MEMORANDUM

TO: Members of the Academic and Research Advancement Committee of the Board of Visitors

Michael J. Henry, Chair
Toykea S. Jones, Vice Chair
Carlton F. Bennett, *(ex-officio)*
Lisa B. Smith, *(ex-officio)*
R. Bruce Bradley
Jerri F. Dickseski
Alton J. Harris
Frank Reidy
Maurice D. Slaughter
Andres Sousa-Poza *(Faculty Representative)*

FROM: Augustine O. Agho
Provost

DATE: November 27, 2017

The purpose of this memorandum is to provide you with background information for our meeting on Thursday, December 7, 2017. The committee will meet from 10:00-11:30 a.m. in the Kate and John R. Broderick Dining Commons, Committee Room A (Room 2203).

I. Approval of Minutes of the September 21, 2017 Meeting

The minutes of the September 21, 2017 meeting will be presented for approval as previously distributed.

II. Closed Session

The members of the Academic and Research Advancement Committee will receive information related to the items to be discussed in closed session.

III. Reconvene in Open Session and Vote on Resolutions

IV. Consent Agenda

Included in the consent agenda materials are resolutions recommending five faculty appointments, 15 administrative appointments, three emeritus appointments, and the appointment of the Louis I. Jaffe Professor in Arts and Letters.

V. Vote on Consent Agenda Resolutions

VI. Regular Agenda

The regular agenda includes a proposal for a Master of Science degree program in cybersecurity.

VII. Vote on Regular Agenda Resolution

VIII. Information Items

Information items include a request for a leave of absence without compensation, the report from the Provost, and the report from the Vice President for Research. The report from the Provost will include information on program additions and discontinuations since 2011 and faculty salary data. The report from the Vice President for Research will include information on GO Virginia and the Virginia Research Investment Fund.

VII. Topics of Interest to Board of Visitors Members

Committee members will have an opportunity to discuss topics of interest.

C: John R. Broderick
Donna Meeks

OLD DOMINION UNIVERSITY
BOARD OF VISITORS
ACADEMIC AND RESEARCH ADVANCEMENT COMMITTEE
DECEMBER 7, 2017
AGENDA
REVISED

10:00-11:30 a.m. – Kate and John R. Broderick Dining Commons, Committee Room A (Room 2203)

I. APPROVAL OF THE MINUTES OF SEPTEMBER 21, 2017

II. CLOSED SESSION

III. RECONVENE IN OPEN SESSION AND VOTE ON RESOLUTIONS

IV. CONSENT AGENDA

A. Faculty Appointments (p. 4-5)
B. Administrative Appointments (p. 6-9)
C. Emeritus Appointments (p. 10-12)
D. Appointment of the Louis I. Jaffe Professor in Arts and Letters (p. 13)

V. VOTE ON CONSENT AGENDA RESOLUTIONS

VI. REGULAR AGENDA

A. Proposal for a Master of Science Degree Program in Cybersecurity (p. 14-44)
B. Proposal to Rename the Center for Economic Analysis and Policy to Dragas Center for Economic Analysis and Policy (p. 44a)

VII. VOTE ON REGULAR AGENDA RESOLUTION

VIII. INFORMATION ITEMS

A. Request for Leave of Absence without Compensation (p. 45)
B. Report from the Provost
    1. Information on program additions and discontinuations since 2011
    2. Faculty Salary Data
C. Report from the Vice President for Research
    1. Information on GO Virginia and the Virginia Research Investment Fund

IX. TOPICS OF INTEREST TO BOARD OF VISITORS MEMBERS

December 7, 2017

FACULTY APPOINTMENTS

RESOLVED that, upon the recommendation of the Academic and Research Advancement Committee, the Board of Visitors approves the following faculty appointments.

Name and Rank	Salary	Effective Date	Term
Dr. Amelia M. Anderson Assistant Professor of STEM Education and Professional Studies Tenure Track	$64,000	7/25/18	10 mos

Dr. Anderson received a Ph.D. in Information Studies and an M.S. in Library and Information Studies from Florida State University and a B.S. in Journalism and Communications from the University of Florida. Previously she was a Lead Instructor at Florida State University's School of Information.

Dr. Peter B. Baker Lecturer and Curriculum Coordinator College of Continuing Education and Professional Development	$66,950	9/10/17	12 mos

Dr. Baker received a Ph.D. in Curriculum and Instruction and an M.S. in General Secondary Education from Old Dominion University and a B.A. in English Literature and Composition from the College of William and Mary. Previously he was a Lecturer in the College of Continuing Education and Professional Development and the Department of Teaching and Learning at Old Dominion University. (new position)

Ms. Sara Barger Lecturer of Communication and Theatre Arts	$27,500	12/25/17	5 mos

Ms. Barger received an M.A. in Journalism and Public Affairs and a B.A. in Visual Media and Political Science from The American University. Previously she was Video Editor and Videographer at Creative Associates International and a Video Production Consultant.

Dr. Yun Chen Post-Doctoral Research Associate in Mathematics and Statistics	$40,000	10/25/17	10 mos

Dr. Chen received a Ph.D. in Mathematics from Sun Yat-sen University, an M.S. in Applied Mathematics from Shantou University and a B.S. in Applied Mathematics from

Hulunbuir College, China. Previously he was a Research Assistant at City University of Hong Kong, China. (new position)

Dr. Kristian Petersen Assistant Professor of Philosophy and Religious Studies Tenure Track	$59,038	7/25/18	10 mos

Dr. Petersen received a Ph.D. in Near and Middle Eastern Studies from the University of Washington, an M.A. in Religious Studies from the University of Colorado and a B.A. in Religious Studies from Stony Brook University. Previously he was Assistant Professor in the Department of Religious Studies at the University of Nebraska Omaha.

December 7, 2017

ADMINISTRATIVE FACULTY APPOINTMENTS

RESOLVED that, upon the recommendation of the Academic and Research Advancement Committee, the Board of Visitors approves the following administrative faculty appointments.

Name and Rank	Salary	Effective Date	Term
Ms. Susan Boyd Interim Director of Administration, Housing and Residence Life and Instructor	$81,600	10/25/17	12 mos

Ms. Boyd earned a B.S. in Business Administration from the College of New Jersey and an M.S. in Organizational Behavior from the University of Hartford. She previously served as the Assistant to the Dean of Students at Old Dominion University.

Mr. Robert Cooper III Counselor Coordinator, Upward Bound and Instructor	$43,000	11/13/17	12 mos

Mr. Cooper received an M.A. in Christian Education from Virginia Union University. Previously, he served as the Coordinator for Student Leadership, Involvement, and Community Engagement for Tidewater Community College's Portsmouth campus.

Dr. Joshua DeSilva Psychologist/Groups Coordinator and Assistant Professor	$62,000	10/25/17	12 mos

Dr. DeSilva earned a B.A. in Liberal Arts and an M.Psy. and Psy.D from George Washington University. Previously, he worked as a licensed psychologist for the Potomac Center in Washington, DC.

Mr. Rohit Dalal International Admissions and Recruitment Coordinator and Instructor	$37,871	9/25/17	12 mos

Mr. Dalal earned an M.B.A. from Old Dominion University. He previously worked as the Enrollment Planning and Data Analyst for the University's Department of Enrollment Management.

Ms. Katie Ferrara Academic Success Coordinator, Advising Administration and Academic Partnerships and Instructor	$47,000	10/10/17	12 mos

Ms. Ferrara earned an M.S.Ed. in School Counseling from Old Dominion University. Previously, she worked as the Student Success Advisor for the University's Office of Advising and Transfer Programs.

Mr. Spencer Grubbs Assistant Recruiting Coordinator, Football and Assistant Instructor	$30,000	9/11/17	12 mos

Mr. Grubbs received a B.S. in Sports Management from the University of Tennessee. Previously, he worked as a football operations student worker at the University of Tennessee.

Mr. Matthew Hart Student Success Director, Distance Learning and Instructor	$53,040	11/25/17	12 mos

Mr. Hart obtained a B.S. in Occupational and Technical Studies from Old Dominion University and an M.A. in Business Management and Leadership from Liberty University. Previously, he was the Assistant Director of Student Activities at Southwest Virginia Community College and an Enrollment and Operations Coordinator with ODUOnline.

Ms. Dorianne Johnson Athletic Academic Advisor and Instructor	$45,000	11/25/17	12 mos

Ms. Johnson earned a B.A. in Journalism from the University of Mississippi and an M.S. in Human Development from Alabama A&M University. Previously, she worked as the Athletic Director for Wilberforce University.

Ms. Krista Kimme Major Gift Officer and Instructor	$83,000	11/25/17	12 mos

Ms. Kimme received a B.S. in Community Health and an M.B.A. from the University of Illinois, Urbana-Champaign. Previously, she worked as the Associate Director of Development in the Applied Health Sciences Department and Chief Advancement Officer at the University of Illinois.

Dr. Amy Moynihan Senior Development Writer, Office of Development and Assistant Professor	$75,000	10/25/17	12 mos

Dr. Moynihan received a B.A. in History from Columbia University and an M.S.Ed. and Ph.D. in Higher Education from the University of Virginia. Previously, she worked as a higher education consultant and grant writer for various organizations in Bristol, TN.

Ms. Yalana Orr Student Success Director, Distance Learning and Instructor	$53,040	11/25/17	12 mos

Ms. Orr received a B.A. in Psychology from Hampton University and an M.S.W. from Michigan State University. Previously, she served as the Recruiting Counselor at Nash Community College and as an Academic Advisor at East Carolina University.

Ms. Melissa Turnage Interim Coordinator of Fitness and Wellness and Assistant Instructor	$38,500	10/25/17	12 mos

Ms. Turnage received a B.S. in Recreation and Tourism Studies from Old Dominion University. Previously she was a graduate assistant in the Department of Recreation and Wellness at Old Dominion University.

Ms. Reda Valentin Enrollment Planning and Data Analyst, Office of Enrollment Management and Assistant Instructor	$52,000	10/10/17	12 mos

Ms. Valentin received a B.A. in Psychology from San Diego State University. Previously, she served as an intern for the Office of Assessment and Planning and as an administrative assistant for the Office of Student Outreach and Support at Old Dominion.

Ms. Merideth Warinner Athletics Operations and Events Coordinator, Division of Athletics and Assistant Instructor	$35,700	10/4/17	12 mos

Ms. Warinner received a B.S. in Sports Management from the University of Kansas. Previously, she worked as the Assistant Marketing Director for RDP Food Services in Columbus, OH.

Mr. Bill Williams Assistant Diving Coach and Assistant Instructor	$28,000	10/10/17	12 mos

Mr. Williams earned a B.S. in Sports Administration from Lock Haven University of Pennsylvania. Previously, he worked as a camp coach for the University of Texas.

December 7, 2017

EMERITUS APPOINTMENTS

RESOLVED that, upon the recommendation of the Academic and Research Advancement Committee, the Board of Visitors approves the granting of the title of emeritus to the following faculty members. A summary of their accomplishments is included.

Name and Rank	Effective Date
Stephen Knott Senior Lecturer Emeritus of Human Movement Sciences	July 24, 2017
John R. McConaugha Associate Professor Emeritus of Ocean, Earth and Atmospheric Sciences	January 1, 2018
Marek Wermus Associate Professor Emeritus of Information Technology and Decision Sciences	January 1, 2018

STEPHEN KNOTT

Stephen E. Knott received a B.S. in Health and Physical Education from Old Dominion University in 1972 and a Ph.D. in Curriculum and Instruction from Old Dominion University in 2016. He joined Old Dominion University as a Lecturer of Health and Physical Education in 2006 and achieved the rank of Senior Lecturer in 2012. Recognition of his teaching accomplishments included numerous "Shining Star" awards, which are student-nominated awards given to faculty. In 2016, Knott was selected for the "Most Inspiring Faculty Award" by the top undergraduate scholar in the Darden College of Education. He was also awarded "Game Day Professor" for the women's lacrosse team in 2017.

Knott served as Health and Physical Education Undergraduate Program Coordinator for 11 years. During this time the program developed into one of the largest Health and Physical Education Teacher Preparation programs in the Commonwealth of Virginia. He was instrumental in the development of the Coaching Education minor as well as the Coaching emphasis area in the Physical Education master's program. He also served on numerous committees, led the accreditation process for the Health and Physical Education Teacher Preparation program, and represented Old Dominion University at the Virginia Department of Education's Virginia-NCATE SPA Alignment Initiative.

Knott represented Old Dominion University in the community by working with several school divisions on professional development activities. Additionally, he developed a coaching efficacy scale for the Virginia High School League to use in assessing the effectiveness of their coaching education course, and he spearheaded the development of a coaching education partnership with the Children's Hospital of the King's Daughters. Moreover, he presented his work and research at several state and national conferences, and he served as a Vice President for the Virginia Association for Health, Physical Education, Recreation, and Dance.

JOHN R. MCCONAUGHA

John McConaugha, Associate Professor of Ocean, Earth and Atmospheric Sciences, received a B.S. in Biology from the University of Miami and a Ph.D. in Biology from the University of Southern California. Following post-doctoral training at Duke University, he joined the faculty at Old Dominion University in 1980. He has served on numerous state and regional scientific and fisheries management committees including a gubernatorial appointment to the Virginia Marine Resources Committee. Besides teaching numerous undergraduate and graduate courses throughout his career, McConaugha served as the chair of six Ph.D. student dissertation committees and served on an additional 13 dissertation committees. He also advised 18 master's students and served on 13 additional master's student committees. For the past 20 years, he has worked on developing skills in K-12 teacher candidates in an effort to improve science education at the elementary school level.

McConaugha's research interests center on invertebrate reproduction and larval biology with a specialization in blue crab biology and fisheries management. His laboratory was instrumental in determining that blue crab larvae exit the Chesapeake Bay to complete their development, previously a gap in the knowledge of the blue crab lifecycle. To fund these research efforts he obtained more than $3 million in external funding throughout his career. This resulted in over 90 publications, technical reports and published abstracts with more than 1200 citations in the scientific literature and more than 100 presentations at scientific meetings.

McConaugha served as Assistant Chair of the Oceanography Department for nine years and as the Chief Departmental Advisor for the department for 10 years. Part of his duties as Assistant Chair included serving as planning and construction advisor for the department in the construction of the Physics/Oceanography building.

MAREK WERMUS

Marek Wermus, Associate Professor of Information Technology and Decision Sciences, received an M.S. in Mathematics and a Ph.D. in Economics from the Technical University of Wroclaw, Poland. He joined Old Dominion as an Assistant Professor of Decision Sciences in 1982 and achieved the rank of Associate Professor with tenure in 1987.

Wermus played a significant role in developing, updating and facilitating the Business Analytics and Operations Management discipline. He taught business analytics and operations management to thousands of business students and mentored many junior professors who joined

the department after him. He served as the Business Analytics Discipline coordinator from 2015-2017.

Wermus was actively involved in scholarly work. He is a principal investigator or co-principal investigator of several externally funded research projects that have a total amount of $3,173,000. He published 19 peer-reviewed journal articles, two book chapters, and made 36 research presentations at academic conferences.

Wermus played a significant role in serving Old Dominion University and the professional community. He was a faculty senator for many years and served on the university library committee, department P&T committee, portfolio review committee, recruiting committee, and many others. He coordinated Research Seminar Series and served as the faculty advisor of ODU Student Chapter of American Production and Inventory Society (APICS).

December 7, 2017

APPOINTMENT OF THE LOUIS I. JAFFE PROFESSOR
COLLEGE OF ARTS AND LETTERS

RESOLVED that, upon the recommendation of the Academic and Research Advancement Committee, the Board of Visitors approves the appointment of Dana Heller as the 2017-2020 Louis I. Jaffe Professor in Arts and Letters. A summary of her career is included below for information purposes.

The Jaffe Professorship recognizes an individual who is an outstanding faculty scholar in the College of Arts and Letters who has exhibited sustained excellence in teaching and/or research as well as a continuing, exemplary commitment to the university.

Dana Heller joined Old Dominion University in 1990 and currently serves as Eminent Scholar and Professor of English. She received the Conference of Southern Graduate Schools Achievement Award for New Scholars in 1995, the State Council of Higher Education for Virginia Outstanding Faculty Award in 1997, the Burgess Award for Research and Creativity in the College of Arts and Letters in 2007, and the John R. Broderick Diversity Champion Award in 2016.

Heller has published nine books, 24 refereed articles, 24 chapters, and a variety of other works. Her books have been published by high quality academic presses, and her articles and chapters have appeared in several prominent outlets in her specialty areas. Her scholarly contributions also extend into the classroom, where she is recognized as a superb teacher. Heller's administrative appointments include Director of the Humanities Institute and Graduate Programs, Chair of the Department of English, and Interim Dean of the College of Arts and Letters.

December 7, 2017

APPROVAL OF A NEW MASTER OF SCIENCE DEGREE PROGRAM IN CYBERSECURITY

RESOLVED that, upon the recommendation of the Academic and Research Advancement Committee, the Board of Visitors approves the proposal for a new Master of Science program in Cybersecurity to be effective with the fall 2018 semester.

Rationale: Old Dominion University seeks approval to initiate a Master of Science in Cybersecurity. The program 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.

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; and
- 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.

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 _____ School(s) or college(s) of The Graduate School Campus(es) or off-campus site(s) Main Campus, Norfolk Mode(s) of delivery: face-to-face __X___ distance (51% or more web-based)__X__ hybrid (both face-to-face and distance) _____	
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	

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.

This proposed MS in Cybersecurity program is designed to educate students to develop solid solutions to secure the cyber space of individuals and organizations in various sectors of industry, military, and government. The program will prepare students with a deep understanding of cyber systems, cyber threats, and cyber defense and operation technologies. The program will offer coursework to introduce the state-of-the-art techniques and to address the existing challenges in 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. Graduates will be knowledgeable in the theory, technologies, skills, and practices necessary to handle the daily challenges in protecting critical cyber infrastructure and assets. Students will learn oral and written communication skills to articulate cybersecurity problems and decisions in a cohesive and well-structured way. Students will clearly understand ethical standards and rules for cybersecurity professionals and to promote social responsibility.

Students will be educated to develop skills and competencies in 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 projects and coordination of cyber operation teams. The program will prepare graduates to work within the cybersecurity industry, U.S. Army, Navy, Air Force, and other branches of the military, and the federal, state, or local government or government contractors. Graduates will fill the demand for senior technical positions such as cyber security project managers, principal cyber security engineer, senior security analyst, chief information security officer, cybersecurity data scientist, computer network defense lead, senior cybersecurity systems architect, just to name a few. The program will also prepare students to teach cybersecurity courses in 2-year colleges and 4-year universities.

The proposed MS in Cybersecurity program responds to the urgent need for cybersecurity professionals in the Commonwealth of Virginia, the nation, and the world. “During the first half of 2017 there were 918 data breaches worldwide, compared with 815 in the last six months of 2016”, according to the latest findings by digital security provider Gemalto. “The rise is far more dramatic in terms of the number of records involved. Some 1.9 billion data records were lost or stolen during the first half, compared with 721 million during the previous six months, an increase of 164%. There were 22 breaches in which more than 1 million records were compromised, stolen, or lost in the first half of 2017.”[1] For example, the Equifax data breach alone could affect 143 million people in the US including 4 million in Virginia.[2] The proposed

[1] “Findings from the first half of 2017 Breach Level Index”, Page 3, Gemalto, http://breachlevelindex.com/assets/Breach-Level-Index-Report-H1-2017-Gemalto.pdf

[2] Daily Press, http://www.dailypress.com/news/dp-nws-virginia-equifax-breach-20170914-story.html

degree program will contribute to addressing such cybersecurity problems by preparing students to understand cybersecurity threats and develop more robust cyber defense systems. They will become the next generation in the cybersecurity workforce to safeguard information relating to national security and various sensitive business and personnel data.

Executive Order Thirty-Nine from the Governor of Virginia's states: "Cyber security instruction, training, and programs will be requisite components to prepare those currently seeking new occupational options as well as the next generation for the rapidly developing cyber security workplace. Focusing on cutting edge education and training will be essential for Virginia's cyber security workforce and economic development as occupations in the cyber security industry are highly in demand and among the fastest growing in the economy."[3] 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 address the multifaceted cybersecurity problems,[4] which require an advanced education to develop skillsets that not only cover basic cybersecurity coursework but that will also provide students with multidisciplinary perspectives to examine security from a holistic view. The proposed program will prepare students with the ability to manage the security complexities present in a wide range of cyber systems, to analyze and diagnose cyber system risks and vulnerabilities, to clearly articulate complex cybersecurity problems and solutions, and to lead projects and teams for cyber defense and operations.

Rationale for the Program at Old Dominion University

Old Dominion University has led the effort to establish the Hampton Roads Cybersecurity Education, Workforce and Economic Development Alliance (HRCyber).[5] 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 skill 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 to conform to the NICE Framework, and increasing the pipeline of students pursuing cybersecurity careers. HRCyber makes ODU an ideal place to host the proposed Master of Science in Cybersecurity.

[3] "Commonwealth of Virginia Office of the Governor Executive Order Number Thirty Nine", Page 2, https://governor.virginia.gov/media/3627/eo39-launching-cyber-virginia-and-the-virginia-cyber-security-commissionada.pdf.

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

[5] http://securitybehavior.com/hrcyber/

Mission

The Master of Science in Cybersecurity aligns with 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 rigorous academic program enriches the Commonwealth of Virginia, the nation, and the world by (1) expanding the pipeline for a cybersecurity workforce; (2) strengthening ODU's commitment to contributing to the economy and workforce of the Hampton Roads region and the Commonwealth of Virginia; and (3) enhancing the brand awareness of ODU's cybersecurity program worldwide.

Online Delivery

The proposed master's degree program will be fully online, with students accessing course materials through 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, which has been shown to be an important factor in stimulating students' interest and sharpening their scientific reasoning and problem solving skills. To this end, ODU has made significant investments in the creation of a state-of-the-art cybersecurity infrastructure, including a cybersecurity lab consisting of 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.

Admission 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
- 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

Two sets of students will be targeted for the proposed program. The first will be Old Dominion University students who are currently 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 with an interest in cybersecurity. They may be drawn to 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.

The second target group includes current cybersecurity professionals who seek promotions to senior technical positions in industry, military, and federal, state, or local government. This may include individuals with five to twenty years' of experience in the field.

Curriculum

The Master of Science in Cybersecurity is a 30-credit hour program that is designed to address the advanced educational needs of students and employers in the area of cybersecurity. This program consists of four core courses (12 credit hours), five electives (15 credit hours), and one capstone course (3 credit hours).

It will establish a solid educational foundation and prepare students with the theory, technologies, skills, and practices necessary to safeguard critical cyber infrastructure and protect confidential information against unauthorized access, unauthorized use, loss, or damage. The curriculum will include all core components of cybersecurity including cryptography, critical infrastructures, cyber threats and vulnerabilities, risk assessment and management, cyber defense and operation techniques, forensic investigation, and cyber laws and ethics. The required 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. Students will have opportunities to choose five restricted electives 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. Students will learn how to identify problems, gather information, analyze data, define hypotheses, develop solutions, establish contingencies, and effectively articulate and communicate results. They will also have many opportunities to interact with potential employers through recruitment and networking events.

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 the faculty member and the 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. 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 the following, with new courses denoted with the asterisk.

Foundational Core Courses (12 hours)

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. A maximum of three courses can be selected at the 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 A provides sample schedules for full-time and part-time students. Course descriptions may be found in Appendix B.

Student Retention and Continuation Plan

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

- Requiring an online orientation session for all new students, which introduces the program, curriculum, requirements, expectations, faculty, facility, and other relevant resources that are online or remotely accessible through the myODU portal;
- Providing an up-to-date curriculum and a long-range course schedule to help students plan their enrollment and time to completion;
- Holding online and face-to-face advising sessions and providing personalized advising throughout students' program of study;
- Holding special advising sessions for nontraditional students (e.g., working professionals);
- Teaming with faculty and industrial partners to mentor students in subject matter and career direction to help students stay in track; 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:

- Individualized advising and mentoring to help the student pass the courses;
- Connecting to a successful local cybersecurity professional to motivate the student to understand the importance of cybersecurity, appreciate the work of cybersecurity professionals, and develop a pride to become cybersecurity professionals;
- Involvement in state-of-the-art cybersecurity projects to stimulate student's interest to become motivated and excited to study cybersecurity and learn beyond classroom instruction; and
- Creating a cohort to increase interactions and peer learning.

Faculty

Ten faculty members affiliated with the Center for Cyber Security Education and Research (CCSER) hold credentials to teach in the Master of Science in Cybersecurity. They hold tenure or tenure-track positions in four colleges: College of Arts and Letters (Sociology and Criminal Justice; Philosophy and Religious Studies), Strome College of Business (Information Technology and Decision Science), Batten College of Engineering and Technology (Electrical and Computer Engineering; Engineering Management and Systems Engineering; Modeling, Simulation and Visualization Engineering), and College of Sciences (Computer Science). Among the ten faculty members, four will teach the core coursework, including 2 professors, one of whom serves as the director of CCSER, 1 associate professor, and 1 assistant professor.

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.

Brief CVs for existing full time faculty members can be found in Appendix C. Appendix D provides data on grant funding faculty have successfully obtained in this field.

Program Administration

This proposed program will be administered by the Center for Cyber Security Education and Research (CCSER) and the Graduate School. CCSER was established to weave together distinct threads of programmatic and facility resources to create a strong education and research program focusing on cybersecurity. It represents an interdisciplinary effort related to faculty, degree programs, certificates, and research initiatives from four colleges, eight academic departments, the Office of Research, Information Technology Services, and the Virginia Modeling, Analysis and Simulation Center. It consists of about 30 affiliated faculty and staff from across ODU.

A tenured CCSER faculty will be appointed as the graduate program director (GPD). She or he will assume responsibility for setting class schedules, coordinating student meetings and activities, gathering student input, handling students' concerns, providing admission and enrollment information to the Graduate School, and meeting with the faculty, the CCSER director, and dean or associate dean of Graduate School to discuss program matters. 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; approximately 20% of this individual's time will be devoted to the proposed 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 to analyze and diagnose cyber system risks and vulnerabilities	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 articulate 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 abilities 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

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

Relationship to Existing ODU Degree Programs

Old Dominion University has no similar or related programs at the master's level in the area of this proposed program.

Compromising Existing Programs

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

Collaboration or Standalone

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

Justification for the Proposed Program

Response to Current Needs (Specific Demand)

Cybersecurity is a 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 attacks rank 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

[6] "James Clapper, intel chief: Cyber ranks highest on worldwide threats to U.S.", http://www.washingtontimes.com/news/2015/feb/26/james-clapper-intel-chief-cyber-ranks-highest-worl/

techniques. Many malicious attacks are designed to steal information and disrupt, deny access to, degrade, or destroy critical information systems."[7] The proposed program will prepare students to help IT professionals in the federal enterprise to understand cyber risks and vulnerabilities and design stronger and more robust defense systems against cyber attacks.

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] The proposed program provides advanced courses in cybersecurity. Students will be educated to develop skills and competencies with proficiency in a diversity of current and emerging cyber security technologies, and will be prepared to assume responsibility for the management of cybersecurity projects and coordination of cyber operation teams for a wide range of business sectors.

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] The proposed program will prepare students with oral and written communication skills to help people understand such cyber attacks and learn how to mitigate their impacts.

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

[7] "Securing Federal Networks", https://www.dhs.gov/topic/securing-federal-networks
[8] "Cyber Crime Costs Projected To Reach $2 Trillion by 2019", https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#5f8e8fcb3a91
[9] "Cybercrime Report", http://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
[10] "2016 U.S. Government Cybersecurity Report", Page 2, 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.

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, "The data clearly demonstrate much work is yet to be done to secure businesses, government agencies and organizations of all sizes, and the critical importance of having a properly staffed, agile and reactive workforce. However, in the 2015 edition of the GISWS, 62% of information security workers reported having too few workers to address the threats they encountered. In 2017, that number has ticked higher, with 66% indicating that they do not have the staff necessary to address the threats, indicating that the shortage of information security workers is widening, as more sectors recognize the importance of deploying a skilled cyber workforce to protect their data."[14]

Based on a 2015 global survey of 649 cybersecurity and IT managers or practitioners, only 16% feel at least half of their applicants were qualified; 53% say it can take as long as six months to find a 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] The proposed program is aimed at filling the gap. Students will be educated to develop skills and competencies in technical aspects of cyber security, and will be prepared to take leadership roles to the manage cybersecurity projects and coordination of cyber operation teams.

Employment Demand

National/International Focus

The cybersecurity unemployment rate was 0% in 2016, and it is expected to remain there from 2017 to 2021.[17] 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.[18] 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."[19]

---

[13] "State of Cybersecurity: Implications for 2015", An ISACA and RSA Conference Survey, 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

[14] "2017 Global Information Security Workforce Study", Page 3, https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf

[15] "State of Cybersecurity: Implications for 2015", 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] "Cybersecurity skills shortage holding steady", http://www.csoonline.com/article/3177374/security/cybersecurity-skills-shortage-holding-steady.html

[17] "Zero-percent cybersecurity unemployment, 1 million jobs unfilled**",** https://www.csoonline.com/article/3120998/techology-business/zero-percent-cybersecurity-unemployment-1-million-jobs-unfilled.html

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

[19] "Cybersecurity job market to suffer severe workforce shortage", http://www.csoonline.com/article/3201974/it-careers/cybersecurity-job-market-statistics.html

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

- "In 2017, the U.S. employs nearly 780,000 people in cybersecurity positions, with approximately 350,000 current cybersecurity openings, 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." [20]
- 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.[21]
- According to the Bureau of Labor Statistics, the rate of growth for jobs in information security is projected at 28% from 2016–2026, "much faster than the average."[22]
- 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.[23]
- The ISACA, a non-profit information security advocacy group, predicts there will be a global shortage of two million cyber security professionals by 2019.[24]
- Cybersecurity Ventures predicts there will be 3.5 million unfilled cybersecurity positions globally by 2021.[20]

Virginia Focus

Cybersecurity is among Governor McAuliffe's top priorities for building the New Virginia Economy. There are approximately 33,000 cybersecurity job openings in Virginia – the 2nd highest among all states and the highest in terms of demand concentration.[25]

"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

[20] "Cybersecurity labor crunch to hit 3.5 million unfilled jobs by 2021", https://www.csoonline.com/article/3200024/security/cybersecurity-labor-crunch-to-hit-35-million-unfilled-jobs-by-2021.html

[21] "Job Market Intelligence: Cybersecurity Jobs, 2015", Page 3, http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf

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

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

[24] "The Fast-Growing Job With A Huge Skills Gap: Cyber Security", https://www.forbes.com/sites/jeffkauflin/2017/03/16/the-fast-growing-job-with-a-huge-skills-gap-cyber-security/#65b9059a5163

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

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."[26]

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. [27]

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]

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, such as cyber security project managers, principal cyber security engineer, senior security analyst, chief information security officer, cybersecurity data scientist, computer network defense lead, senior cybersecurity systems architect, just to name a few, require advanced education and experience (see the job announcements in Appendix G). The proposed online interdisciplinary graduate program gives students additional technical, theoretical, leadership, managerial and business skills required in senior 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.[29] Given a total of 350,000 cybersecurity openings in the US and 33,000 in Virginia, it is estimated that over 80,000 in the US and 7500 positions in Virginia require at least a master's degree. There are senior cybersecurity 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

[26] "36,000 unfilled Va. jobs have $88,000 starting pay, governor says", http://wtvr.com/2017/07/24/virginia-computer-jobs/

[27] "Virginia's Cybersecurity Industry", Page 1, 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=

[29] "Job Market Intelligence: Cybersecurity Jobs", Page 6, http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf

that 100% of large companies globally will have a CISO position by 2021.[30] The skills and experiences gained through the advanced degree in cybersecurity open up vast opportunities for long-term career advancement.

- Most cybersecurity bachelor's program 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.

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.

Letters of support from several of these employers may be found in Appendix E. A survey will be conducted among employers with results of the survey are found in Appendix F.

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

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%

[30] "Cybersecurity Jobs Report", http://cybersecurityventures.com/jobs/

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.

The 30 credit-hour program aims to prepare graduates to fill the current and future need for information security and assurance professionals.

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 does not focus on network security, but 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 36 credit-hour Master of Science in Executive Management of Secure Information Systems and a 48 credit-hour 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. The 30 credit-hour program focus on computer security.

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 The 30 credit-hour program provides for the scholarly and professional needs of several groups who have either accepted or are keen to take on the challenge of protecting information resources of firms and society at large.

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:[31,32]

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	
-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	12	12	14	21	16

[31] http://research.schev.edu/enrollment/E16_report.asp
[32] http://research.schev.edu/Completions/C1Level2_Report.asp

Sys Security Enrollments					
-MS Computer and IT Sys Security Graduates	6	3	5	5	

Projected Resource Needs for the Proposed Program

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 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

December 7, 2017

APPROVAL TO RENAME THE CENTER FOR ECONOMIC ANALYSIS AND POLICY TO DRAGAS CENTER FOR ECONOMIC ANALYSIS AND POLICY STROME COLLEGE OF BUSINESS

RESOLVED that, upon the recommendation of the Academic and Research Advancement Committee, the Board of Visitors approves renaming the Center for Economic Analysis and Policy to Dragas Center for Economic Analysis and Policy in the Strome College of Business effective January 1, 2018.

Rationale: Over the years, the Center for Economic Analysis and Policy in the Strome College of Business has played a significant role in economic forecasting and analysis of issues that impact the economy in Hampton Roads and in the Commonwealth of Virginia. Such work includes studies related to transportation, the military, economic activities, and other reporting for entities in Virginia. The Center will continue this work in the foreseeable future for Hampton Roads and for the Commonwealth.

In consideration of the creation of an endowment from the George and Grace Dragas Family Foundation in support of the Center, it is recommended that the Center be renamed the Dragas Center for Economic Analysis and Policy in the Strome College of Business.

December 7, 2017

REQUEST FOR LEAVE OF ABSENCE WITHOUT COMPENSATION

The President has approved the following request for leave of absence without compensation.

Name and Rank	Leave of Absence From To	Contract Salary
Dr. Jelmer Vos Associate Professor Department of History	Spring 2018 semester	$29,901.50 (spring semester)

Reason for Leave: Serve as lecturer at the University of Glasgow in Scotland.