
*CYSE 615	Mobile and Wireless Security	(3 credits)
*CYSE 625	Advanced Ethical Hacking and Penetration Testing	(3 credits)
ECE 516	Cyber Defense Fundamentals	(3 credits)
ECE 519	Cyber Physical Systems Security	(3 credits)
ENMA 670	Foundations of Cyber Security	(3 credits)
IT 649	Information Systems and Network Security	(3 credits)
MSIM 670	Cyber Systems Engineering	(3 credits)
MSIM 673	Threat Modeling and Risk Analysis	(3 credits)
*CYSE 697	Independent Study in Cybersecurity	(3 credits)
MSIM 773	Networked System Security	(3 credits)

Capstone Core Course (3 hours)

*CYSE 698	Master's Project	(3 credits)

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

Student Retention and Continuation Plan

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

- Requiring an orientation session for all new students, which introduces the program, curriculum, requirements, expectations, faculty, facility, and other relevant resources that are online or remotely accessible through the myODU portal;
- Publishing an up-to-date curriculum and a long-range course schedule to help students plan their enrollment and time to completion;
- Holding advising sessions each semester and providing personalized advising throughout students' program of study;
- Teaming with faculty and industrial partners to mentor students in subject matter and career direction; and
- Encouraging students to join ODU's Cybersecurity Student Association, which hosts meetings regularly for students to share success stories, talk about strategies to complete the program and discuss future career pathways.

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

- Additional advising and mentoring of the student;
- Connecting to a successful local cybersecurity professional as role-model;
- Involvement in state-of-the-art cybersecurity projects to stimulate student's interest; and
- Creating a cohort to increase interactions and peer learning.

To remain in good standing after admission to the program, students must maintain a minimum, cumulative grade point average of 3.0 in all graduate course work attempted at the University. Students who fall below this minimum standard will have 12 credit hours to remedy this deficiency. The graduate program director will work with such students to success, to the degree possible.

Faculty

Ten faculty members affiliated with CCSER hold credentials to teach in the Master of Science in Cybersecurity. They hold tenure or tenure-track positions in four colleges, including the College of Arts and Letters (Sociology and Criminal Justice; Philosophy and Religious Studies), Strome College of Business (Information Technology & Decision Science), Batten College of Engineering and Technology (Electrical and Computer Engineering; Engineering Management and Systems Engineering; Modeling, Simulation and Visualization Engineering), and College of Sciences (Computer Science).

The group includes 3 professors, one of whom serves as the director of CCSER, 4 associate professors and 3 assistant professors. Three of them were recruited recently through ODU's cybersecurity cluster hiring.

The faculty offer a diversity of cybersecurity expertise, 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 90 recent publications (during the past three years) in peer-reviewed journals and conferences in cybersecurity fields. They currently have 15 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, and Department of Energy.

The faculty will work collaboratively to teach the core courses and to mentor students in the proposed program. Brief CVs for existing full time faculty members can be found in Appendix D. Appendix E provides data on grant funding faculty have successfully obtained in this field.

Program Administration

This proposed program would be administered by the Center for Cybersecurity Education and Research (CCSER) and the Graduate School. CCSER was established under the Office of Academic Affairs to weave together disparate threads of programmatic and facility resources at ODU to create a strong education and research program focusing on cybersecurity. It represents

an interdisciplinary effort bringing together faculty, staff, degree programs, certificates, and research initiatives from four colleges, eight academic departments, the Office of Research, the Office of Information Technology Services, and the Virginia Modeling, Analysis and Simulation Center. It consists of about 30 affiliated faculty and staff from across the university. The CCSER also oversees an interdisciplinary undergraduate major in cybersecurity, an undergraduate major in cyber operations, an undergraduate major in cybercrime, as well as an undergraduate minor in cybersecurity.

A tenured CCSER faculty would be appointed as the graduate program director (GPD). She or he will assume responsibility for setting class schedules, coordinating student meetings and activities, gathering students' input, handling students' concerns, providing admission and enrollment information to the Graduate School, and meeting with the faculty, the CCSER director, and dean or associate dean of Graduate School to discuss program matters. He or she will also have teaching responsibilities in the program. A graduate committee, to include the graduate program director and other faculty members at CCSER, will be formed to review applicants for admission, evaluate curriculum in meeting student and employer needs, and conduct regular program assessments.

The administrative assistant in CCSER will support faculty and students in this program.

Student Assessment

Students will be evaluated throughout the program using formative assessments, such as quizzes, tests, cases studies, papers, research project, and presentations. Student learning outcomes cover many of the technical and management competencies that are required for the area of cybersecurity. Specifically, graduates will be able to:

1. Analyze ethical and social issues in the area of cybersecurity to clearly understand ethical standards and rules for cybersecurity professionals and to promote social responsibility;
2. Communicate in writing their understanding of cybersecurity problems and decisions about cyber defense and operations in a cohesive and well-structured manner;
3. Integrate principles and methods from a variety of disciplines to develop and implement best practices to solve cybersecurity complexities;
4. Analyze global cybersecurity problems and make decisions that enhance the effectiveness of cyber defense and operation solutions based on these analyses; and
5. 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.

Map of MS in 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 clearly understand ethical standards and rules for cybersecurity professionals and to promote social responsibility	CYSE 600. Cybersecurity Principles CRJS/CYSE 603. Advanced Cybersecurity Law and Policy	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) CRJS/CYSE 603 • 80% of students will successfully present and debate on alternative methods to accomplish ethics in the cybersecurity industry. (Presentation)
2. **Written Communication** Communicate in writing their understanding of cybersecurity problems and decisions about cyber defense and operations in a cohesive and well-structured manner.	CYSE 600. Cybersecurity Principles CYSE 601. Advanced Cybersecurity Techniques and Operations	CYSE 600 • 80% of students will design a cyber defense plan for a campus network (Research paper) • 90% of students will use cybersecurity principles to analyze vulnerabilities of a given computer system (Exam) 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)

3. Analytical Problem Solving Integrate principles and methods from a variety of disciplines to develop and implement best practices to solve cybersecurity complexities	CYSE 601. Advanced Cybersecurity Techniques and Operations CYSE 698. Master's Project	CYSE 601 • 80% of students will perform a thorough analysis of cybersecurity vulnerabilities in mobile wireless networks. (Group project, presentation, paper) CYSE 698 • 90% of students will solve a cybersecurity problem in a real-world business setting: gather information, understand business systems, analyze data, identify problems, define hypotheses, develop solutions, and articulate and communicate results. (Project, presentation, and report).
4. Global Perspective Analyze global cybersecurity problems and make decisions that enhance the effectiveness of cyber defense and operation solutions based on these analyses	CYSE 600. Cybersecurity Principles CYSE 605. Leadership and Management in Cybersecurity	CYSE 600 • 80% of students will conduct a thorough case study of the global impact of a cyber attack. (Project, presentation and report) CYSE 605 • 90% of students will correctly answer questions about international cybersecurity management. (Exam)
5. Oral Communication Orally communicate their understanding of cybersecurity, and explain decisions in cohesive and well-structured presentations to both technical and non-technical audience	CYSE 605. Leadership and Management in Cybersecurity CYSE 698. Master's Project	CYSE 605 • 90% of students will design a cybersecurity management plan and present it as a group leader. (Presentation) CYSE 698 • 90% of students will articulate cybersecurity problems in a business setting, communicating next steps to technical and non-technical audiences (Project, oral communication and presentation)

Workplace Competencies and Employment Skills

Graduates of the Master of Science in Cybersecurity will have the skills and ability needed for employment and workplace competencies in the field of cybersecurity. Specifically, they will have the:

1. Ability to manage the security complexities present in a wide range of cyber systems, from clouds to the Internet-of-Things
2. Awareness and knowledge of contemporary cybersecurity standards, practices, procedures and methods
3. Understanding of vulnerabilities in common computer systems and networks
4. Strong analytical and diagnostic skills for cyber system risks and vulnerabilities and their economic impacts
5. Demonstrated skills in innovation and collaboration
6. Ability to clearly articulate complex cybersecurity concepts, problems and solutions both written and verbally
7. Presentation and communication skills to effectively communicate with colleagues, management and customers
8. Ability to examine security from a holistic view, including threat modeling, specifications, implementation, testing, vulnerability assessment, and human factors
9. Ability to lead teams for cyber defense and operations

Program Assessment

The program will be assessed by faculty and administrators in CCSER, the Graduate School, and the provost's office. The review will be completed annually in the fall starting from the second year after the program is approved, 2019, 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;
- Curriculum 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 Academic Affairs for review. The Vice Provost will offer guidance, as needed, for improvement, and will provide updates about the review to the Provost.

Old Dominion University maintains a robust program review process for graduate programs; as such, this master's program will have an internal review conducted by external faculty after five years (i.e., in fall of year 6 or 2023). This review will include a self-study, a visit from faculty external to the program, and an action plan developed in concert with the graduate program director, program faculty, and dean and associate dean of Graduate School.

Benchmarks of Success

Benchmarks of success for the Master of Science in Cybersecurity include the following student enrollment and graduate goals:

- 20-30 new students will be admitted each year
- The program will graduate a minimum of 12 students annually by the completion of the program's fourth 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 one year 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
- 80% of employers will be satisfied with the level of education and skill of graduates, as measured by an employer survey administered within one year of hire.

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

The proposed program does not represent an expansion of a concentration or focus area at the master's level at Old Dominion University.

Relationship to Existing ODU Degree Programs

Old Dominion University has no related degree offering in the area of this proposed program at the master's level.

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 fast-growing field creating new jobs over the next decade, as both government and industry make significant 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.

Former national intelligence director, James Clapper, noted that cyber attack ranks highest on worldwide threats to U.S. national security.[6] According to Department of Homeland Security, "The federal enterprise depends on information technology (IT) systems and computer networks for essential operations. These systems face large and diverse cyber threats that range from unsophisticated hackers to technically competent intruders using state-of-the-art intrusion techniques. Many malicious attacks are designed to steal information and disrupt, deny access to, degrade, or destroy critical information systems."[7]

[6] http://www.washingtontimes.com/news/2015/feb/26/james-clapper-intel-chief-cyber-ranks-highest-worl/
[7] https://www.dhs.gov/topic/securing-federal-networks

IBM Corporation's Chairman, CEO and President, Ginni Rometty, said that cybercrime may be the greatest threat to every company in the world.[8] According to an analysis conducted by Cybersecurity Ventures, the global annual cybercrime costs has been estimated at $3 trillion in 2015, and it could reach $6 trillion by 2021.[9] Global spending on cybersecurity products and services for defending against cybercrime is projected to exceed $1 trillion cumulatively over the next five years, from 2017 to 2021, according to the Cybersecurity Market Report, which is published quarterly by Cybersecurity Ventures.[9]

Cyber-attacks not only impact national security and the economy, but also affect individuals personally in their daily lives. For example, in July 2015, hackers stole social security numbers, health records, and other highly sensitive data from 21 million Americans through the Office of Personnel Management in what, at the time, was the largest data breach in U.S. history.[10] In 2017, malware WannaCry affected more than 230,000 users in some 150 countries.[11]

As the volume and sophistication of cyber-attacks grow, there is a surging demand for well-trained cybersecurity workforce to safeguard the cyber space. Dr. Ronald Dodge from the United States Military Academy and Drs. Costis Toregas and Lance Hoffman from The George Washington University noted in their article that "The cybersecurity workforce is one of the most critical employment sectors in the world."[12]

However, recent studies have shown that there is a serious shortage of talent to fill cybersecurity positions. According to a study conducted by Information Systems Audit and Control Association (ISACA), a global leader in cybersecurity, "82 percent of organizations expect to be attacked, but they are relying on a talent pool they view as largely unqualified and unable to handle complex threats or understand their business. More than one in three (35 percent) are unable to fill open positions."[13] According to International Information System Security Certification Consortium's, or (ISC)²'s, Global Information Security Workforce Study, which queried 19,000 cybersecurity professionals worldwide, 66% of survey respondents feel they do not have enough employees to address the increasing level of threats coming their way.[14]

Based on a global survey of 649 cybersecurity and IT managers or practitioners, only 16% feel at least half of their applicants are qualified; 53% say it can take as long as six months to find a

[8] https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#5f8e8fcb3a91
[9] http://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
[10] "U.S. Government Cybersecurity Report", 2016, SecurityScorecard R&D Department, https://cdn2.hubspot.net/hubfs/533449/SecurityScorecard_2016_Govt_Cybersecurity_Report.pdf
[11] "How the WannaCry Attack Will Impact Cyber Security", May 2017, http://knowledge.wharton.upenn.edu/article/massive-global-cyberattack/
[12] Ronald C Dodge, Costis Toregas and, Lance Hoffman, "Cybersecurity Workforce Development Directions", in Proceedings of The Sixth International Symposium on Human Aspects of Information Security & Assurance, 2012.
[13] "State of Cybersecurity: Implications for 2015", An ISACA and RSA Conference Survey, http://www.isaca.org/cyber/Documents/State-of-Cybersecurity_Res_Eng_0415.pdf
[14] "Cybersecurity Faces 1.8 Million Worker Shortfall By 2022", http://www.darkreading.com/careers-and-people/cybersecurity-faces-18-million-worker-shortfall-by-2022/d/d-id/1329084

qualified candidate; and more than a third are left with job openings they cannot fill.[15] According to ESG's annual IT spending intentions research based on 600 IT and cybersecurity professionals, cybersecurity has been identified as the number one "problematic shortage" area across all of IT for the past six years in a row. In 2017, 45% of organizations say they have a "problematic shortage" of cybersecurity skills.[16]

Given the high demand for this cybersecurity workforce and the serious shortage of cybersecurity talent, the proposed program is aimed at filling the gap. While a bachelor's degree in a related field is required for almost all cyber security positions from entry-level and higher, many cybersecurity positions require advanced education and experience. The proposed online interdisciplinary graduate program gives students additional technical, theoretical, leadership, managerial and business skills required in high-level cybersecurity positions. It is on the cutting edge of supporting the growing government and industry demand for qualified cybersecurity professionals. Specific justification related to the proposed graduate degree include the following:

- An advanced degree opens up career options. A report by Burning Glass Technologies showed that 23% of cyber security postings require at least a master's degree.[17] There are high-level job openings in almost every state and across almost every sector, both private and public. For example, right now, approximately 65% of large U.S. companies have a CISO (Chief Information Security Officer) position, up from 50% in 2016, according to the Information Systems Audit and Control Association (ISACA), an independent, nonprofit, global association. Cybersecurity Ventures predicts that 100% of large companies globally will have a CISO position by 2021.[18] The skills and experiences gained through the advanced degree in cybersecurity open up vast opportunities for long-term career advancement.
- Most cybersecurity bachelor's programs focus on fundamental technical knowledge. As part of the master's program, students will be exposed to advanced technologies and leadership skills, along with managerial training. They will learn how to lead and manage teams of IT professionals, including cybersecurity personnel. The proposed program will offer essential knowledge and skills for cybersecurity professionals to advance in their careers and land those senior positions.
- Cybersecurity professionals are well paid, with information assurance specialists averaging $75,000 annually. Further, those with a master's degree have the potential to earn more; for example, an information security manager averages $100,000 a year and a chief information security officer earns about $145,000 annually.[19]

Thus, obtaining a master's degree in cybersecurity is highly desired by professionals in the field. Faculty members at ODU anticipate that graduates of the program will be highly sought-after by employers across the nation and from local organizations and governments in Hampton Roads.

[15] http://www.isaca.org/About-ISACA/Press-room/News-Releases/2015/Pages/Study-82-percent-of-Organizations-Expect-a-Cyberattack-Yet-35-percent-Are-Unable-to-Fill-Open-Security-Jobs.aspx
[16] http://www.csoonline.com/article/3177374/security/cybersecurity-skills-shortage-holding-steady.html
[17] "Job Market Intelligence:Cybersecurity Jobs", http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf
[18] http://cybersecurityventures.com/jobs/
[19] https://news.clearancejobs.com/2016/02/01/8-reasons-to-get-your-masters-degree-in-cybersecurity/

Employment Demand

National/International Focus

The cybersecurity unemployment rate was 0% in 2016, and it is expected to remain there from 2017 to 2021. U.S. News and World Report ranked a career in information security analysis seventh on its list of the 10 best technology jobs for 2017.[20] Further, "The field of cyber security is the least populated of any field of technology," according to John McAfee, founder of McAfee, Inc. "There are two job openings for every qualified candidate."[21]

The high demand for cybersecurity talent has been reported by multiple sources:

- According to CyberSeek, a project supported by the National Initiative for Cybersecurity Education (NICE), a program of the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce, the U.S. employs nearly 780,000 people in cybersecurity positions in 2017, with approximately 350,000 current cybersecurity openings.[21]
- Burning Glass Technologies, an analytics software company powered by the world's largest and most sophisticated database of labor market data, reports that cybersecurity openings are growing three times faster than overall IT postings.[22]
- According to the Bureau of Labor Statistics, the rate of growth for jobs in information security is projected at 18% from 2014–2024, much faster than the average for all other occupations.[23]
- Michael Brown, CEO at Symantec, the world's largest security software vendor, estimates that the demand for cybersecurity professionals is estimated to reach 6 million globally by 2019.[24]
- The ISACA, a non-profit information security advocacy group, predicts there will be a global shortage of two million cyber security professionals by 2019.[8]
- Cybersecurity Ventures predicts there will be 3.5 million unfilled cybersecurity positions globally by 2021.[24]

Virginia Focus

Cybersecurity is among Governor McAuliffe's top priorities for building the New Virginia Economy. There are approximately 36,000 cybersecurity job openings in Virginia – the 2nd highest among all states and the highest in terms of demand concentration.[25]

[20] "Best Technology Jobs", U.S. News, https://money.usnews.com/careers/best-jobs/rankings/best-technology-jobs
[21] http://www.csoonline.com/article/3201974/it-careers/cybersecurity-job-market-statistics.html
[22] http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf
[23] https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm
[24] http://www.csoonline.com/article/2953258/it-careers/cybersecurity-job-market-figures-2015-to-2019-indicate-severe-workforce-shortage.html
[25] http://cyberseek.org/heatmap.html

"At a time when Virginia is home to 36,000 open jobs in the cybersecurity sector, we must do everything we can to encourage students to enter this growing industry," said Governor Terry McAuliffe at an event to announce the recipients of the Commonwealth's first Cybersecurity Public Service Scholarship. "Our problem in Virginia, unlike other states, is we have too many open jobs, high-paying jobs we cannot fill in Virginia today. Standing here today I have 36,000 cyber jobs open. I tell (students) the starting pay is $88,000," McAuliffe said in another event, "We either fill these jobs or they go to other states."

In May, 2015 over 7,500 job openings for cyber-security related occupations were advertised through the Virginia Employment Commission. The number of persons employed in this occupational group in the Commonwealth is expected to increase by 25% from 2012 through 2022. [26]

In May, 2015 over 7,500 job openings for cyber-security related occupations were advertised through the Virginia Employment Commission (VEC). The number of persons employed in this occupational group in the Commonwealth is expected to increase by 25% from 2012 through 2022.[27] The VEC indicated that jobs in this field, such as Information Security Analysts, are abundant. As of August 16, 2017, there were 519 openings for Information Security Analysts and fewer than 100 candidates seeking these positions.[28]

Hampton Roads Focus

The Hampton Roads area includes organizations that are keenly interested in this program. Letters of support from several of these employers may be found in Appendix F.

A survey will be conducted among employers with results of the survey are found in Appendix G.

Appendix H contains current job descriptions and position announcements demonstrating a need for prospective employees with the knowledge that this degree program would provide.

Student Demand

A student/alumni survey will be conducted with results of the survey available in Appendix I.

Following the administration of this survey, xx students offered unsolicited letters of interest in the program. Their letters may be found in Appendix J.

[26]http://www.yesvirginia.org/Content/pdf/Industry%20Profiles/VA%20Cybersecurity%20Summary%202016.pdf

[27]http://www.yesvirginia.org/Content/pdf/Industry%20Profiles/VA%20Cybersecurity%20Summary%202016.pdf

[28]https://data.virginialmi.com/vosnet/lmi/occ/occsummary.aspx?enc=Vdx1uREThVt4ZXZqIde02x70XpsllwN0fJQZHOtORsY0Kpt0r4ot0R85Y5htQjKgPOWJFjC/JGcHVA5YNAJtky6oiKJcV2AzDM0wrIEHXLQ=

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)**		
2018 - 2019		2019 - 2020		2020 - 2021		2021 - 2022			2022 - 2023		
HDCT	FTES	HDCT	FTES	HDCT	FTES	HDCT	FTES	GRAD	HDCT	FTES	GRAD
15	10	25	15	34	28	45	34		50	35	12

Assumptions
Retention: 90%
Part-time students: 60% / Full-time students: 40%
Full-time students credit hours per semester: 12
Part-time students credit hours per semester: 6
Full-time students graduate in 1.5 years
Part-time students graduate in 2.5 years

Duplication

Several master's degree programs are offered in the Commonwealth of Virginia that cover areas similar to the proposed program.

George Mason University (GMU)
George Mason University (GMU) offers a Master of Science in Information Security and Assurance.

Similarities to ODU
One of the three required core courses of the Master of Science in Information Security and Assurance at GMU is ISA 562, Information Security Theory and Practice. The content of the course includes some areas covered in an ODU's core course, CYSE 600, Cybersecurity Principles.

Differences from ODU
The other two core courses in the GMU program are heavily network related, including a course about computer communications and another course about network security. In contrast, the ODU program includes a broad coverage of cybersecurity ranging from cyber operations to cyber laws, policies, and leadership skills. It covers both technical aspects and human factors in cybersecurity.

The GMU program is computer science oriented, housed in the Department of Computer Science, whereas the ODU program takes an interdisciplinary approach, with the courses taught by interdisciplinary faculty from four different colleges.

The GMU program does not include a capstone course, while the ODU program requires a capstone that will focus on a master's project to solve a cybersecurity problem in a real-world business setting. Finally, the GMU program is offered in a traditional format, whereas the ODU program will be available in an online format, with the option for local students to attend classes on campus.

George Mason University also offers a Master of Science in Management of Secure Information Systems and an Executive Master of Business Administration (EMBA) in Critical Infrastructure Protection and Management, through the School of Business. The former focuses on business management aspect of information security. It is run as a cohort with no electives. The entire program has a duration of 16 months including about seven days of study abroad. The latter addresses the analysis and management within critical infrastructure sectors. Its curriculum includes 17 required EMBA courses.

Similarities with GMU M.S. in Management of Secure Information Systems
The GMU program includes a 2-credit course, Foundations of Cyber Security (MSEC 510). The content of the course is partially covered in an ODU's core course, CYSE 600, Cybersecurity Principles. It also includes a 2-credit course, Leadership and Change Management, which includes some areas covered in the ODU's core course, CYSE 605, Leadership and Management in Cybersecurity.

Differences from GMU M.S. in Management of Secure Information Systems
The GMU program is business management oriented, including a variety of courses that focus on enterprise, finance, and management. The proposed M.S. in Cybersecurity has a different goal and target population. It focuses on cybersecurity technologies, covering advanced cybersecurity principles, techniques, and operations, as well as various important cybersecurity topics such as reverse software engineering, digital forensics, thread modeling, and ethical hacking and penetration testing. It aims to produce technical leaders who can take senior cybersecurity positions in a wide range of federal, state and local governments, military agencies, and the private sector, including various senior engineering positions such as cyber security engineers, cyber security architects, and cyber security analysts, that need different skill sets than those taught in the M.S. in Management of Secure Information Systems offered by the School of Business at George Mason University.

Similarities with GMU EMBA in Critical Infrastructure Protection and Management
The content of EMBA 718, Leadership & Change Management, is partially covered in an ODU's core course, CYSE 605, Leadership and Management in Cybersecurity.

Differences from GMU EMBA in Critical Infrastructure Protection and Management
This GMU EMBA program emphasizes business/government coordination to achieve business efficiency, ensure business continuity, and develop capacities to create resilience and

competitive advantage. The program includes 7 modules of EMBA courses. None of them focus on cybersecurity technologies. On the other hand, the ODU program aims to prepare students with deep understanding of cybersecurity technologies and become technical leaders in the field. It covers advanced cybersecurity principles, techniques, and operations, and provides students with opportunities to learn about a diversity of cybersecurity topics such as reverse software engineering, digital forensics, thread modeling, mobile wireless security, and ethical hacking and penetration testing.

Norfolk State University (NSU)
Norfolk State University (NSU) offers a Master of Science in Cybersecurity through the Department of Computer Science.

Similarities with NSU program
The NSU program includes 11 foundation courses, which are all required. One of the courses is CSC 535, Computer Security I. The content of the course is partially covered in an ODU's core course, CYSE 600, Cybersecurity Principles. In addition, the NSU program includes CSC 555, Management of Information Security, which has some areas covered in the ODU's core course, CYSE 605, Leadership and Management in Cybersecurity.

Differences with NSU program
The NSU program has no electives, whereas the proposed ODU program offers 5 elective courses that allow students to learn different aspects of cybersecurity, e.g., in information systems, network systems, mobile and wireless systems, and cyber-physical systems. The elective courses also cover important cybersecurity topics such as reverse software engineering, digital forensics, thread modeling, and ethical hacking and penetration testing.

The ODU program stresses real-world hands-on experience. It includes a lab-based class CYSE 601, Advanced Cybersecurity Techniques and Operations. Moreover, every course in the curriculum involves extensive hands-on activities.

The ODU program emphasizes leadership in cybersecurity, aiming to educate the next generation of technical leaders in the field. The NSU program does not include a course for leadership skills, which is essential for cybersecurity professionals to advance in their careers.

The NSU program is housed in the Computer Science Department, whereas the ODU program takes an interdisciplinary approach. It would be administrated by the interdisciplinary Center for Cybersecurity Education and Research, and the courses would be taught by faculty from four different colleges.

Virginia Commonwealth University (VCU)
Virginia Commonwealth University (VCU) offers a Master of Science in Computer and Information Systems Security through the Department of Computer Science.

Similarities with VCU program
One of the six required core courses of the Master of Science in Computer and Information Systems Security at VCU is CISS/INFO 644, Principles of Computer and Information Systems

Security. The content of the course is partially covered in an ODU's core course, CYSE 600, Cybersecurity Principles. Another VCU core course CISS 634, Ethical, Social and Legal Issues in Computer and Information Systems Security, is similar to an ODU core course CRJS/CYSE 603, Advanced Cybersecurity Law and Policy.

Differences with VCU program

The VCU program has no capstone course, whereas the proposed ODU program includes a required capstone, i.e., a master's project that focuses on solving real-world cybersecurity problems. The faculty member who teaches the capstone course will work with industrial and academic partners who will serve as external mentors of the capstone course. Students will learn how to gather information, understand the business system, identify problems, define hypotheses, develop solutions, analyze data, and effectively articulate and communicate ideas and results.

The VCU program does not include a course about leadership skills, which is essential for cybersecurity professionals to advance in their careers and take senior technical positions. The ODU program emphasizes leadership. It includes a core course CYSE 605, Leadership and Management in Cybersecurity, in order to train the next generation of technical leaders in the field of cybersecurity.

The VCU program is computer science oriented, offered by the Department of Computer Science, whereas the ODU program is based on an interdisciplinary framework. It would be administrated and taught by faculty from different colleges and departments.

Finally, the VCU program is offered in a traditional format, whereas the ODU program will be available online and at the same time allow local students to attend classes on campus.

It is also worth pointing out that the combined graduates of these relevant programs are far behind the workforce demand, which is estimated about 36,000 in the Commonwealth of Virginia.

Enrollment and number of graduates for these programs include the following:[29,30]

GMU	2012-13	2013-14	2014-15	2015-16	2016-17
-MS Info Security and Assurance Enrollments	98	73	78	66	54
-MS Info Security and Assurance Graduates	41	24	32	26	
-MS Mgmt of Secure Information Enrollments	27	19	18	32	21
-MS Mgmt of Secure Information Graduates	27	16	19	29	

[29] http://research.schev.edu/enrollment/E16_report.asp
[30] http://research.schev.edu/Completions/C1Level2_Report.asp

-EMBA Enrollments	86	95	72	72	69
EMBA Graduates	32	39	25	27	
NSU					
-MS Cybersecurity Enrollments				14	49
-MS Cybersecurity Graduates					
VCU					
-MS Computer and IT Sys Security Enrollments	12	12	14	21	16
-MS Computer and IT Sys Security Graduates	6	3	5	5	

Projected Resource Needs for the Proposed Program

Projected Resource Needs

The Center for Cyber Security Education and Research (CCSER) and Old Dominion University have sufficient resources to launch and sustain the proposed program. Specifically, faculty members who have expertise in cybersecurity have been teaching both graduate and undergraduate courses for a number of years. This program successfully presents a graduate degree that provides robust information to students who wish to obtain a credential focused on cybersecurity. It will not compromise existing programs; in fact, it is designed to enhance the breadth of programs in the university.

Full-Time Faculty
No faculty member at the university will have a teaching load that is solely devoted to the proposed program. Each faculty member teaches in undergraduate and graduate programs, as well as general education assignments for their respective departments.

Part-Time Faculty
Ten faculty members at the university, who are affiliated with the CCSER, will teach part-time loads in the proposed program. Combined, they will account for 1.5 FTE faculty when the program is launched. By the target year, the combined part-time faculty members will account for 4.0 FTE faculty. The average salary among these faculty members for 1 FTE is $110,000 plus fringes of $40,810.

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

Graduate Assistants
Two part-time graduate assistants will be required to launch and sustain the program. The cost of each position is $16,000 in salary for two semesters, a total of $32,000 plus FICA in the amount of $2,448.

Classified Positions
A classified person—administrative assistant—who supports CCSER will assist with this program. This person will devote approximately ¼ time to the program, or $7,500 in salary and $2,783 in fringe benefits.

Targeted Financial Aid
No targeted financial aid is projected in launching and operating the program.

Library
No new library resources are required to launch and sustain the program. The University Libraries have adequate resources to support this program from the time it is launched to the target year.

Telecommunications
No new telecommunication equipment or software is needed to launch or sustain the program. With one new faculty member to be hired, an office with a computer and phone are in place.

Equipment (including computers)
No new equipment or related resources are needed to initiate and sustain this proposed program. Computer and peripherals, in addition to a phone, are in place.

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

Other Resources (specify)
No resources other than those described above will be required to launch or operate the proposed Master of Science in Cybersecurity.

PROJECTED RESOURCE NEEDS FOR PROPOSED PROGRAM

Part A: 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

Part B: Fill in the number of FTE and other positions needed for the program

	Program Initiation Year 2018-2019		Expected by Target Enrollment Year 2022-2023	
	On-going and reallocated	**Added (New)**	**Added (New)*** **	**Total FTE positions**
Full-time faculty FTE*				0.00
Part-time faculty FTE**	1.50		2.50	4.00
Adjunct faculty				0.00
Graduate assistants (HDCT)	2.00			2.00
Classified positions	0.25			0.25
TOTAL	3.75	0.00	2.50	6.25

*Faculty dedicated to the program. **Faculty effort can be in the department or split with another unit.

*** Added **after** initiation year

Part C: Estimated resources to initiate and operate the program				
	Program Initiation Year		**Expected by Target Enrollment Year**	
	2018- 2019		**2022- 2023**	
Full-time faculty	0.00	0.00	0.00	0.00
salaries				$0
fringe benefits				$0
Part-time faculty (faculty FTE split with unit(s))	1.50	0.00	2.50	4.00
salaries	$165,000		$275,000	$440,000
fringe benefits	$61,215		$102,025	$163,240
Adjunct faculty	0.00	0.00	0.00	0.00
salaries				$0
fringe benefits				$0
Graduate assistants	2.00	0.00	0.00	2.00
salaries	$32,000			$32,000
fringe benefits	$2,448			$2,448
Classified Positions	0.25	0.00	0.00	0.25
salaries	$7,500			$7,500
fringe benefits	$2,783			$2,783
Personnel cost				
salaries	$204,500	$0	$275,000	$479,500
fringe benefits	$66,446	$0	$102,025	$168,471
Total personnel cost	$270,946	$0	$377,025	$647,971
Equipment				$0
Library				$0
Telecommunication costs				$0
Other costs				$0
TOTAL	**$270,946**	**$0**	**$377,025**	**$647,971**

Part D: 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 2018 – 2019	Target enrollment year 2022 - 2023
Reallocation within the department *(Note below the impact this will have within the department.)*	$75,405	$75,405
Reallocation within the school or college *(Note below the impact this will have within the school or college.)*		
Reallocation within the institution *(Note below the impact this will have within the institution.)*	$195,541	$572,566
Other funding sources *(Specify and note if these are currently available or anticipated.)*		

2. Statement of Impact/Other Funding Sources.

Reallocation within the Department:
The Center for Cyber Security Education and Research (CCSER), in collaboration with the Graduate School, will administer the proposed program. The Director of the CCSER will oversee the program and teach a minimum of one course in the program. Funds from the CCSER will be available at the program's launch and through the target year. In addition, two graduate assistants will assist with this program. The faculty and administration anticipate no negative impact from the implementation of this program.

Reallocation within the Institution:
Most courses in this interdisciplinary program will be taught by faculty from four colleges across the institution. No negative impact is anticipated for any of the colleges or from any other areas of the University.

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

The Hampton Roads Cybersecurity Education, Workforce and Economic Development Alliance (HRCyber)

Members of The Hampton Roads Cybersecurity Education, Workforce and Economic Development Alliance (HRCyber)

Anuswith, Chris
VP Risk Management
ABNB FCU

Armistead, Leigh
President
Peregine Technical Solutions

Bouchard, Joe
Principle
VNA Consulting

Bowden, Dan
VP & CISO
Sentara Healthcare

Burke, Diana
Executive Director
Va Beach Hotel Association

Cook, Steve
Vice President of Workforce Innovation
Opportunity Inc. of Hampton Roads

Crisler, Kane
Director, Technical Operations
Packet Forensics

Dabbs, Derek
CIO
Sera-Brynn

Escobar, Katherine
President
ISSA-HR

Francis, Adrian
Vice President
ISSA-HR

Gracia, Johnny
Founder/CEO
SIMIS Inc

Hegedus, Rob
CEO
Sera-Brynn

Johann, Joe
Senior VP & ISO
Towne Bank

Johnson, Richard
CEO
Rileen Innovation Technologies, Ince

Jones, Gray
Strategic Business Consultant
Klett Consulting

Joseph, Martin
President and CEO
360 IT Partners

Kelly, Patrick
President
CMIT Solutions

Klett, Mark
President and CEO
Klett Consulting

Longe, Mark
Vice President, Business Development
C5BDI

Morgan, Penny
President
AERMOR

Morrozoff, Natalie
Senior Associate
Booz Allen Hamilton

Oppleman, Sasha
Vice President & FSO
Vostrom Holdings, Inc

Page, Grant
Founder & President
MI Systems

Pizzini, Robert
CEO
iFLY

Prevette, Thom
Director of Advocacy and Community Relations
Bon SeCours Health System

Quinn, Joseph
Vice President Navy Fleet Programs
SAIC

Reece, Terry
CISSP-ISSMP Principal
Sera-Brynn

Richmond, Domonick
Manager
Alvarez & Marsal

Rose, Matt
Account Director
Lumos Networks

Runyan, Darich
Senior Director, Terminal Technology
Port of Virginia

Severinghaus, Richard
President and CEO
CRTN Solutions

Spino, Romeo
Co-founder & Executive VP
StratasCorp Technologies

Tomchick, Greg
Security Strategy Analyst
Klett Consulting

Upchurch, Justin
Computer Security Engineer
Hunting Ingalls, NNSY

Villanueva, Ron
President and CEO
StratasCorp Technologies

Watkins, Stephen
VP and Chief Security Strategist
G2 Ops

Weatherly, Michael
Owner
C5BDI

Zeliaman, Steven
Cybersecurity Solutions Architect
SAIC

APPENDIX B

PLANS OF STUDY

Sample Schedule for Full-Time Students

Course	Credits	Category
Fall I		
CYSE 600 Cybersecurity Principles	3	Core
Restricted Elective	3	Elective
Restricted Elective	3	Elective
CRJS/CYSE 603 Advanced Cybersecurity Law and Policy	3	Core
TOTAL 12 credits		
Spring I		
CYSE 601 Advanced Cybersecurity Techniques and Operations	3	Core
CYSE 605 Leadership and Management in Cybersecurity	3	Core
Restricted Elective	3	Elective
Restricted Elective	3	Elective
TOTAL 12 credits		
Fall II		
CYSE 698 Master's Project	3	Capstone
Restricted Elective	3	Elective
TOTAL 6 credits		

Total Required for Degree—30 credits

Sample Schedule for Part-Time Students

Course	Credits	Category
Fall I		
CYSE 600 Cybersecurity Principles	3	Core
CRJS/CYSE 603 Advanced Cybersecurity Law and Policy	3	Core
TOTAL 6 credits		
Spring I		
CYSE 601 Advanced Cybersecurity Techniques and Operations	3	Core
Restricted Elective	3	Elective
TOTAL 6 credits		
Fall II		
CYSE 605 Leadership and Management in Cybersecurity	3	Core
Restricted Elective	3	Elective
TOTAL 6 credits		
Spring II		
Restricted Elective	3	Elective
Restricted Elective	3	Elective
TOTAL 6 credits		
Fall III		
CYSE 698 Master's Project	3	Capstone
Restricted Elective	3	Elective
TOTAL 6 credits		

Total Required for Degree—30 credits

APPENDIX C

COURSE DESCRIPTIONS

Foundational 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, 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 forensic investigation, and practice techniques for penetration testing.

CRJS/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.

Restricted Elective Courses

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 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/CYSE 595 Software Reverse Engineering (3 credits)
This course provides students with the understanding and practice to perform analysis on malware, deduce its design, determine how malware works, and to aid the analysis via disassembly. Students will be able to use a combination of tools (IDAPro, OllyDbg) to safely perform static and dynamic analysis of malware, including encoded, packed, obfuscated ones. Students are expected to have extensive hands-on exercises through in-class practice, homework and projects.

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 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 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.

ECE 516 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.

ECE 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.

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.

IT 624 Information Technology Assurance Services (3 credits)
Standards, ethics, and practice of information technology assurance services particularly as it concerns the governance and control of information systems.

IT 664 Project Management in Information Technology (3 credits)
This course provides basic knowledge of project management including tools to manage scope, time, cost, quality, risk, team, communications and procurement. Special issues in the IT context are emphasized.

IT 685 Introduction to Information Security (3 credits)
Introduction to technical and administrative aspects of information security. Topics include identification and authentication, access control, security models, computer intrusion detection, trust management, cryptography, PKI, fire walls, network security, web security, and secure e-commerce and e-business.

MSIM 673 Threat Modeling and Risk Analysis (3 credits)
This course discusses how to develop cyber threat models using attack graphs/trees, STRIDE, Universal Modeling Language (UML), attack graphs/trees and common of risk analysis tools. Course also discusses the need for quantitative security analysis and formal validation of security models and basic principles of formal model validation.

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

MSIM 773 Networked System Security (3 credits)
Course presents an overview of theory, techniques and protocols that are used to ensure that networks are able to defend themselves and the end-systems that use networks for data and information communication. Modeling of threats to networked systems, attack modeling with attack trees/graphs, cyber physical systems survivability to attacks, and behavior modeling of malware are explored.

Capstone Course

CYSE 698 Master's Project (3 credits)
Individual project directed by the student's professor in major area of study.

APPENDIX D

ABBREVIATED CVs FOR CORE FACULTY

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.

Graham, Rod, PhD, 2009, Sociology, City University of New York. Assistant Professor of Sociology and Criminal Justice. Specialization areas: African American digital practices, digital practice of mobile phones, the role of digital literacy in reducing phishing victimization, exploring the characteristics of Darknet—an anonymous space online.

Haines, Russel, PhD, 2002, Management Information Systems, University of Houston. Associate Professor of Information Technology and Decision Sciences. Specialization areas: Cybersecurity, application development, communication and collaboration systems.

He, Wu, PhD, 2006, Information Science, University of Missouri. Associate Professor of Information Technology and Decision Sciences. Specialization areas: Cyber security, social media, data mining, computational thinking, case-based reasoning, and computing education.

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.

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.

Wang, Cong, PhD, 2017, Electrical and Computer Engineering, State University of New York at Stony Brook. Assistant Professor of Computer Science. Specialization areas: cybersecurity, mobile computing, machine learning, network optimizations and energy-efficiency.

Wu, Hongyi, PhD, 2002, Computer Science, State University of New York at Buffalo. Professor of Electrical and Computer Engineering and Batten Chair of Cybersecurity. Specialization areas: Networked cyber-physical systems for security, safety, and emergency management applications.

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.

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.

APPENDIX E

FUNDED SCHOLARSHIP

Recent research projects funded by federal grants (within 2 years):

- "REU Site: Cybersecurity Research in a Multidisciplinary Environment", NSF, $360,000, March 2017 – Feb. 2020, ChunSheng Xin and Khan Iftekharuddin.
- "On-Demand Spectrum Access: Application-Oriented Dynamic Spectrum Access," NSF, 12/2013 – 08/2017, $498,000, Chunsheng Xin.
- "Enhancing Spectral Access via Directional Spectrum Sensing Employing 3D Cone Filterbanks: Interdisciplinary Algorithms and Prototypes," 12/2013–08/2017, $157K, Chunsheng Xin.
- "Data provenance Assurance in Cloud using Blockchain", AFRL, 08/2016- 3/2017, $100,000, Sachin Shetty.
- "Analyzing and Supporting the Development of the Cyber-insurance Market as a Market-Based Solution for Cyber Resiliency Project", DHS Critical Infrastructure Resilience Institute, 07/2016 - 12/2016, $80,000, Sachin Shetty.
- "Cyber Resilient Energy Delivery Consortium", DOE, 07/2016 - 7/2020, $740,000, Sachin Shetty.
- "Center of Excellence in Cyber Security", DOD OASD, 07/2016 - 3/2020, $480,000, Sachin Shetty.
- "Large-Scale Opportunistic Data Crowdsourcing and Dissemination in Device-to-Device (D2D) Networks", NSF, 08/2015-08/2018, $385,024, Hongyi Wu.
- "Distributed In-network Data Storage and Retrieval in 3D Wireless Sensor Networks", NSF, 09/2013-08/2017, $372,513, Miao Jin and Hongyi Wu.
- "Enhancing Cybersecurity Education Using POGIL", NSF, 09/2016-8/2019, $140,696, Wu He and Xu Li.
- "GenCyber: Preparing Tomorrow's Heroes to Secure the Cyberspace", NSF and NSA, 04/2016-04/2017, $93,061, Wu He, Chunsheng Xin, Dylan Wittkower, Tammi Milliken and Melva Grant.
- "Improving Security Behavior of Employees in Cyberspace through Evidence-based Malware Reports and E-Learning Materials", NSF SaTC, 09/2013-08/2016, $245,460, Wu He, Li Xu, Ling Li, and Ivan Ash.
- "The Effectiveness of Pair Programming for Students with Learning Disabilities" $299,999, NSF, 08/15/2017 – 07/31/2020, Wu He.

Recent publications:

- W. He, X. Tian, and M. Anwar, "Developing and Using Evidence-based E-learning Videos for Cybersecurity Education". KSU Conference on Cybersecurity Education, Research and Practice. October 29-30, 2016. Paper 3.
- M. Anwar, W. He, and X. Yuan, "Employment Status and Cybersecurity Behaviors", The 3rd International Conference on Behavioral, Economic, and Socio-Cultural Computing (BESC), South Point, Durham, NC, USA, November 11-13, 2016.
- X. Yuan, W. He, L. Simpkins, and Y. Liu, "Teaching Security Management for Mobile Devices", The 17th Annual Conference on Information Tech. Education (SIGITE), Boston, 9/28-10/1, 2016.

- D. Brill, A. Dinh, Y. Li, and W. He, "Malware Sequence Alignment", in Proceedings of the 6th IEEE International Conference on Big Data and Cloud Computing, Atlanta, GA, USA, October 8-10, 2016.
- W. He, M. Anwar, I. Ash, X. Yuan, L. Li, and L. Xu, "A Study of Employees' Self-Reported Cybersecurity Behaviors", in Proceedings of the 22nd Americas Conference on Information Systems (AMCIS), San Diego, USA, August 11-13, 2016.
- W. He, X. Tian, J. Shen, and Y. Li, "Understanding Mobile Banking Applications' Security risks through Blog Mining and the Workflow Technology", in Proceedings of the International Conference on Information Systems 2015, Fort Worth, Texas, December 13-16. 2015.
- W. He and X. Yuan, "Behavioral Information Security Research with Emerging Technologies", Journal of Information Privacy and Security, 10(4), 157-159, 2014.
- W. He, A. Kshirsagar, and A. Nwala, "Teaching Information Security with Workflow Technology – A Case Study Approach", Journal of Information Systems Education, 25(3), pp. 201-210, 2014.
- W. He, X. Yuan, and L. Yang, "Supporting Case-based Learning in Information Security with Web-based Technology", Journal of Information Systems Education, 24(1), 31-40, 2013.
- A. Sharah, T. Oyedare, and S. Shetty, "Detecting and Mitigating Smart Insider Jamming Attacks in MANETs Using Reputation-Based Coalition Game", Journal Comp. Network and Communications, 2016.
- P. McNeil, S. Shetty, D. Guntu, and G. Barve, "CREDENT: Scalable Real-time Anomalies Detection and Notification of Targeted Malware in Mobile Devices", in proceedings of The 7th International Conference on Ambient Systems, Networks and Tech., pp. 1219-1225, 2016.
- W. Chen, L. Hong, S. Shetty, D. Lo, R. Cooper, "Cross-Layered Security Approach with Compromised Nodes Detection in Cooperative Sensor Networks", in IPDPS Workshops, pp. 499-508, 2016.
- X. Yuchi and S. Shetty, "Enabling security-aware virtual machine placement in IaaS clouds", in proceedings of MILCOM, pp. 1554-1559, 2015.
- B. Ban, M. Jin, and H. Wu, "Optimal Marching of Autonomous Networked Robots", in *IEEE International Conference on Distributed Computing Systems (ICDCS)*, 2016.
- U. Tatar, B. Bahsi, and A. Gheorghe, "Impact Assessment of Cyber Attacks: A Quantification Study on Power Generation Systems", System of Systems Engineering Conference (SoSE), 2016.
- U. Tatar, B. Karabacak, and A. Gheorghe, "An Assessment Model of Improving National Cyber Security Governance", 11th International Conference on Cyber Warfare and Security, 2016.
- V. Ashok and R. Mukkamala, ``Data Mining Without Data: A Novel Approach to Privacy-preserving Collaborative Data Mining," Workshop on Privacy in the Electromic Society (WEPS 2011), CCS 2011, Chicago, IL, October 2011.

- T. Sayi, R.K.N. Sai Krishna, R. Mukkamala, and P.K. Baruah, ``Privacy Preserving Distribution in Outsourced Environments," HiPC 18th International Conference on High-performance Computing: Student Research Symposium, Bangalore, India, December 2011.
- M. R. Gorai, K.S. Sridharan, T. Aditya, R. Mukkamala, and S. Nukavarapu, ``Employing Bloom Filters for Privacy Preserving Distributed Collaborative kNN Classification," World Congress on Information and Communication Technologies, WICT 2011, Mumbai, India, December 2011.
- S. Tummalapalli, R.K.N. Sai Krishna, R. Mukkamala, P.K. Baruah, "Data outsourcing in cloud environments: A privacy preserving approach," 9th Int. Conf. Information technology: New Generations, April 16-18, Las Vegas, 2012.
- S. Tummalapalli, R.K.N. Sai Krishna, R. Mukkamala, P.K. Baruah, "Privacy Preserving Data Distribution in Outsourced Environments," HiPC 2011, December 18-21, 2011.
- S. Tummalapalli, R.K.N. Sai Krishna, R. Mukkamala, P.K. Baruah, "Privacy Preserving Data Management in Mobile Environments: A partial encryption approach,"13th Intl. Conf. Mobile data Management, MDM 2012, July 23-26, 2012.
- R.K.N. Sai Krishna, S. Tummalapalli, R. Mukkamala, P.K. Baruah, "Efficient Privacy-preserving Data Distribution in Outsourced Environments: A Fragmentation-based Approach," International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2012.
- R.K.N. Sai Krishna, S. Tummalapalli, R. Mukkamala, P.K. Baruah, “Preserving Privacy of Outsourced Data: A Cluster-Based Approach,” 2012 IEEE International Workshop on Data Integration and Mining (DIM-2012), August 8-10, 2012.
- S. Tummalapalli, R.K.N. Sai Krishna, R. Mukkamala, P.K. Baruah, "Data Outsourcing in Cloud Environments: A Privacy Preserving Approach,” ITNG 2012, April 16-18, 2012.
- R. Krishna Prasanth, R. Mukkamala, and P.K. Baruah, "Employing GPU accelerators for efficient enforcement of data integrity in outsourced data," IEEE 19th Intl. Conf. High performance Computing, HiPC 2012, 18-21 Dec, 2012.
- R. Sairam, N. Ramachandran, M. Gorai, R. Mukkamala, and P.K. Baruah, "A computationally efficient and scalable approach for privacy preserving kNN classification," IEEE 19th Intl. Conf. High performance Computing, HiPC 2012, 18-21 Dec, 2012.
- V. Ashok and R. Mukkamala, "A Scalable and Efficient Privacy Preserving Global Itemset Support Approximation using Bloom Filters,"DBSec 2014 : 28th Annual IFIP WG 11.3 Working Conference on Data and Applications Security and Privacy, Vienna, Austria, July 14-16, 2014.
- R. K. Dhandhania, P. K. Baruah, and R. Mukkamala, "Privacy-Preserving Mining of Decision Trees Using Data Negation Approach," International Conference on Contemporary Computing and Informatics (IC3I), Mysore,India, November 2014.
- V. Ashok, K. Navuluri, A. Alhafdhi, and R. Mukkamala, "Dataless Data Mining: Association Rules-based Distributed Privacy-preserving Data Mining," 12th International

Conference on Information Technology: New Generations (ITNG 2015), Las Vegas, NV, April 2015.

- C. Iyer, P. K. Baruah, and R. Mukkamala, "Privacy-preserving frequent itemset mining in outsourced transaction databases," Fourth International Conference on Advances in Computing, Communications, and Informatics," August 10-13, 2015.
- K. Navuluri, R. Mukkamala, and A. Ahmad, "Privacy-aware Big Data Warehouse Architecture," 2016 IEEE International Congress on Big Data (BigData Congress), pp. 341-344, 2016.
- K. Navuluri and R. Mukkamala, "Effect of threat modeling on Identity System Management design," pp. 183-189, 10th MSVESCC, Modeling, Simulation, Visualization Conference, 2016.
- A. Ahmad A. Ahmad and R. Mukkamala, "A Novel Information Privacy Metric," ITNG 2017, April 2017, Springer-Verlag.
- A. Ahmad and R. Mukkamala, "A Layered Model for Understanding and Enforcing Data Privacy," ITNG 2017, April 2017, Springer-Verlag.
- A. Rezaei, D. Zhao, M. Daneshtalab, and H. Wu, "Shift Sprinting: Fine-Grained NoC-based MCSoC Architecture in Dark Silicon Age", in *ACM/IEEE Design Automation Conference (DAC)*, 2016.
- T. Luo, S. Kanhere, H-P. Tan, F. Wu, and H. Wu, "Crowdsourcing with Tullock Contests: A New Perspective", in *IEEE International Conference on Computer Communications (INFOCOM)*, HongKong, China, April 26-May 1, 2015. (Best Paper Award nominee)
- S. Xia, H. Wu, and M. Jin, "Trace-Routing in 3D Wireless Sensor Networks: A Deterministic Approach with Constant Overhead", in *ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, pp. 357-366, Philadelphia, PA, August 11-14, 2014.
- Y. Yang, M. Jin, and H. Wu, "3D Surface Localization with Terrain Model", in *IEEE International Conference on Computer Communications (INFOCOM)*, pp. 46-54, 2014.
- H. Zhou, S. Xia, M. Jin and H. Wu, "Localized and Precise Boundary Detection in 3D Wire- less Sensor Networks", in *IEEE/ACM Trans. on Networking*, Vol. 23, No. 6, pp. 1742-1754, 2015.
- Y. Yang, M. Jin, Y. Zhao, and H. Wu, "Distributed Information Storage and Retrieval in 3D Sensor Networks with General Topologies", in *IEEE/ACM Transactions on Networking*, Vol. 23, No. 4, pp. 1149-1162, 2015.
- J. Backens, C. Xin, M. Song, "A Novel Protocol for Transparent and Simultaneous Spectrum Access between the Secondary User and the Primary User in Cognitive Radio Networks," Elsevier Computer Communications, vol. 69(9), p. 98-106, Sep. 2015.
- C. Xin and M. Song, "An Application-Oriented Spectrum Sharing Architecture," IEEE Transactions on Wireless Communications, vol. 14(5), p. 2394-2401, May 2015.

- J. Backens, C. Xin, M. Song, and C. Cheng, "DSCA: Dynamic Spectrum Co-Access between the Primary Users and the Secondary Users," IEEE Transactions on Vehicular Technology, vol. 64(2), p. 668-676, Feb. 2015.
- C. Cheng, M. Song, and C. Xin, "CoPD: A Conjugate Prior based Detection Scheme to Countermeasure Spectrum Sensing Data Falsification Attacks in Cognitive Radio Networks," Springer Wireless Networks, vol. 20(8), p. 2521-2528, Nov. 2014.
- C. Xin and M. Song, "Detection of PUE Attacks in Cognitive Radio Networks based on Signal Activity Pattern," IEEE Transactions on Mobile Computing, vol. 13(5), p. 1022 - 1034, May 2014.

APPENDIX F

SUPPORT LETTERS

APPENDIX G

EMPLOYER SURVEY

MS in Cybersecurity

Results of Employer Survey

A survey was sent via email to 51 employers to ascertain interest in hiring individuals who earn the Master of Science in Cybersecurity. The survey was conducted between September 5 and 22, 2017. The results of the survey are summarized as follows:

- A total of 16 potential employers responded to the survey about their interest in the MS program in Cybersecurity.
- All employers reported being somewhat interested (25%) or very interested (75%) in hiring an applicant with the MS in Cybersecurity.

	Not at all interested % (n)	**Not very interested % (n)**	**Somewhat interested % (n)**	**Very interested % (n)**
How interested would your organization be in hiring an applicant with the MS in Cybersecurity described on the previous page?	0% (0)	0% (0)	25% (4)	75% (12)

- A majority (87.6%) of employers said they would be somewhat likely (18.8%) or very likely (68.8%) to hire an applicant with M.S. in Cybersecurity from ODU.

	Not at all likely % (n)	**Not very likely % (n)**	**Somewhat likely % (n)**	**Very likely % (n)**
What is the likelihood that you would hire an applicant with M.S. in Cybersecurity from ODU if that applicant met all other hiring requirements?	12.5% (2)	0% (0)	18.8% (3)	68.8% (11)

- All of the organizations responding indicated they needed skills that were difficult to find in the typical applicant pool.
- Of those who indicated that they needed skills that are difficult to find, 93.8 percent felt that the MS degree in Cybersecurity addresses some of those needed skills.

	Yes % (n)
Does your organization need skills that are difficult to find in the typical applicant pool?	100% (16)
Does the M.S. in Cybersecurity address some of the those needed skills?	93.8% (15)

- When responding employers were asked about what type of organization or industry they work in, IT (62.5%), Military (62.5%), and Federal, State, or Local Government (50%) were the most frequently selected industries.

What type of organization/industry do you work? Check all that apply.	**Yes % (n)**
Healthcare	6.3% (1)
IT	62.5% (10)
Finance	6.3% (1)
Military	62.5% (10)
Education	12.5% (2)
Federal, State, Local Government	50% (8)
Energy	6.3% (1)
Other	6.3% (1)

- All employers were from organizations located in Virginia. A majority of them (93.8%) are based in the Hampton Roads.

APPENDIX H

JOB ANNOUNCEMENTS

APPENDIX I

STUDENT DEMAND SURVEY

MS in Cybersecurity

Results of Student Survey

A survey was sent via email to 1603 undergraduate students at ODU, majoring in Cybersecurity, Computer Science, Electrical and Computer Engineering, and Information Technologies. The survey was conducted between September 5 and 22, 2017. The results of the survey are outlined below:

- A total of 286 current students responded to the survey about the proposed MS degree in Cybersecurity.
- Most students (85.3%) reported being somewhat interested (27.6%) or very interested (57.7%) in pursuing graduate education in general.
- Most responding students (84%) indicated they were somewhat interested (43.4%) or very interested (40.6%) in the MS in Cybersecurity degree.
- When asked about the likelihood of applying for admission to the MS program in Cybersecurity, 169 students said they were somewhat likely (97) or very likely (72) to apply.

	Not at all interested % (n)	**Not very interested % (n)**	**Somewhat interested % (n)**	**Very interested % (n)**	**Not Sure % (n)**
What is your level of interest in pursuing graduate education in general?	1.0% (3)	2.4% (7)	27.6% (79)	57.7% (165)	10.8% (31)
What is your level of interest in the M.S. in Cybersecurity described above?	2.1% (6)	4.9% (14)	43.4% (124)	40.6% (116)	9.1% (26)
What is the likelihood that you would enroll in the M.S. in Cybersecurity at ODU?	5.6% (16)	9.8% (28)	33.9% (97)	25.2% (72)	25.5% (73)

- 44.8 percent of the respondents indicated they would use the MS degree in Business and Industry.
- Furthermore, 26.2 percent said they would use the degree in the Public Sector/Federal, State, or Local Government, 7.7 percent reported wanting to use the degree in Academia/University or 4-year College, and 3.8 indicated they would use the degree in military.
- If admitted, about 52.8% expect to enroll full-time (3 or 4 classes a semester) and 31.8% expect to be part-time students (1 or 2 classes a semester).

Would you use the MS degree in:	Yes % (n)
Academia/University or 4-year College	7.7% (22)
Business and Industry	44.8% (128)
Public Sector/Federal, State, or Local Government	26.2% (75)
Not-For-Profit Organizations and Public Advocacy	0.7% (2)
Military	3.8% (11)
Other	1.0% (3)

- The opportunity to achieve professional goals (63.6%), the opportunity to expand working knowledge of cybersecurity (50.3%), the availability of online courses (43.4%), and the opportunity to work in the private sector (41.6%) were the most commonly selected factors that would influence students' decision to pursue an MS in Cybersecurity.

Which of the following factors would influence your decision to pursue a MS in Maritime Trade and Supply Chain Management?	Yes % (n)
Opportunity to achieve professional goals	63.6% (182)
Opportunity to work in the private sector	41.6% (119)
Opportunity to work in the public sector	30.8% (88)
Proximity of the campus to where I work/live	23.8% (68)
Reputation of faculty	19.2% (55)
Opportunity to conduct research with a faculty member	19.9% (57)
Availability of graduate assistantships	25.9% (74)
Availability of night courses	26.2% (75)
Availability of online courses	43.4% (124)
Opportunity to expand working knowledge of cybersecurity	50.3% (144)

- Most students (81.8%) agree (43.7%) or strongly agree (38.1%) that the proposed M.S. in Cybersecurity would meet their expectations for courses in a Master's program.
- Most students (82.2%) agree (38.8%) or strongly agree (43.4%) that the proposed M.S. in Cybersecurity would prepare professionals to be competitive in the field.
- Most students (82.2%) agree (34.3%) or strongly agree (47.9%) that the proposed M.S. in Cybersecurity would help them advance in their career.

	Disagree % (n)	**Agree % (n)**	**Strongly Agree % (n)**
The M.S. in Cybersecurity described above would meet my expectations for courses in a Master's program	1.7% (5)	43.7% (125)	38.1% (109)
The M.S. in Cybersecurity described above would prepare professionals to be competitive in the field	1.0% (3)	38.8% (111)	43.4% (124)
The M.S. in Cybersecurity described above would help me advance in my career	0.3% (1)	34.3% (98)	47.9% (137)

- Most respondents were junior (30.4%) and senior (28.0%) students.

Check all degrees that you currently hold:	**Yes % (n)**
Freshman	16.1% (46)
Sophomore	10.1% (29)
Junior	30.4% (87)
Senior	28.0% (80)
Other	0.7% (2)

APPENDIX J

STUDENT LETTERS OF INTEREST