FACULTY SENATE ISSUE FORM
Date Submitted: August 23, 2018
Title of Issue (a short descriptive title by which the issue may be referenced)
Proposal for a Bachelor of Science in Cybersecurity
Description of Issue: Old Dominion University seeks approval to initiate a Bachelor of Science in Cybersecurity to begin fall 2019. This program will be administered by the Center for Cyber Security Education and Research (CCSER) and housed in the Department of Interdisciplinary Studies, College of Arts & Letters.
Rational for Submission: The proposed BS in Cybersecurity is designed to provide students with a strong understanding of cyber systems, threats, defense, and operation technologies. Graduates will be knowledgeable in the theory, technologies, skills, and practices necessary to protect critical cyber infrastructure and assets. They will have enhanced oral and written communication skills to articulate cybersecurity problems and decisions, and clearly understand ethical standards and rules. The proposed program responds to the vital needs for cybersecurity professionals in the Commonwealth of Virginia, the nation, and the world. Graduates will be prepared to work within the cybersecurity industry, U.S. Army, Navy, Air Force, and other branches of the military, and within federal, state, or local government or government contracting. Graduates will fill the demand for cybersecurity technical positions such as Cyber Intelligence Analyst, Cyber Security Analyst, Data Security Associate, Incident Response Analyst, Information Assurance Analyst, Information Security Analyst, Information Systems Security Officer, Security Consultant, Security Engineer, Security Specialist, Vulnerability Analyst, just to name a few. The proposed degree program represents an expansion of the current cybersecurity major within the Bachelor of Science in Interdisciplinary Studies, which has been offered for the past three years. This expansion is needed to eliminate curricular restraints of a major and to allow students to earn a degree that more closely matches the coursework they take and job opportunities they pursue after graduation. Further, a stand-alone degree program in cybersecurity will provide students with the degree—and degree name—that more accurately reflects the coursework taken. The focus on cybersecurity will advance students' understanding of a broad range of cybersecurity topics in Virginia, in the United

States, and internationally. Ultimately, the degree title will be more recognized for professionals employed in the field of cybersecurity, as opposed to a degree in interdisciplinary studies.
Name: Judy Bowman, submitted on behalf of Austin Agho
Department: Academic Affairs
Date: August 23, 2018
Signature:
For Faculty Senate Use Only
Assigned to Committee:
Date Assigned:

STATE COUNCIL OF HIGHER EDUCATION FOR VIRGINIA
PROGRAM PROPOSAL COVER SHEET

1. Institution Old Dominion University	2. Academic Program (Check one): New program proposal ☒ Spin-off proposal ☐ Certificate document ☐
3. Name/title of proposed program Cybersecurity	4. CIP code 11.1003
5. Degree/certificate designation Bachelor of Science	6. Term and year of initiation Fall 2019
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 Department of Interdisciplinary Studies School(s) or college(s) of College of Arts & Letters Campus(es) or off-campus site(s) Main Campus in Norfolk	
Mode(s) of delivery: face-to-face ☐ hybrid (both face-to-face and distance) ☐	Distance (51% or more web-based) ☒
13. Name, title, and telephone number(s) 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 the modified program. Jeanie Kline, Ed.D. SCHEV Liaison, 757.683.3261.	

TABLE OF CONTENTS

Description of the Proposed Program

Program Background

Old Dominion University (ODU) seeks approval to initiate a Bachelor of Science in Cybersecurity, scheduled to begin fall 2019 in Norfolk, Virginia. This proposed program will be administered by the Center for Cyber Security Education and Research (CCSER) and housed in the Department of Interdisciplinary Studies, College of Arts & Letters.

The proposed BS in Cybersecurity is designed to provide students with a strong understanding of cyber systems, threats, defense and operation technologies. Graduates will be knowledgeable in the theory, technologies, skills, and practices necessary to protect critical cyber infrastructure and assets. They will have enhanced oral and written communication skills to articulate cybersecurity problems and decisions, and clearly understand ethical standards and rules.

The program will prepare graduates to work within the cybersecurity industry, U.S. Army, Navy, Air Force, and other branches of the military, and within federal, state, or local government or government contracting. Graduates will fill the demand for cybersecurity technical positions such as Cyber Intelligence Analyst, Cyber Security Analyst, Data Security Associate, Incident Response Analyst, Information Assurance Analyst, Information Security Analyst, Information Systems Security Officer, Security Consultant, Security Engineer, Security Specialist, Vulnerability Analyst, just to name a few.

The proposed BS in Cybersecurity responds to the vital needs for cybersecurity professionals in the Commonwealth of Virginia, the nation, and the world. In recent years, cyberattacks have become more common, sophisticated, and harmful. In fact, no organization or individual with an online presence is immune to attacks, and the impact of cyberattacks can be devastating. Year 2017 is "a record year for stolen data", according to digital security provider Gemalto,[1] which reports 1,765 data breaches in 2017 with a total of 2,600,968,280 compromised data records. The Gemalto report indicates that "One of the most significant developments of the year was an abundance of poor security practices. Malicious actors were able to hack Equifax in the summer of 2017, for example, because the credit bureau failed to improve its security practices after thieves made off with its data in May 2017 and earlier that year." The Equifax data breach alone could affect 143 million people in the U.S., including 4 million in Virginia.[2] The Gemalto report also shows that "Incidents involving accidental loss increased significantly from under 250 million in 2016 to nearly 2 billion the following year" and "ransomware detections in 2017 were up 90 percent and 93 percent for businesses and consumers, respectively."[1]

As the volume and sophistication of cyberattacks grow, there is a strong demand for a well-trained cybersecurity workforce to address the multifaceted cybersecurity problems.[3] This will

[1] "Findings from the first half of 2017 Breach Level Index", Page 3, Gemalto, https://breachlevelindex.com/assets/Breach-Level-Index-Report-2017-Gemalto.pdf
[2] Daily Press, http://www.dailypress.com/news/dp-nws-virginia-equifax-breach-20170914-story.html
[3] "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

require a solid 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.

Executive Order Thirty-Nine from the Governor of Virginia 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."[4] The proposed degree program will contribute to addressing such cybersecurity problems by preparing students to understand cybersecurity threats and develop more robust cyber defense systems. Graduates will become the next generation in the cybersecurity workforce to safeguard information relating to national security and various sensitive business and personnel data.

Mission

The mission of the institution states: "Old Dominion University, located in the City of Norfolk in the metropolitan Hampton Roads region of coastal Virginia, is a dynamic public research institution that serves its students and enriches the Commonwealth of Virginia, the nation and the world through rigorous academic programs, strategic partnerships, and active civic engagement."

The proposed Bachelor of Science in Cybersecurity degree program aligns with this mission by (1) offering a "rigorous academic program" that trains individuals in the field of cybersecurity, (2) strengthening ODU's "civic engagement" in its commitment to contributing to the economy and workforce of the Hampton Roads region and the Commonwealth of Virginia, and (3) enhancing the "strategic partnerships" in cybersecurity that ODU has developed throughout the region.

Online Delivery

The upper-level coursework in the proposed BS in Cybersecurity degree program will be offered primarily in online settings, with several upper-level classes available on campus as well. Lower-level general education and cybersecurity classes may be completed in online and on-campus settings. Within both formats, students will be able to access course materials through Blackboard, the University's course management system. All assignment submissions and other course management actions will 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

[4] "Commonwealth of Virginia Office of the Governor Executive Order Number Thirty Nine", Page 2, https://vdocuments.mx/commonwealth-of-virginia-office-of-the-governor-executive-of-virginia-office.html.

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

The requirements for admission to the proposed Bachelor of Science in Cybersecurity will include:

- An online admission application and associated application fee
- For freshmen: official transcripts from secondary institution(s) and/or General Education Development (GED) work
- For transfer students: official transcripts from all regionally-accredited post-secondary institutions or equivalent foreign institutions attended, with a minimum GPA of 2.5 in prior coursework; a GPA of 3.0 or better will make the applicant more competitive

Non-native English speakers are required to have a provide official scores of 550 on the paper-based, or 79-80 on the iBT, Test of English as a Foreign Language (TOEFL).

Other factors such as co/extra-curricular activities, community service, personal statements, recommendations, and special talents and leadership may also be considered.

Target Population

The proposed bachelor's program will target students who are enrolled in cybersecurity associate degrees where ODU has developed articulation agreements. These include the following colleges:

- Tidewater Communication College
- Thomas Nelson Community College
- Northern Virginia Community College

The articulations facilitate the seamless transfer of community college graduates to ODU. The students who graduate under the articulations are guaranteed admission to ODU's cybersecurity program, which is the most affordable doctoral research institution in the state.

Curriculum

The proposed Bachelor of Science in Cybersecurity is a 120-credit hour degree program focused on the subject of cybersecurity and provides opportunities for students to integrate education and training with the application of problem-solving skills in the lab environment.

The curriculum of the proposed BS in Cybersecurity includes a cybersecurity core that introduces fundamental concepts associated with the field of cybersecurity. The faculty also developed an interdisciplinary core that allows for students to gain an understanding of theory and practice related to combining disciplines in academic and professional areas. In addition, faculty included a law/ethics component that provides essential details about ethical and/or legal aspects of cybersecurity. The cybersecurity foundations area consists of key concepts related to threats and vulnerabilities, infrastructures, cryptography, and other facets of cybersecurity that students will need in the field. Finally, the curriculum includes opportunities for students to apply their knowledge of cybersecurity in hands-on applications with digital forensics, networks, enterprises, and others.

Ultimately, the proposed program will establish a solid educational foundation and prepare students for jobs in cybersecurity 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.

Program Requirements

Lower-Division General Education (35-44 credit hours):

- Written Communication 6
- Oral Communication 3
- Mathematics (MATH 162M required) 3
- Language and Culture 0-6
  (may be met prior to matriculation)
- Information Literacy and Research 3
- Human Creativity 3
- Interpreting the Past 3
- Literature 3
- Philosophy and Ethics (can be met by PHIL 355E) 0-3
- The Nature of Science 8
- Impact of Technology (CYSE 200T required) 0
- Human Behavior 3

Cybersecurity Core Courses (12 credit hours):

- CYSE 200T Cybersecurity, Technology, and Society 3
- CYSE 250 Basic Cybersecurity Programming and Networking 3
- CYSE 300 Introduction to Cybersecurity 3
- CYSE 301 Cybersecurity Techniques and Operations 3

Interdisciplinary Studies Core (9 credit hours):

- IDS 300W Interdisciplinary Theory and Concepts 3
- CYSE 368 Cybersecurity Internship or
  CYSE 494 Entrepreneurship in Cybersecurity 3
- IDS 493 IDS Electronic Portfolio Project 3

Law and Ethics (3 credit hours)

Select one of the following: 3

- CRJS 405 Cybercrime and Cybersecurity
- CRJS/CYSE/CPS 406 Cyber Law
- PHIL 355E Cybersecurity Ethics

Cybersecurity Foundations (9 credit hours)

Select three from the following:

- CS 462 Cybersecurity Fundamentals (3)
  or ECE/MSIM 470 Foundations of Cyber Security (3)
- CS 463 Cryptography for Cybersecurity (3)
- CS 464 Networked Systems Security (3)
  or ECE/MSIM 411 Networked System Security (3)
- CS 465 Information Assurance (3)
- CYSE/POLS 495 Topics in Cybersecurity (Cybersecurity and Policy, 3)
- ECE/MSIM 416 Cyber Defense Fundamentals (3)
- ECE/MSIM 419 Cyber Physical System Security (3)
- IT 315 Introduction to Networking and Security (3)
- IT 417 Management of Information Security (3)

Cybersecurity Applications (9 credit hours)

Select three from the following:

- CS 471 Operating Systems (3)
- CS 495 Topics in Computer Science (Software Reverse Engineering, 3)
- CYSE 407/CRJS 395 Digital Forensics (3)
- CYSE/POLS 495 Topics in Cybersecurity (Cyberwar, 3)
- ECE/MSIM 417 Secure and Trusted Operating Systems (3)
- ECE 452 Introduction to Wireless Communication Networks (3)
- ECE 455 Network Engineering and Design (3)
- IT 410 Business Intelligence (3)
- IT 416 Network Server Configuration and Administration (3)
- IT 418 Information Assurance (3)
- IT 419 Enterprise Cyber Defense (3)
- IT 461 Implementing Internet Applications (3)

Prerequisites and/or Electives: 34-43 credit hours, as needed to complete the required 120 credit hours

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

Student Retention and Continuation Plan

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

- Requiring an online orientation session for all new students, aimed at introducing the program, curriculum, requirements, expectations, faculty, facility, and other relevant resources that are online or remotely accessible through the myODU portal;
- Providing an up-to-date curriculum and a long-range course schedule to help students plan their enrollment and time to completion;
- Requiring a minimum of one advising session per semester (online or face-to-face) and providing personalized advising throughout students' program of study;
- Holding special advising sessions for transfer students; and
- Encouraging students to join ODU's Cybersecurity Student Association, which hosts regular meetings for students to share success stories, talk about strategies to complete the program and discuss future career pathways. This is a means of building a community of cybersecurity learners who can support each other throughout the program.

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

- Individualized advising and mentoring to help the student pass course(s);
- Connecting 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.

Time to Degree

Full-time students will be able to complete the proposed BS in Cybersecurity in four calendar years. Part-time students can complete the program in six to eight calendar years, depending on their course load each semester. Courses are also offered in summer terms for students to complete in an accelerated pace, if desired.

Faculty

Seven faculty members affiliated with the Center for Cyber Security Education and Research (CCSER) will teach in the proposed Bachelor of Science in Cybersecurity degree program. Three faculty members are tenured: two professors and one associate professor. Four faculty members are lecturers. The seven faculty represent several colleges at the university: College of Arts and

Letters), Strome College of Business, Batten College of Engineering and Technology), and College of Sciences. They will teach core, foundation, law/ethics, and application coursework.

The faculty have breadth and depth in areas of cybersecurity, ranging from software to hardware security and from fundamental cybersecurity technologies to human factors in cybersecurity. Combined, they have over 100 years of postsecondary teaching experience, an extensive record of scholarship with over 90 recent publications in peer-reviewed journals and conferences in cybersecurity fields. They currently have approximately 10 active research grants from prestigious organizations such as the National Science Foundation.

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

Program Administration

This proposed Bachelor of Science in Cybersecurity degree program will be housed in the Department of Interdisciplinary Studies, College of Arts & Letters, and administered by the Center for Cyber Security Education and Research (CCSER). 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 approximately 30 affiliated faculty and staff from across Old Dominion University.

A CCSER faculty will be appointed as the program coordinator. She or he will assume responsibility for setting class schedules, advising students, coordinating student meetings and activities, gathering student input, handling students' concerns, collecting admission and enrollment information, and meeting with the faculty, the CCSER director, and dean or associate dean of the College of Arts and Letters to discuss programmatic matters.

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. The assistant will help with the processing of applications, scheduling of courses, handling registration issues, updating the catalog, and website management.

Student Assessment

Students will be evaluated throughout the program using formative assessments, such as quizzes, tests, cases studies, papers, research projects, and presentations. Student learning outcomes cover many of the technical 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.

Curriculum Map of Cybersecurity Program Core Courses

Learning Outcomes	Courses	Assessment Methods
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 200T Cybersecurity, Technology, and Society	Formative: Group reading and book review; critical thinking and analysis assignments. Summative: Midterm and final exams assessing knowledge of the ethical standards and rules for cybersecurity professionals.
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 200T Cybersecurity, Technology, and Society IDS 300W Interdisciplinary Theory and Concepts IDS 493 IDS Electronic Portfolio Project	Formative: Group reading and discussion; written assignments; short essays; and digital portfolio. Summative: Midterm and final exams assessing critical thinking and written communication skills.

3. Analytical Problem Solving Integrate principles and methods to analyze and diagnose cyber system risks and vulnerabilities	CYSE 250 Basic Cybersecurity Programming and Networking CYSE 300 Introduction to Cybersecurity CYSE 301 Cybersecurity Techniques and Operations	<u>Formative:</u> Real-world application scenarios; case analysis; critical thinking and analysis assignments. <u>Summative:</u> Midterm and final exams assessing knowledge of the cyber system risks and vulnerabilities and diagnosis principles and methods.
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 200T Cybersecurity, Technology, and Society CYSE 250 Basic Cybersecurity Programming and Networking	<u>Formative:</u> Real-world application scenarios; case study of the global impact of a cyberattack; critical thinking and analysis assignments. <u>Summative:</u> Midterm and final exams assessing knowledge of the international cybersecurity threats in the Internet.
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 250 Basic Cybersecurity Programming and Networking	<u>Formative:</u> Design assignments; oral presentation of a cyber defense plan for a campus network. <u>Summative:</u> Midterm and final exams assessing knowledge of technical communication principles and practice.

Employment Skills/Workplace Competencies

Graduates of the proposed BS in Cybersecurity degree program will have the skills and abilities needed for employment and workplace competencies in the field of cybersecurity. Specifically, they will have the ability to:

1. apply leading-edge principles, theories, and concepts to the development of information security standards, procedures, and guidelines;
2. plan, design, implement and operate security-related technologies;
3. perform vulnerability analyses and assessment and develop plans for vulnerability mitigation;
4. troubleshoot and/or provide technical support in the cybersecurity event;
5. participate in network and systems design to ensure implementation of appropriate systems security policies;
6. identify and specify information systems security requirements associated with migrations to new environments;
7. communicate the value of cyber security throughout all levels of the organization's stakeholders.

Program Assessment

The program will be assessed by faculty and administrators in the Center for Cyber Security Education and Research, the Department of Interdisciplinary Studies, the College of Arts & Letters, and the provost's office. The review will be completed annually in the fall starting from the second year after the program is approved, and will consist of:

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

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

- Student recruitment, admissions, advising, and retention;
- Enrollment projections including consideration of the context of the SCHEV 5-year benchmark and other on-going enrollment targets;
- Course descriptions and implementation;

- Approved curricular changes and development;
- Faculty development and research activities;
- Facilities;
- Internal and external funding; and
- Description of strengths and weaknesses with attention to action items for the future.

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

Benchmarks of Success

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

- Approximately 75 new students will be admitted each year
- The program will graduate a minimum of 45 students annually by the completion of the program's target year
- 60% 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 undergraduate studies within six months of completion
- 80% of students will be satisfied with the program as determined by the university's Student Satisfaction Survey
- 80% of alumni will be satisfied with the program as determined by the university's 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 program coordinator 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 degree program represents an expansion of the current cybersecurity major within the Bachelor of Science in Interdisciplinary Studies, which has been offered for the past 3 years. This expansion is needed to eliminate curricular restraints of a major and to allow students to earn a degree that more closely matches the coursework they take and job opportunities they pursue after graduation.

The curriculum required for the cybersecurity degree program is not the curriculum required for the cybersecurity major in interdisciplinary studies. The focus on the need for trained cybersecurity professionals has heightened since the major started, and it has become its own disciplinary area. The faculty has determined that cybersecurity needs a separate curriculum in order to provide the didactic and application coursework needed to fully educate students in the area of cybersecurity.

Further, a stand-alone degree program in cybersecurity will provide students with the degree—and degree name—that more accurately reflects the coursework taken. The focus on cybersecurity will advance students' understanding of a broad range of cybersecurity topics in Virginia, in the United States, and internationally. Ultimately, the degree title will be more recognized for professionals employed in the field of cybersecurity, as opposed to a degree in interdisciplinary studies.

If the proposed BS in Cybersecurity is approved, the cybersecurity major in the BS in Interdisciplinary Studies will be discontinued.

Relationship to Existing ODU Degree Programs

The proposed BS in Cybersecurity is not similar or related to any other existing degree program at ODU.

Compromising Existing Programs

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

Collaboration or Standalone

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

Justification for the Proposed Program

Response to Current Needs (Specific Demand)

Cybersecurity is a rapidly-growing field that is expected to generate a significant number of new jobs over the next decade, as both government and industry make substantial investments to protect their cyber space.

With the increasing reliance on computer systems and networks, more pervasive, sophisticated, and destructive cyberattacks are occurring with greater frequency. In fact, no organization or individual anywhere in the world is completely immune to cyberattacks.

Impact of Cyber Attacks on National Security, Private Sectors, and Society

Former national intelligence director, James Clapper, noted that cyberattacks rank highest on worldwide threats to U.S. national security.[5] 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."[6] The proposed program will prepare students to help IT professionals in the federal and state government enterprise to understand cyber risks and vulnerabilities and design stronger and more robust defense systems against cyberattacks.

IBM Corporation's Chairman, CEO and President, Ginni Rometty, said that cybercrime may be the greatest threat to every company in the world.[7] According to an analysis conducted by Cybersecurity Ventures, the global annual cybercrime costs have been estimated at $3 trillion in 2015, and it could reach $6 trillion by 2021.[8] 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] In response to these efforts, the proposed program provides advanced education in leadership in the field of cybersecurity, thus enhancing their skills and competencies that address cybersecurity-related matters.

Cyberattacks not only impact national security and the economy, but they 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. In 2017, malware WannaCry affected more than 230,000 users in some 150 countries.[10] The proposed program will prepare students with oral and written communication skills to help people understand such cyberattacks and learn how to mitigate their impacts.

[5] "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/
[6] "Securing Federal Networks", https://www.dhs.gov/topic/securing-federal-networks
[7] "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
[8] "Cybercrime Report", http://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
[9] "2016 U.S. Government Cybersecurity Report", Page 2, https://cdn2.hubspot.net/hubfs/533449/SecurityScorecard_2016_Govt_Cybersecurity_Report.pdf
[10] "How the WannaCry Attack Will Impact Cyber Security", May 2017, http://knowledge.wharton.upenn.edu/article/massive-global-cyberattack/

Shortage of Cybersecurity Talent

As the volume and sophistication of cyberattacks grow, there is a strong 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 that "the cybersecurity workforce is one of the most critical employment sectors in the world."[11]

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."[12] According to International Information System Security Certification Consortium's, or (ISC)²'s, Global Information Security Workforce Study (GISWS), 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."[13]

Based on a global survey of 461cybersecurity managers and practitioners,[14] 75 percent of respondents expect to fall prey to a cyberattack in 2016. "82 percent of respondents report that their enterprise board of directors is 'concerned' or 'very concerned' about cybersecurity." "Although enterprises continue to increase spending and effort on cybersecurity, respondents indicate that they struggle to fill positions with highly skilled workers—60 percent of all respondents do not believe their information security staff can handle anything more than simple cybersecurity incidents."[14] According to Enterprise Strategy Group (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

[11] 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.

[12] "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

[13] "2017 Global Information Security Workforce Study", Page 3, https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf

[14] "State of Cybersecurity: Implications for 2016", https://www.isaca.org/cyber/Documents/state-of-cybersecurity_res_eng_0316.pdf

skills."[15] The proposed program is aimed at filling the gap. Students will be educated to develop skills and competencies in technical aspects of cyber security.

Demand for Bachelor's Degree Program in Cybersecurity

In the article by Dan Restuccia about "How to Get a Cybersecurity Job in Three Charts", the first step is to get a bachelor's degree. The article cites that "more than eight in 10 (83%) of job postings for cybersecurity workers ask for a bachelor's degree or higher. That means 'quick fix' training programs won't necessarily close the talent gap, or allow a jobseeker to compete."[16]

The expectations are that the demand for a bachelor's degree is likely to increase further, considering that computer systems and software are becoming more and more pervasive. A look at one way the government has tried to build and recruit such talent—offering university scholarships—shows why.[17] For example, NSF's CyberCorps Scholarship for Service (SFS) program "provides funding to award scholarships to students in cybersecurity."[18] It "provides academic-year stipends of $22,500 per year for undergraduate students."[18] After school, recipients serve in government for the same length of time as they received funding, typically two to three years.

The demand for bachelor level education is also evidenced by the National Security Agency (NSA) Centers of Academic Excellence (CAE) designations. For example, the "CAE Cyber Operations program is intended to be a deeply technical, inter-disciplinary, higher education program firmly grounded in the computer science (CS), computer engineering (CE), and/or electrical engineering (EE) disciplines, with extensive opportunities for hands-on applications via labs/exercises." [19] (The proposed program offers such an interdisciplinary focus.) Fourteen out of the 20 NSA CAE centers are BS programs.[19] Thus, a bachelor's degree in cybersecurity is a credential that is—and will continue to be—desired by professionals in the field.

Employment Demand

National/International Focus

According to a recent study of cybersecurity professionals, "more than one-third (34%) have less than 3 years' experience while 30% have been cybersecurity professionals for at least 15 years."[20] The cybersecurity unemployment rate was 0% in 2016, and it is expected to remain

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

[16] "How to Get a Cybersecurity Job in Three Charts: a Degree, a Certification, and a Clearance", Dan Restuccia, Labor Market Analysis, Research, May 13, 2016, https://www.burning-glass.com/blog/how-to-get-a-cybersecurity-job-in-three-charts-a-degree-a-certification-and-a-clearance/

[17] "The U.S. Government Wants 6,000 New 'Cyberwarriors' by 2016", by Dune Lawrence, available online at https://www.bloomberg.com/news/articles/2014-04-15/the-u-dot-s-dot-government-wants-6-000-new-cyberwarriors-by-2016

[18] NSF Program Solicitation 17-556. https://www.nsf.gov/pubs/2017/nsf17556/nsf17556.htm

[19] National Centers of Academic Excellence in Cyber Operations, https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-operations/centers.shtml

[20] "The Life and Times of Cybersecurity Professionals", Page 9, Nov., 2017. https://c.ymcdn.com/sites/www.issa.org/resource/resmgr/surveyes/ESG-ISSA-Research-Report-Lif.pdf

there from 2017 to 2021.[21] 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.[22] Further, "the field of cybersecurity 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."[23]

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."[24]

In addition, the high demand for cybersecurity talent has been reported by multiple sources:

- In 2017, the U.S. employed 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."[25]
- 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.[26]
- Cybersecurity Ventures predicts there will be 3.5 million unfilled cybersecurity positions globally by 2021.[25]
- Michael Brown, CEO at Symantec, the world's largest security software vendor, estimates that the demand for cybersecurity professionals will reach 6 million globally by 2019.[27]
- The ISACA, a non-profit information security advocacy group, predicts there will be a global shortage of two million cyber security professionals by 2019.[28]

[21] "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
[22] "Best Technology Jobs," U.S. News, https://money.usnews.com/careers/best-jobs/rankings/best-technology-jobs
[23] "Cybersecurity job market to suffer severe workforce shortage"
http://www.csoonline.com/article/3201974/it-careers/cybersecurity-job-market-statistics.html
[24] https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm
[25] "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
[26] "Job Market Intelligence: Cybersecurity Jobs, 2015," Page 3
http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf
[27] "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
[28] "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

Virginia Focus

There are over 30,000 cybersecurity job openings in Virginia – one of the highest among all states.[29] "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."[30]

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 41.51% from 2016 through 2026 (3.53% Annual Average % Change).[31] The VEC indicated that jobs in this field, such as Information Security Analysts, are abundant. [32] As of July 31, 2018, there were 1,365 openings for Information Security Analysts and 0.21 candidates available per job opening.

A report by Burning Glass Technologies showed that 61% of cyber security postings require at least a bachelor's degree.[33] Given a total of 350,000 cybersecurity openings in the U.S. and 33,000 in Virginia, it is estimated that over 213,500 in the US and 20,130 positions in Virginia require at least a bachelor's degree.

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 it may be possible to find entry-level cyber security positions with an associate's degree, most jobs require a four-year bachelor's degree in cyber security or a related field such as information technology or computer science. Coursework in cyber technologies with classes in ethics and computer forensics prepare students with the technical and analytical skills required for successful careers in cyber security.

Job announcements are included in Appendix D.

Student Demand

Student demand for a bachelor's degree in cybersecurity is strong, as evidenced by two sets of data, as follows.

1. Enrollments in the current Bachelor of Science in Interdisciplinary Studies with a major

[29] http://cyberseek.org/heatmap.html
[30] "36,000 unfilled Va. jobs have $88,000 starting pay, governor says", http://wtvr.com/2017/07/24/virginia-computer-jobs/
[31] https://data.virginialmi.com/vosnet/analyzer/results.aspx?session=occproj
[32] The Official Site of The Commonwealth of Virginia, https://data.virginialmi.com.
[33] "Job Market Intelligence: Cybersecurity Jobs", Page 6, http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf

in cybersecurity has gained tremendous growth in enrollment since it was launched in 2015. Specifically, the Office of Institutional Research at ODU reports those enrollments in cybersecurity as follows:

Fall 2015	11
Fall 2016	69
Fall 2017	121

The first 8 graduates completed their BS in Interdisciplinary Studies with a major in cybersecurity in 2017-18.

2. Results of a survey sent to students enrolled in cybersecurity programs at Tidewater Community College, Thomas Nelson Community College, and Northern Virginia Community College demonstrate strong demand for the program. (To be described)

The student survey and results may be found in Appendix E.

Projected enrollment:

Year 1		Year 2		Year 3		Year 4 **Target Year (2-year institutions)**			Year 5 **Target Year (4-year institutions)**		
2019 - 2020		2020 - 2021		2021 - 2022		2022 - 2023			2023 - 2024		
HDCT 150	FTES 100	HDCT 150	FTES 100	HDCT 175	FTES 125	HDCT 175	FTES 125	GRAD ____	HDCT 175	FTES 125	GRAD 45

Assumptions
Retention: 90%
Part-time students: 60% / Full-time students: 40%
Full-time students credit hours per semester: 15
Part-time students credit hours per semester: 6
Full-time students graduate in 4 years
Part-time students graduate in 6-8 years

Duplication

There is no baccalaureate degree program in cybersecurity offered by a public university in the Commonwealth of Virginia. Therefore, the proposed program would be the first of its kind in the state.

Projected Resource Needs for the Proposed Program

Resource Needs

Old Dominion University and the Center for Cyber Security Education and Research (CCSER) have sufficient resources to launch and sustain the proposed program. Specifically, faculty, staff, equipment, space, and library resources are available to launch and maintain the proposed program. The proposed program will allocate 1.0 FTE of instructional effort for every 24.0 FTE of enrollment. During the 2019-2020 academic year when the program is launched, a total of 4.1 FTE of instructional effort will be required, and it will rise to 5.2 FTE by the target year, 2023-2024.

Full-Time Faculty
One faculty member will contribute 50% (.5 FTE) of his teaching load when the proposed program is launched and into the target year.

Part-Time Faculty
Nine additional faculty members at the university will contribute less than half of their teaching loads in the proposed program. Combined, they will account for 3.6 FTE faculty when the program is launched. By the target year, the combined part-time faculty members will account for 4.7 FTE faculty.

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

Graduate Assistants
No graduate assistants are required to launch and sustain the proposed program.

Classified Positions
A classified person—an administrative assistant—who supports the Center for Cyber Security Education and Research will assist with this proposed program. This person will devote approximately .25 FTE to the program, or $7,500 in salary and $2,783 in fringe benefits.

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

Library
No new library resources are required to launch and sustain the proposed program. The University Libraries have adequate resources to support this program, including journals such as IEEE Security & Privacy, IEEE Transactions on Information Forensics and Security, and IEEE Transactions on Dependable and Secure Computing through the online IEEExplore database.

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

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

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

Other Resources (specify)
No new resources will be required to launch or operate the proposed Bachelor of Science in Cybersecurity degree program.

Resource Needs: Parts A - D

Part A: Answer the following questions about general budget information.

- Has the institution submitted or will it submit an addendum budget request to cover one-time costs? Yes ☐ No ☒
- Has the institution submitted or will it submit an addendum budget request to cover operating costs? Yes ☐ No ☒
- 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 ☒
- Will each type of space for the proposed program be within projected guidelines? Yes ☒ No ☐
- Will a capital outlay request in support of this program be forthcoming? Yes ☐ No ☒

Part B: Fill in the number of FTE and other positions needed for the program				
	Program Initiation Year		Expected by Target Enrollment Year	
	2019- 2020		2023- 2024	
	On-going and reallocated	Added (New)	Added (New)***	Total FTE positions
Full-time faculty FTE*	0.50			0.50
Part-time faculty FTE**	3.60		1.10	4.70
Adjunct faculty				0.00
Graduate assistants (HDCT)	2.00			2.00
Classified positions	0.25			0.25
TOTAL	6.35	0.00	1.10	7.45
*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 2019- 2020		Expected by Target Enrollment Year 2023- 2024	
Full-time faculty	0.50	0.00	0.00	0.50
salaries	$75,000			$75,000
fringe benefits	$28,927			$28,927
Part-time faculty (faculty FTE split with unit(s))	3.60	0.00	1.10	4.70
salaries	$288,000		$88,000	$376,000
fringe benefits	$111,082		$33,942	$145,024
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				$0
Classified Positions	0.25	0.00	0.00	0.25
salaries	$7,500			$7,500
fringe benefits	$2,893			$2,893
Personnel cost				
salaries	$402,500	$0	$88,000	$490,500
fringe benefits	$142,902	$0	$33,942	$176,844
Total personnel cost	$545,402	$0	$121,942	$667,344
Equipment				$0
Library				$0
Telecommunication costs				$0
Other costs				$0
TOTAL	**$545,402**	**$0**	**$121,942**	**$667,344**

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

Please complete Items 1, 2, and 3 below.

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

Funding Source	Program initiation year 2019 - 2020	Target enrollment year 2023 - 2024
Reallocation within the department *(Note below the impact this will have within the department.)*		
Reallocation within the school or college *(Note below the impact this will have within the school or college.)*		
Reallocation within the institution *(Note below the impact this will have within the institution.)*	$545,402	$667,344
Other funding sources *(Specify and note if these are currently available or anticipated.)*		

2. Statement of Impact/Funding Source(s). A separate detailed explanation of funding is required for each source used and a statement of impact on existing resources.

Reallocation within the Institution:
Funding for faculty in departments across Old Dominion University will be reallocated within the institution. The faculty are from the Center for Cyber Security Education and Research, as well as 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; Modeling, Simulation and Visualization Engineering), and College of Sciences (Computer Science). The colleges and departments will maintain existing funding, and classes will be offered across various programs, including the proposed Bachelor of Science in Cybersecurity. No negative impact is anticipated for any degree program in any of the colleges or from any other areas of the university.

The Center for Cyber Security Education and Research (CCSER) will reallocate personnel funds within the center to accommodate the proposed program. This support from the CCSER will be available at the program's launch and through the target year. The faculty and administration anticipate no negative impact from the implementation of this program.

3. Secondary Certification.

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

X Agree _____

Signature of Chief Academic Officer

___ Disagree _____

Signature of Chief Academic Officer

APPENDICES

APPENDIX A
PLAN OF STUDY

Full-Time Student

Year	Fall Semester	Spring Semester
Freshman (28)	Written Communication I: ENGL 110C (3)	Written Communication II: ENGL 231 recommended (3)
	Oral Communication (3)	Nature of Science I (4)
	Info. Literacy and Research (3)	Elective or Prerequisites Course (3)
	Human Behavior: CRJS 215S or SOC 201s (3)	Elective or Prerequisites Course (3)
	MATH 162M (3)	
	Total: 15 credit hours	Total: 13 credit hours
Sophomore (31)	Literature (3)	Interpreting the Past (3)
	Nature of Science II (4)	CYSE 250 (3)
	Impact of Technology: CYSE/IT 200T (3)	Elective or Prerequisites Course (3)
	Elective or Prerequisites Course (3)	Elective or Prerequisites Course (3)
	Elective or Prerequisites Course (3)	Elective or Prerequisites Course (3)
	Total: 16 credit hours	Total: 15 credit hours
Junior (31)	IDS 300W (3)	Philosophy and Ethics (3)
	Elective or Prerequisites Course (3)	Human Creativity (3)
	Elective or Prerequisites Course (3)	Elective or Prerequisites Course (3)
	Elective or Prerequisites Course (3)	Elective or Prerequisites Course (3)
	Law and Ethics (3), Choose One: CRJS 405, CRJS 406, or PHIL 355E	Elective or Prerequisites Course (3) Elective Course (1)
	Total: 15 credit hours	Total: 16 credit hours
Senior (30)	Cyber Foundations (3)	Cyber Applications (3)
	Cyber Foundations (3)	Cyber Applications (3)
	Cyber Foundations (3)	Cyber Applications (3)
	Cyber Foundations (3)	Cyber Applications (3)
	IDS 493 (3)	CYSE 368 or CYSE 494 (3)
	Total: 15 credit hours	Total: 15 credit hours
Program Total: 120 credit hours		

Part-Time Student

Year	Fall Semester	Spring Semester
Year 1 (13)	Written Communication I: ENGL 110C (3)	Written Communication II: ENGL 231 recommended (3)
	Oral Communication (3)	Nature of Science I (4)
	Total: 6 credit hours	Total: 7 credit hours
Year 2 (16)	Info. Literacy and Research (3)	Elective or Prerequisites Course (3)
	Human Behavior: CRJS 215S or SOC 201s (3)	Elective or Prerequisites Course (4)
	MATH 162 (3)	
	Total: 9 credit hours	Total: 7 credit hours
Year 3 (16)	Literature (3)	Interpreting the Past (3)
	Nature of Science II (4)	CYSE 250 (3)
		Elective or Prerequisites Course (3)
	Total: 7 credit hours	Total: 9 credit hours
Year 4 (15)	Impact of Technology: CYSE/IT 200T (3)	Elective or Prerequisites Course (3)
	Elective or Prerequisites Course (3)	Elective or Prerequisites Course (3)
	Elective or Prerequisites Course (3)	
	Total: 9 credit hours	Total: 6 credit hours
Year 5 (15)	IDS 300W (3)	Philosophy and Ethics (3)
	Elective or Prerequisites Course (3)	Human Creativity (3)
		Elective or Prerequisites Course (3)
	Total: 6 credit hours	Total: 9 credit hours
Year 6 (15)	Elective or Prerequisites Course (3)	Elective or Prerequisites Course (3)
	Law and Ethics (3), Choose One: CRJS 405, CRJS 406, or PHIL 355E	Elective or Prerequisites Course (3)
	Elective or Prerequisites Course (3)	
	Total: 9 credit hours	Total: 6 credit hours
Year 7 (15)	Cyber Foundations (3)	Cyber Foundations (3)
	Cyber Foundations (3)	IDS 493 (3)
	Cyber Foundations (3)	
	Total: 9 credit hours	Total: 6 credit hours
Year 8 (15)	Cyber Applications (3)	Cyber Applications (3)
	Cyber Applications (3)	CYSE 368 or CYSE 494 (3)
	Cyber Applications (3)	
	Total: 9 credit hours	Total: 6 credit hours
Program Total: 120 credit hours		

APPENDIX B
COURSE DESCRIPTIONS

Cybersecurity Core Courses

CYSE 200T. Cybersecurity, Technology and Society. 3 Credits.
Students will explore how technology is related to cybersecurity from an interdisciplinary orientation. Attention is given to the way that technologically-driven cybersecurity issues are connected to cultural, political, legal, ethical, and business domains.

CYSE 250. Basic Cybersecurity Programming and Networking. 3 Credits.
This course introduces the cybersecurity-centric programming and networking concepts. Students will develop problem-solving skills by using low-level programming languages (including C and assembly) and learn fundamentals of network protocols. This course is the technical base for students to take cybersecurity major courses.

CYSE 300. Introduction to Cybersecurity. 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 301. Cybersecurity Techniques and Operations. 3 Credits.
This course introduces tools and techniques used to secure and analyze large computer networks and systems. 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.

Interdisciplinary Core Courses

CYSE 368. Cybersecurity Internship. 1-6 Credits.
This course allows students to volunteer to work in an agency related to cybersecurity. Students must work for 50 hours per course credit and complete course assignments.

CYSE 494. Entrepreneurship in Cybersecurity. 3 Credits.
This course is designed to help students enhance their personal and professional development through innovation guided by faculty members and professionals. It offers students an opportunity to integrate disciplinary theory and knowledge through developing a nonprofit program, product, business, or other initiative. The real-world experiences that entrepreneurships provide will help students understand how academic knowledge leads to transformations, innovations, and solutions to different types of problems. The course can be delivered either as an independent project for individual students or as group projects similar to those sometimes offered in topics courses.

IDS 300W. Interdisciplinary Theory and Concepts. 3 Credits.
An examination of the history, concepts and application of interdisciplinary study. This course includes an analysis of similarities and differences in academic disciplines and the application of interdisciplinary approaches to a specific topic of study. This is a writing intensive course.

IDS 493. IDS Electronic Portfolio Project. 3 Credits.
The preparation of an electronic portfolio integrating the student's academic study, work experiences, skill identification and work products. Alternative formats are used for varying uses of the portfolio. Prerequisites: IDS 300W and senior standing.

Law and Ethics Courses

CRJS 406. Cyber Law. 3 Credits.
This course tackles two major cyber law subjects. The first part of the course examines various U.S. laws and legal considerations that impact the digital and cyberspace worlds from traditional civil, and to a lesser extent, traditional criminal perspectives. The second part 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. The course will also introduce students to miscellaneous cybersecurity topics such as the Federal Acquisition Requirements.

CRJS 405. Cybercrime and Cybersecurity. 3 Credits.
This course will provide students with an overview of computer-related crimes and how law enforcement officials investigate them. The course begins by describing the environment that has been created through information and communication technologies, and how this new environment facilitates different types of behavior. The course then moves into defining and describing the different types of computer-related crimes, the techniques used by officials, and the legal issues inherent in combating cybercrime.

PHIL 355E. Cybersecurity Ethics. 3 Credits.
This course examines ethical issues relevant to computing and information technology, including: privacy; freedom of speech and content control on the Internet; individual and social responsibility; cybersecurity; cybercrimes; social impact of computers and other digital technologies; and ethical obligations of IT professionals. Students will gain a broad understanding of central issues in cyberethics and the ways that fundamental ethical theories relate to these core issues.

Cybersecurity Foundation Courses

CS 462. Cybersecurity Fundamentals. 3 Credits.
Introduction to networking and the Internet protocol stack; vulnerable protocols such as HTTP, DNS, and BGP; overview of wireless communications, vulnerabilities, and security protocols; introduction to cryptography; discussion of cyber threats and defenses; firewalls and IDS/IPS; Kerberos; Transport Layer Security, including certificates; Network Layer Security.
Or

ECE 470. Foundations of Cyber Security. 3 Credits.
Course provides an overview of theory, tools and practice of cyber security and information assurance through prevention, detection and modeling of cyberattack and recovery from such attacks. Techniques for security modeling, attack modeling, risk analysis and cost-benefit analysis are described to manage the security of cyber systems. Fundamental principles of cyber security and their applications for protecting software and information assets of individual computers and large networked systems are explored. Anatomy of some sample attacks designed to compromise confidentiality, integrity and availability of cyber systems are discussed.

CS 463. Cryptography for Cybersecurity. 3 Credits.
This course covers mathematical foundations, including information theory, number theory, factoring, and prime number generation; cryptographic protocols, including basic building blocks and protocols; cryptographic techniques, including key generation and key management, and applications; and cryptographic algorithms--DES, AES, stream ciphers, hash functions, digital signatures, etc.

CS 464. Networked Systems Security. 3 Credits.
Authentication in cyber systems including password-based, address-based, biometrics-based, and SSO systems; authorization and accounting in cyber systems; securing wired and wireless networks; secured applications including secure e-mail services, secure web services, and secure e-commerce applications; security and privacy in cloud environments.
Or
ECE/MSIM 411. 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. Course will also discuss industry-standard network security protocols at application, socket, transport, network, VPN, and link layers, popular network security tools, security, performance modeling and quantification and network penetration testing. Discussion will be based on development of system level models and simulations of networked systems.

CS 465. Information Assurance. 3 Credits.
Introduction to information assurance. Topics to be covered include metrics, planning and deployment; identity and trust technologies; verification and evaluation, and incident response; human factors; regulation, policy languages, and enforcement; legal, ethical, and social implications; privacy and security trade-offs; system survivability; intrusion detection; and fault and security management.

CS 495. Topics in Computer Science – Reverse Software Engineering
The object of Software Reverse Engineering is to provide students with the understanding and practice to perform analysis on malware, deduce their and determine how malware works, and to aid the analysis via disassembly. Students will be able to use tools (IDAPro, Ollydbg) to safely perform static and dynamic analysis of malware, including encoded, packed, obfuscated ones. In particular, the course will have extensive hands-on labs/assignments on each knowledge unit.

CYSE 495. Topics in Cybersecurity – Cybersecurity Strategy and Policy. 3 Credits.
This course explores cybersecurity within the framework of strategy and policy making. The course covers topics like planning principles in cyber strategy, existing cybersecurity policies and their translation into government and business, strategy and policy development, risk management in cybersecurity. The relevance of cybersecurity strategy and policy to other policy issues and international dimension of cybersecurity policy making including crisis management and conflict resolution mechanisms are also explored within this course.

IT 315. Introduction to Networking and Security. 3 Credits.
Introduction to modern networking concepts and technology. Provides students with the fundamental concepts, technologies, components and issues related to communications and data networks. Topics include network architectures, infrastructures, services, protocols, cyberattacks, adversaries, and defense.

IT 417. Management of Information Security. 3 Credits.
This course emphasizes the need for management and technology to successfully implement an information security program in an organization. Threats, attacks, legal and ethical issues, risk assessment and control strategies; planning, development, and maintenance of security policies; contingency planning; firewalls, intrusion detection systems and security tools; and management of information security are some of the topics covered in this course.

ECE/MSIM 416. Cyber Defense Fundamentals. 3 Credits.
The objective of this course is to give an introduction of cyber hacking techniques and defense mechanisms to detect and thwart cybercrime. Cyberattacks aim at compromising cyber systems to disclose information, alter data or operation, cause denial of service, etc. The course first reviews the attacks to wireless networks, such as WiFi and MANET, and the defense strategies and technologies. Next, it reviews the attacks to general wired networks and information systems, and introduces the corresponding defense mechanisms. Last, it discusses cyber defense security policies and architectures.

ECE 419/MSIM. Cyber Physical System Security. 3 Credits.
Cyber Physical Systems (CPSs) integrate computing, networking, and physical processes. CPSs are known for their ability to: a) monitor the physical environment; b) use the monitored data in detecting the state of the physical environment; c) control the physical environment; and d) use cyber communications to perform its monitoring, detection and control operations. One of the biggest challenges to these systems is the security of its cyber space. This course will cover topics in CPS applications, design issues, and security.

Cybersecurity Applications Courses

CS 471. Operating Systems. 3 Credits.
Laboratory work required. Operating system structures. Multiprogramming and multiprocessing. Process management. Memory and other resource management. Storage management, I/O systems, distributed systems. Protection and security. The concepts will be illustrated through example systems such as Unix and Windows.

CYSE 407/CRJS 395. Digital Forensics. 3 Credits.
This course introduces the basic concepts and technologies of digital forensics. Students will learn the fundamental 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 495. Topics in Cybersecurity – Cyber War. 3 Credits
This course introduces the national security dimension of cybersecurity. The course covers topics like cybersecurity as a component of national security and investigate the topics of operational considerations in cybersecurity, planning in cyber war, different national approaches to cyber war. The international security perspective of the course assists the students view cybersecurity as a component of state power and make inferences about its utilization in international relations.

ECE/MSIM 417. Secure and Trusted Operating Systems. 3 Credits.
Course will review typical operating systems developing system models and identifying potential vulnerabilities. Course will discuss policies and their implementation required to fix such vulnerabilities to arrive at a secure and Trusted Computing Base. Course examines the security architecture Security Enhanced Linux (SELinux) Windows and Android OS.

ECE 452. Introduction to Wireless Communication Networks. 3 Credits.
Introduction to current wireless network technologies and standards. The radio spectrum and radio wave propagation models (pathloss, fading, and multipath). Modulation, diversity, and multiple access techniques. Wireless network planning and operation. Current and emerging wireless technologies (satellite systems, vehicular/sensor networks).

ECE 455. Network Engineering and Design. 3 Credits.
This course is an extension of ECE 355 into a semester long project. Emphasis is on gaining an understanding of networking design principles that entails all aspects of the network development life cycle. Topics include campus LAN models and design, VLANs, internetworking principles and design, WAN design, design of hybrid IP networks, differentiated vs. integrated services, traffic flow measurement and management.

IT 410. Business Intelligence. 3 Credits.
Business intelligence, data warehouse, data mining, and OLAP. The course will use state-of-the-art business intelligence software tools including SAS products to provide hands-on experience in designing and using data warehouses.

IT 416. Network Server Configuration and Administration. 3 Credits.
Advanced course on configuration and management of network servers. Topics include: user and storage management, ACLs, group policy, configuring security, backups and disaster recovery, and server management.

IT 418. Information Assurance. 3 Credits.
Assure information and manage risks related to the use, processing, storage, and transmission of information. Topics include assurance of integrity, availability, authenticity, non-repudiation and

confidentiality. Students will gain a firm understanding of information-related risk management in cyber and physical systems. Hands-on exercises and practice opportunities will be provided to students.

IT 419. Enterprise Cyber Defense. 3 Credits.
Provide students with an awareness of the options available to mitigate security threats in enterprise information systems. Topics include network mapping, network security techniques and components, applications of cryptography, malicious activity detection, countermeasures, and vulnerability scanning. Students will learn how to describe potential attacks, defense tools and methods, and measures to be taken when compromises occur.

IT 461. Implementing Internet Applications. 3 Credits.
Advanced design and implementation strategies are utilized to create dynamic e-commerce applications that solve complex problems in a secure and robust manner. Key concepts include: Internet architecture, structured data languages, scripting languages, programming languages, database connectivity, and Internet security.

APPENDIX C
FACULTY CURRICULUM VITAE (ABBREVIATED)

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.

Kalburgi, Vijay, PhD, 2003, Mechanical Engineering, Old Dominion University. Senior Lecturer of Information Technology & Decision Sciences. Specialization areas: information security, computer networks, and network administration.

Karahan, Saltuk, PhD, 2015, International Studies, Old Dominion University. Lecturer of Political Science and Cybersecurity. Specialization areas: cybersecurity and policy, cyberlaw, cyberwar, and leadership and management in Cybersecurity.

Kirkpatrick, Charles, MS, 2012, Technology Management, University of Virginia. Lecturer of Information Technology and Cybersecurity. Specialization areas: information security, technical infrastructure, networking and data center architecture.

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.

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.

Zehra, Susan, MS, 2012, Norfolk State University. Lecturer of Computer Science. Specialization areas: cybersecurity, software engineering, data organization, artificial intelligence, and the theory of computation.

APPENDIX D
EMPLOYMENT DEMAND
JOB ANNOUNCEMENTS

APPENDIX E
STUDENT DEMAND
STUDENT SURVEYS