Office of the President

January 2, 2018

Michael J. Kiphart, Ph.D.
Director of Academic Affairs
Maryland Higher Education Commission
6 N. Liberty Street
Baltimore, MD 21201

Dear Dr. Kiphart:

I am forwarding the following substantial change for Commission review:

Cybersecurity, AAS
Area of Concentration: Digital Forensics

This proposal includes a degree modification for one of the two requested areas of concentration within the Cybersecurity, AAS degree program: Digital Forensics. These new areas of concentration reflect the needs of a rapidly evolving and growing industry.

This submission has been thoroughly reviewed within the college and approved by the Board of Trustees. If further information is required, please contact Eileen Abel, Vice President of Academic Affairs (301-934-7846).

Sincerely,

Maureen Murphy, Ph.D.
President

LA PLATA • LEONARDTOWN • PRINCE FREDERICK • REGIONAL HUGHESVILLE

Office of the President
Center for Business and Industry, Room 204
8730 Mitchell Road, PO Box 910, La Plata MD 20646-0910
301-934-7625 • www.csmd.edu

MARYLAND HIGHER EDUCATION COMMMISSION ACADEMIC PROGRAM PROPOSAL

PROPOSAL FOR:

____ **NEW INSTRUCTIONAL PROGRAM**

__X__ **SUBSTANTIAL EXPANSION/MAJOR MODIFICATION**

____ **COOPERATIVE DEGREE PROGRAM**

__X__ **WITHIN EXISTING RESOURCES or____REQUIRING NEW RESOURCES**

(For each proposed program, attach a separate cover page. For example, two cover pages would accompany a proposal for a degree program and a certificate program.)

College of Southern Maryland
Institution Submitting Proposal

Fall 2018
Projected Implementation Date

AAS
Award to be Offered

Cybersecurity
Title of Proposed Program

5101.04
HEGIS Code

11.1003
CIP Code

Business and Technology
Department of Proposed Program

Bernice Brezina
Name of Department Head

James B. McNicholas III
Contact Name

JMCNICHOLAS@CSMD.EDU
Contact E-Mail Address

240-934-7595
Contact Phone Number

Signature and Date

President/Chief Executive Approval

12-14-17
Date

Date Endorsed/Approved by Governing Board

A. Centrality to mission and planning priorities, relationship to the program emphasis as outlined in the mission statements, and an institutional priority for program development;

The mission statement of the College of Southern Maryland (CSM, 2015) inspires the development of close partnerships among the college and its tri-county community stakeholders. The institutional commitment to "meet the diverse needs of students and the community" through "accessible, accredited, affordable, and quality learning opportunities for … career enhancement, and personal growth" aligns with the programmatic realities for the redesigned *Cybersecurity* AAS degree program (CSM, 2015).

The following is a description of the proposed changes:

This degree modification will incorporate two areas of concentration within the degree program:

Digital Forensics and *Network Security*.

Careful consideration was made to design the first semester to be common for both areas of concentration. This provides students with the same preparation for study while also providing them with the opportunity to explore the fields of network security and digital forensics before committing to an area of concentration. Further, the sequencing of the courses was determined so that students would have a well-rounded foundation that will ensue a successful progression through the program.

Two new courses are being proposed to support the tracks. They are:

Digital Forensics Track:

- ITS-2560 Digital Forensics II
- ITS-2565 Malware Analysis

In addition, the program will require the creation of a new course to support both programs. The new course will be the combination of two older courses and will incorporate the core fundamentals of the industry A+ certification. The new course will be entitled ITS-1050 (A+ Computing Essentials).

The *Cybersecurity* AAS program is consistent with CSM's Strategic Goal #2, which is to promote student success by providing outstanding education and related support services that help students achieve their goals (CSM, 2015). The new program will serve to increase graduate satisfaction with job preparation.

This program redesign will "effectively serve a changing student population and emerging workforce" (CSM, 2015). The new areas of concentration in *Digital Forensics* and *Network Security* reflect the needs of a rapidly evolving and growing industry. The recommendations enclosed are reflections of these elements and are consistent with the College's Vision, "To transform lives through lifelong learning and service" (CSM, 2015).

A new full-time Cyber\Computer Science faculty member and program coordinator was recently hired to teach the technical courses, manage the cyber lab, and promote the growth of the program.

B. Critical and compelling regional or Statewide need as identified in the State Plan;

The availability of an in-demand, STEM, career path, in an ever-evolving cybersecurity field, will attract both traditional and returning adult students, those entering a new field of opportunity as well as workers changing or upgrading skills. These changes are evident in CSM's enrollment records\statistics (Maryland Higher Education Commission, 2014). An examination of the demographics of our current student population reflects these realities and supports the needs identified in the 2014 Maryland State Plan for Post Secondary Education, "graduating a more diverse population of students in these critical disciplines." (MHEC, 2014).

The redesigned degree in Cybersecurity at CSM is consistent with the elements of the 2014 Maryland State Plan for Postsecondary Education. Much of our focus in curriculum development addressed the advisories cited in this document. All the goals were utilized as required criteria, but considerable attention was given to the Governor's Priorities and Goal #5: Economic Growth and Vitality (MHEC, 2014).

Citations in the State Plan (MHEC, 2014) also address the need for post secondary institutions to strive for academic excellence and effectiveness. The very nature of this charge is to develop student-centered learning bolstered by the partnerships with the various media employers in our region. This format increases experiential learning through internships and other hands on job related activities assuring workplace readiness.

CSM's Cybersecurity AAS program will offer courses that, taken together, enable our students to matriculate and earn their AAS degree. Formative and summative evaluations are an essential value of the educational process at CSM, and are a viable part of the new CSM program. Students are held to standards that are reflective of academic and professional systems, while the structure and operation of the program provides the environment to support the achievement of these standards.

Our cybersecurity advisor council feedback indicates that employers are interested in helping to develop the program, which will include the creation of internships and other opportunities. These are extremely important as they provide students enrolled at CSM in cybersecurity both vital experience and opportunities for networking. In addition, these opportunities will increase student's marketability, especially if a clearance is issued during an internship.

To expand our geographic reach, stimulate enrollment and provide increased access to this new curricular option, the cybersecurity program intends to incorporate alternative means of course delivery. The program intends to provide traditional face-to-face courses complimented by offerings that are hybrid or fully online by form. The College of Southern Maryland has demonstrated success in delivering instruction by alternative methods, increasing flexibility and effective use of new technologies. The Division of Distance Learning and Faculty Development (DLF) support the faculty in developing high quality, accessible and effective teaching and learning environments.

To facilitate these goals, the DLF staff provides service to faculty including planning, consulting, training, and support. The DLF staff makes available the resources necessary to incorporate instructional technologies into their traditional or distance learning courses. As such, the DLF staff will contribute significantly to the delivery of all new courses in Engineering Technology by providing the faculty with the necessary support structures to enhance student success in their

delivery, particularly those identified for distance learning, be the methodology fully on line or hybrid.

In summary, the new degree in Cybersecurity at the College of Southern Maryland as proposed is consistent with and reflective of the current Maryland State Plan for Postsecondary Education (MHEC, 2014).

C. Quantifiable and reliable evidence and documentation of market supply and demand in the region and service area;

Cybersecurity is currently ranked as one of the fastest growing fields in the global marketplace (Kauflin, 2017). The demand for qualified candidates is strong due to a shortage of around 2 million cybersecurity professionals (ISACA, 2017). Maryland and particularly Southern Maryland is no exception to the cyber professional shortage and demand resulting demand.

The Maryland Department of Business & Economic Development (MDBED) (n.d.) notes that "cybersecurity and information innovation technologies represent an unparalleled economic and employment growth opportunity for Maryland." The Cyber Pathways Across Maryland (n.d.) group quantified this growth rate as 41% over the next 8 years. The Maryland State Plan for Postsecondary Education notes, "colleges and universities should continue to prepare students for careers in high-demand, cutting-edge industries such as biotechnology, cyber security, and sustainable energy" (MHEC, 2014). To support this growth the state and federal government has invested a significant amount of money into cyber programs, including the College of Southern Maryland, to develop high quality cyber education programs.

This program redesign is a result of this demand. Our program will provide students with the skills to seek employment with state, local, and federal agencies in additional to private companies. Particularly attention is being directed to develop the skills required by U.S. Navy Cyber Command and the U.S. Cyber Command, both which are based in Maryland (MDBED, n.d.). The demand for these two agencies in particular represents a great opportunity for our students as the demand is so high that there are talks of waiving boot camp requirements for cyber recruits (Gallagher, 2017).

The table below demonstrates the anticipated growth of cybersecurity in Maryland:

Maryland: Cybersecurity Growth	
2014 Employment Estimate*	86,210
2024 Projected Employment	113,750
% Change	31.5%
Projected Annual Openings	4,100

Figure 1. Spotlight on Cybersecurity. Department of Labor, Licensing and Regulations (DLLR), (2017).

A projected growth rate of 31.5% over the given span is quite significant. This number may be rather conservative given the large population of government agencies and contractors that are tasked with supporting the nation's cyber interests. In addition, "Maryland's 11,600 information technology businesses are annually awarded $10.36 billion in federal contracts and generate $39.55 billion in economic activity, making it one of the nation's leaders and a major economic engine for the state" (Maryland, 2017).

STUDENT CHARACTERISTICS	
Spring 2014 – Spring 2017	
Program - AAS.CYBER.SECURITY	
Growth (All Campuses):	+74 students, +80.4%
Growth 4-Year (2014-2017):	100%

Figure 2. Student Characteristics. College of Southern Maryland, (2017).

D. Reasonableness of program duplication, if any;

The following community colleges have programs in cybersecurity, network security, and/or digital forensics:

CYBER SECURITY DEGREES AT MARYLAND COMMUNITY COLLEGES		
Institution	**Program Name**	**Degree Offered**
Anne Arundel Community College	Information Assurance & Cybersecurity	Associates Degree
Carroll Community College	Cybersecurity	Associates Degree
Cecil Community College	Cybersecurity	Associates Degree
College of Southern Maryland	Cybersecurity	Associates Degree
Community College of Baltimore County	Cybersecurity	Associates Degree
Frederick Community College	Cybersecurity	Associates Degree
Garrett College	Cybersecurity	Associates Degree
Hagerstown Community College	Cybersecurity	Associates Degree
Harford Community College	Information Assurance & Cybersecurity	Associates Degree
Montgomery College	Cybersecurity	Associates Degree
Prince Georges College	Cybersecurity	
Source: Maryland Higher Education Commission, Finding a Major http://www.mhec.maryland.gov/utilities/search_major.asp		

The above programs are all similar in providing students with the skills and knowledge to gain employment in entry-level positions in various areas of cybersecurity. CSM's program is

designed with local workforce needs in mind, while still offering students with the education required to pursue non-Navy or DOD job opportunities in other fields of cybersecurity such as law enforcement and civil ligation (e-discovery).

This degree program prepares students who are currently employed in the cybersecurity field, including active law enforcement, as well as those without prior work experience to develop the skills and knowledge required of practitioners in a variety of cybersecurity settings.

The first semester is the same for all students in this program. The first semester is designed to provide all students with a basic foundation in computer theory. The second semester is where students begin to explore cybersecurity concepts. At the conclusion of the second semester the student will select, which track they wish to pursue. This ability to select a track will provide students with the options to meet both their educational and specific career goals.

The tracks are critical to ensuring that the educational plan supports the students career goals considering that cybersecurity is not a homogenous field. The previous degree plan failed to realize this reality, which has required our students to seek additional training in order to seek gainful employment in certain cybersecurity positions. The addition of the tracks also expands our ability to create specific and meaningful relationships with various regional employers.

E. Relevance to the implementation or maintenance of high-demand programs at HBIs;

There is no impact to the uniqueness, identities and missions of HBIs. The only other college in the tri-county area is St. Mary's College.

F. Relevance to the support of the uniqueness and institutional identities and missions of HBIs;

There is no impact to the uniqueness, identities and missions of HBIs. The only other college in the tri-county area is St. Mary's College.

G. Adequacy of curriculum design and delivery to related learning outcomes consistent with Regulation .10 of this chapter;

The program description and requirements are as follows:

No. of Credits: 60

This degree program prepares students who are currently employed in the cybersecurity field as well as those without prior work experience to develop the skills and knowledge required of practitioners within a variety of cybersecurity related settings.

The first semester is the same for all students in this program. The first semester is designed

to provide all students with a basic foundation in computer theory. The second semester is where students begin to explore cybersecurity concepts. At the conclusion of the second semester the student will select, which track they wish to pursue.

Students pursuing the digital forensics track will navigate through the entire digital forensics course sequence and upon completion will have sufficient knowledge to sit for the Global Certified Forensic Examiner (GCFE) and Computer Hacking Forensic Investigator (CHFI) industry certifications. This track will place special emphasis on the knowledge, skills, and abilities to conduct civil and/or criminal digital forensics investigations and to develop and administer policy in support of digital forensic programs.

Regardless of the track that students select, all students will take classes that will help to prepare for the following entry level cybersecurity industry certifications: CompTIA A+, CompTIA Security+, CompTIA Linux+, and Cisco Certified Entry Networking Technician (CCENT).

Students will be taking courses in this program through several course delivery formats. Since it is imperative that students obtain hands-on experience with the various tools, technologies and techniques employed in the cybersecurity field, some courses will only be offered in a face-to-face lab environment. Courses not identified as a program core may be offered in an online only section.

It should be noted that oral and written communication skills are emphasized throughout this program. Both tracks will require several courses in writing and communications. In addition, students will have multiple learning opportunities to improve soft skills by completing activities such as developing a resume or portfolio, preparing for a job interview, and delivering project presentations.

This program has been designated as a CAE-CDE 2Y - National Centers of Academic Excellence in Cyber Defense 2-Year Education by the National Security Agency (NSA) and Department of Homeland Security (DHS)

The maximum number of credits accepted in transfer from other institutions to this program is 45.
The recommended program sequence is as follows:

First Semester
ITS-1050 – A+ Computing Essentials (3) (NEW COURSE)
ITS-2511 – Networking I (3)
Biology/Physical Science (3): Acceptable - See Gen Ed Listing (3)
ENG-1010 – Composition and Rhetoric (3)
Mathematics – Acceptable - See Gen Ed Listing (3)

Second Semester
ITS-1960 – Introduction to Linux (3)
ITS-2090 – Computer Security (3)
ITS-2516 – Networking II (3)
ITS-2555 – Digital Forensics I (3) (NEW COURSE)
ENG-2050 – Business and Technical Writing (3)

Third Semester
ITS-1110 – Program Design and Development (3)
ITS-2545 – Information System Security (3)
ITS-2565 – Digital Forensics II (3) (NEW COURSE)
COM-1250 – Introduction to Interpersonal Communication (3)
PHL-1150 – Cyber Ethics (3)

Fourth Semester
ITS-2500 – Ethical Hacking and Penetration Testing (3)
ITS-2526 – Networking IV (3)
ITS-2536 – Networking Infrastructure and Defense (3)
ITS-2950 – Cybersecurity Capstone (3) (NEW COURSE)
Social Science (3): Acceptable - See Gen Ed Listing (3)

Cybersecurity, AAS

General Education	
3 credits English Composition	ENG-1010 English Composition (3)
3 credits Arts/Humanities	COM-1250 Introduction to Interpersonal Communication (3)
3-4 credits Biological/Physical Sciences	Biological/physical sciences (3 credits) Select 3 credits from the General Education Course List
3 credits Social/Behavioral Sciences	Social/behavioral sciences (3 credits) Select 3 credits from the General Education Course List
3 credits Mathematics	Mathematics Select 3 credits from the General Education Course List
Other General Education (from above categories) (3 credits)	PHL-1150 - Cyber Ethics (3)
	General Education= 18
Major Requirements	ITS-1050 A+ Computing Essentials (3) ITS-2511 Networking I (3) ITS-1960 Introduction to Linux (3) ITS-2090 Computer Security (3) ITS-2516 Networking II (3) ITS-2500 Ethical Hacking and Penetration Testing (3) ITS-2536 Networking Infrastructure and Defense (3) ITS-2545 Information Systems Security (3) ITS-2950 Cybersecurity Capstone (3) ENG-2050 Business and Technical Writing (3)
	Major Requirements=30
Digital Forensics Concentration	ITS-1110 Program Design and Development (3) ITS-2555 Digital Forensics I (3) ITS-2560 Digital Forensics II (3) ITS-2565Malware Analysis (3)
	Concentration Credits= 12
	Credit total= 60

Course descriptions for the required and technical elective courses are provided below:

COM-1250 – Introduction to Interpersonal Communication (3)

Prerequisite: ENG 0900 and RDG 0800 or FYS 1010T

Students are able to combine theory and application of communication principles involved in initiating, developing, and maintaining a relationship. Aspects of one-to-one and small group communication are explored including perception, self-concept, listening, intercultural and gender communication, and conflict management. College-level writing skills are recommended.

ENG-1010 – Composition and Rhetoric (3)

Prerequisite: ENG 0900; and RDG 0800 or FYS 1010T; or placement

Students in this course complete their first semester college-level composition course. Students focus on planning, organizing, and developing a variety of argumentative compositions. Students practice the conventions of written Standard American English, gain information literacy skills, and learn research and documentation techniques including conducting online and print research and documenting sources. By the end of the semester, students demonstrate their ability to write a unified and coherent argument-based essay of about one thousand words that incorporates research and is nearly free of grammatical, mechanical, and structural errors. Students should refer to the schedule of classes for sections of this course taught in a computer lab. Students must pay an additional lab fee when taking this course in a computer-assisted classroom. Students may earn credit for this course through CLEP or Advanced Placement Examination. A minimum grade of "C" is required to pass the course.

ENG-2050 – Business and Technical Writing (3)

Prerequisite: ENG 1010

Students develop writing skills through composing a variety of clear, effective memos, letters, and reports. Subject matter for the papers may come from the student's occupation or interests, whether scientific, technical, or non-technical. Students should refer to the schedule of classes for sections of this course which are taught in computer labs.

ITS-1050 – A+ Computing Essentials (3) (NEW COURSE)

Prerequisite: RDG 0800 or FYS 1010T

Students gain knowledge and practical experience with PC hardware and peripherals, mobile device hardware, networking and troubleshooting, hardware and network connectivity issues. Students also gain practical experience installing and configuring popular operating systems. Students will be introduced to topics in security, the fundamentals of cloud computing and operational procedures. This course helps students to prepare for the CompTIA A+ Certification.

ITS-1110 – Program Design and Development (3)

Prerequisite: RDG 0800 or FYS 1010T

Students learn to solve business-oriented problems with emphasis on structured and object oriented programming techniques. Design tools are used to develop pseudo-code, flowcharting and 3D interactive environments. Students are introduced to several software packages that may be used to develop pseudo-code, flowcharts and interactive 3D environments. For students who plan to use personal computers, this course may have specific computing requirements. Please refer to the Quick Link for Computing Requirements on the Business and Technology website.

ITS-1960 – Introduction to Linux (3)

Prerequisite: ITS-1050

Students learn the basic concepts of the Linux operating system as it relates to computer hardware, software, and operations, including command syntax, file management and maintenance, and troubleshooting of user problems. For students who plan to use personal computers, this course may have specific computing requirements. Please refer to the Quick Link for Computing Requirements on the Business and Technology website.

ITS-2090 – Computer Security (3)

Co-requisite: ITS-1050

ITS-2090 covers the fundamentals of operational security, network security, managing a public key infrastructure (PKI), authentication, access control, external attack, and cryptography. Students learn about the security procedures to protect data in computer environments, the different network attack scenarios, the many tools and procedures used by organizations to protect their resources, and the ethical issues raised by computer security in the business world. This course helps prepare students for the CompTIA Security+ exam. The vendor neutral CompTIA Security+ certification is the acceptable industry-level security certification. For students who plan to use personal computers, this course may have specific computing requirements. Please refer to the Quick Link for Computing Requirements on the Business and Technology website.

ITS-2150– Business Continuity and Disaster Recovery (3) (NEW COURSE)

Prerequisite: ENG-2050, ITS-1050, ITS-2511

Students will analyze and implement strategies to ensure business continuity in an information technology environment. This will involve the study of various risk management frameworks to support a robust and proactive approach to various types of threats. In addition, students will develop disaster recovery plans to support the entire business continuity and disaster recovery process.

COM-1450 - Groups, Teams, and Leadership* (3)

Prerequisite: ENG 0900 and RDG 0800 or FYS 1010T

Students learn leadership skills by working in teams to design and complete group projects. Students learn to plan, conduct, and participate in meetings. Student work includes working in groups outside of class, participating in service learning projects, and observing public groups and meetings.

ITS-2500 – Ethical Hacking & Penetration Testing (3)

Prerequisite: ITS 2090
Co-requisite: ITS-2190 PHL-1150 ITS-2536

Students learn how intruders, including hackers, attack systems and networks as well as best ethical practices for scanning, auditing, penetration testing, and securing assigned systems. In addition students will explore how intruders escalate privileges, strategies for preempting attacks as well as the legal and ethical nature of security countermeasures.

ITS-2511 – Networking I (3)

Co-requisite: ITS-1050

Students learn networking fundamentals and network terminology in this first of a four-course series. Topics covered include open system interconnection (OSI) models, Ethernet technologies, network media, basics of TCP/IP, and IP addressing. Training is provided in the use of networking software and tools that are required to troubleshoot networking problems. For students who plan to use personal computers, this course may have specific computing requirements. Please refer to the Quick Link for Computing Requirements on the Business and Technology website.

ITS-2516 – Networking II (3)

Prerequisite: ITS 2511

Students learn router and routing basics in this second of a four-course series. This course provides students with an understanding of TCP/IP, basic router configuration, installation of routing protocols, network troubleshooting skills, and configuration of networking software and tools that are required to troubleshoot networking problems. For students who plan to use personal computers, this course may have specific computing requirements. Please refer to the Quick Link for Computing Requirements on the Business and Technology website.

ITS-2521 – Networking III (3)

Prerequisite: ITS 2516

Students learn switching basics and intermediate routing in this third of a four-course series. Topics covered include Ethernet switching, switch concepts, and configuration of switches using command-line interface. Training is provided in the use of networking software and tools that are required to troubleshoot network problems. For students who plan to use personal computers, this course may have specific computing requirements. Please refer to the Quick Link for Computing Requirements on the Business and Technology website.

ITS-2526 - Networking IV (3)

Prerequisite: ITS 2521

Students learn WAN technology and terminology in the final course of a four-course series. Topics include ISDN and DDR, Frame Relay technologies, configuring PPP, level 1 troubleshooting service, DHCP for dynamic address management, and address translation with NAT and PAT. Training is provided in the use of networking software and tools that

are required to troubleshoot network problems. For students who plan to use personal computers, this course may have specific computing requirements. Please refer to the Quick Link for Computing Requirements on the Business and Technology website.

ITS-2536 – Network & Infrastructure Defense (3)

Co-requisite: ITS 2090

ITS 2536 focuses on teaching students how to manage and apply technologies to protect networks. An understanding of security technologies including firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), virus protection, TCP packet sniffing and analysis, VPNs (virtual private networks), and disaster recovery will be addressed. For students who plan to use personal computers, this course may have specific computing requirements. Please refer to the Quick Link for Computing Requirements on the Business and Technology website.

ITS-2545 – Information Systems Security (3)

Prerequisite: ITS 2090

Students learn the management principles of information security. The course will cover many aspects of security including hardware, software, communication, and physical security. Security policy, legal and ethical issues will also be covered. The relationship between course topics and CISSP domains are also highlighted. For students who plan to use personal computers, this course may have specific computing requirements. Please refer to the Quick Link for Computing Requirements on the Business and Technology website.

ITS-2555 Digital Forensics I (3) (NEW COURSE)

Prerequisite: ITS-1050, ITS-2511
Corequisite: ITS-2050

Students will navigate through each phase of the digital forensics analysis methodology using a practical and hands-on approach. Various open source and commercial digital forensic software packages will be used in conjunction with hardware based tools to support the process. Topics such as anti-forensics measures will be examined to demonstrate the impact they can have on an investigation. Students will also explore the various laws and regulations that guide the digital forensics process during both criminal and civil litigation. In addition, students will learn how to prepare policy documentation to build and maintain a successful digital forensics laboratory.

ITS-2560 – Digital Forensics II (3) (NEW COURSE)

Prerequisite: ITS-2555 Digital Forensics I

Students will navigate through each phase of the digital forensics analysis methodology with special emphasis on conducting full scale civil and criminal investigations. Students are expected to build and support a digital forensics laboratory that will be utilized throughout the entire course. Digital forensics specific hardware and software will be used to acquire and analyze images from common hardware and mobile based device types. Network forensics concepts will also be explored along with an introduction to malware analysis. At the end of the course students must present and defend their final case report in front of a live jury.

ITS-2565 – Malware Analysis (3) (NEW COURSE)

Prerequisite: ITS-2560 Digital Forensics II, ITS-1110

Students will explore various types of malware types, their functions, and their potential impact. Basic, static, and dynamic analysis methods will be examined and demonstrated using various industry standard tools. Concepts such as packing, unpacking, and rooting will be explored along with countermeasures and anti-forensics. Various case studies will be examined to identify deficiencies in technology and society with the goal of improving the malware analysis process.

ITS-2950 – Cybersecurity Capstone (NEW COURSE)

Prerequisite: 45 credits completed
Corequisite: ITS-2526 or ITS-2565 Malware Analysis

Students from each track will work together to establish and maintain a secure information technology enterprise. All of the key topics and concepts covered in the program, and within each track, will be expected to be incorporated into each team's architecture and support infrastructure. Threats and challenges will be presented to determine the effectiveness of the policies, procedures, tools, and techniques employed by each team. Each team will be expected to present a final report on their experience that demonstrates the strengths and weaknesses of their approach along with possible improvements. During the course cycle the instructor will assist students in generating a portfolio of their activities and achievements that can be utilized when seeking employment or applying to a four year institution.

Through the curriculum, professional organizations and engagement activities, graduates of the College of Southern Maryland's Cybersecurity AAS program will achieve the following educational objectives:

a. Provide graduates with a common body of knowledge in cybersecurity.
b. Provide graduates with the capability to develop the skills and knowledge required of cybersecurity practitioners in a variety of cybersecurity settings.
c. Provide graduates the resources and skills allowing them to find employment or enter trainee programs in cybersecurity and related professions.

Through the curriculum, professional organizations and engagement activities, graduates of the College of Southern Maryland's Cybersecurity AAS program will achieve the following intended student learning outcomes:

Students will…

1. Students will be utilize industry standard tools and technology in order to identify, respond to, and remediate various types of cyber threats.
2. Students will apply industry standard information security practices to solve a variety of business and technical problems.
3. Students will be able to identify and analyze professional, ethical, technical, and social issues related to cybersecurity and the use of information\computing technologies.
4. Students will examine and apply knowledge in each of the following cybersecurity domains: Security and Risk Management; Asset Security; Security Engineering; Communication and Network Security; Identify and Access Management, Security Assessment and Testing, Security Operations.
5. Students will be able to develop and present (oral & written) reports to both technical and non-technical audiences.

Digital Forensics Concentration:

Students will…

1. Students will be able to understand and navigate through each phase of the digital forensics lifecycle.
2. Students will conduct digital forensic investigations in mock environments that will represent what is encountered during real civil and criminal investigations.
3. Students will learn the importance of evidentiary integrity.
4. Students will be able to perform physical acquisitions on various types of media (USB, HDD, SSD, Mobile Devices, ect.)
5. Students will be able to identify artifacts in Windows, MAC, Linux, and various other environments.
6. Students will conduct malware investigations and reverse engineer malware with the goal of remediation and attribution.
7. Students will present complied analysis reports as expert witnesses during mock trials.
8. Students will be able to develop and maintain policies and procedures to support a digital forensics laboratory\unit.
9. Students will learn the laws government digital evidence during civil and criminal proceedings.

There are 18 General Education credits required for this program (A.A.S). The General Education course requirements are

Both Concentrations		
Course	**Fulfils**	**Credits**
ENG-1010	English Composition	3
Biology/Physical Sciences (Any Gen. Ed.)	Biological/Physical Sciences	3
Social/Behavioral Sciences (Any Gen. Ed.)	Social/Behavioral Sciences	3
Math (Any Gen Ed.)	Mathematics	3
PHL-1150	Arts/Humanities	3
COM-1250 or COM-1450	Arts/Humanities	3
	TOTAL:	18

H. Adequacy of any articulation;

The division is currently taking steps to create and/or strengthen articulation agreements with partner institutions. We are particularly interested in creating an agreement with 4-year colleges and universities in the region to support the forensics track and the networking track. Considering the demand for cyber security professionals, we anticipate many partnerships as we move forward with the new program. Existing articulation agreements will be updated.

I. Adequacy of faculty resources consistent with Regulation .11 of this chapter;

Faculty Name	Appointment Type	Terminal Degree Title & Field	Academic Title & Rank	Status	Course(s)
James B. McNicholas III	Permanent	▪ M.S. – Digital Forensics & Cyber Investigation ▪ M.S. Information Technology – Software Engineering (P.S.M. Designated Degree) ▪ M.B.A – Master of Business Administration	Assistant Professor	Full-time	ITS-1050 ITS-1110 ITS-2090 ITS-2500 ITS-2536 ITS-2545 ITS-2550 ITS-2560 ITS-2570 ITS-2552 ITS-2910 PHL-1150
Ronda Jacobs	Permanent	▪ M.A. – Adult Education & Distance Learning	Assistant Professor	Full-time	ITS-1050
Renee Jenkins	Permanent	▪ Ed. D. – Higher Education Adult Education/Math Education ▪ M.E. – Educational Technology	Professor	Full-time	ITS-1960 ITS-2536
Daphne Powell	Permanent	▪ M.S. – Human Resource Development	Professor	Full-time	ITS-2511 ITS-2516 ITS-2521 ITS-2526
James Graves	Adjunct	▪ M.S. - Telecommunications Management	Adjunct	Part-Time	ITS-2511 ITS-2516 ITS-2521 ITS-2526
Richard White	Permanent	▪ M.S. – Information Technology, Database Adm. ▪ M.S. – Project Management ▪ M.B.A – Master of Business Administration	Assistant Professor	Full-time	ITS-1050 ITS-1110 ITS-2090
John Wilson	Permanent	▪ M.A. – National Security Affairs	Professor	Full-time	PHL-1150 ITS-2190

J. Adequacy of library resources consistent with regulation .12 of this chapter

Students may borrow circulating materials from any of the three CSM library branches. Through the interlibrary loan program (ILL), students can order almost any book, periodical article, or ERIC

document needed, generally available within one week of the request. Library resources also include audiovisual collections use in the library and classrooms only. Additionally, substantial material is available through online databases, including ProQuest and EBSCO.

The President assures that appropriate library resources are available to support the needs of this program.

K. Adequacy of physical facilities, infrastructure, and instructional equipment consistent with Regulation .13 of this chapter;

CSM is a leader among Maryland community colleges in offering courses which meet the busy schedules of our students, traditional weekday face to face courses, weekend and evening classes, Web-hybrid courses which offer a mix of online and traditional classroom face-to-face instruction and a popular online learning community. The college makes available state of the art facilities on three campuses to accomplish its mission in support of our community's academic, professional, and self-enrichment pursuits.

Courses supporting the new degree program in Cybersecurity will taught across each of the three campuses (La Plata, Leonardtown, and Prince Frederick). Each campus will have a room dedicated for the exclusive use of the cyber program. Each lab will be outfitted with identical equipment, through funds provided by the TAACT grant.

"The President assures that appropriate physical facilities, infrastructure, and instructional equipment are available to support the needs of this program."

L. Adequacy of financial resources with documentation consistent with Regulation .14 of this chapter;

TABLE 1: RESOURCES					
Resource Categories	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**
1. Reallocated Funds	0	0	0	0	0
2. Tuition/Fee Revenue (c + g below)	$113,250	$129,105	$167,610	$183,465	$199,320
a. Number of F/T Students	25	30	35	40	45
b. Annual Tuition/Fee Rate ($151 x 21 credits)*	$3,171	$3,171	$3,171	$3,171	$3,171
c. Total F/T Revenue (a x b)	$79,275	$95,130	$110,985	$126,840	$142,695
d. Number of P/T Students	15	15	25	25	25
e. Credit Hour Rate	$151	$151	$151	$151	$151
f. Annual Credit Hours Rate	15	15	15	15	15
g. Total P/T Revenue (d x e x f)	$33,975	$33,975	$56,625	$56,625	$56,625

3. Grants, Contracts & Other External Sources	0	0	0	0	0
4. Other Sources	0	0	0	0	0
TOTAL (Add 1 – 4)	$113,250	$129,105	$167,610	$183,465	$199,320
* The credit hour rate ($151) is based upon CSM's current tuition rate of $123 plus 23% combined fee.					

TABLE 2: EXPENDITURES:					
Expenditure Categories	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**
1. Faculty (b + c below)	$ 70,000	$ 70,000	$ 140,000	$ 140,000	$ 140,000
a. # FTE	1 FT x 5 courses	1 FT x 5 courses	2 FT x 5 courses	2 FT x 5 courses	2 FT x 5 courses
b. Total Salary	$ 70,000	$ 70,000	$ 140,000	$ 140,000	$ 140,000
c. Total Benefits	0	0	0	0	0
2. Admin. Staff (b + c below)	0	0	0	0	0
a. # FTE	0	0	0	0	0
b. Total Salary	0	0	0	0	0
c. Total Benefits	0	0	0	0	0
3. Support Staff (b + c below)	0	0	0	0	0
a. # FTE	0	0	0	0	0
b. Total Salary	0	0	0	0	0
c. Total Benefits	0	0	0	0	0
4. Equipment	0	0	0	0	0
5. Library	0	0	0	0	0
6. New or Renovated Space	0	0	0	0	0
7. Other Expenses	0	0	0	0	0
TOTAL (Add 1 – 7)	$ 70,000	$ 70,000	$ 140,000	$ 140,000	$ 140,000

M. Adequacy of provisions for evaluation of program consistent with Regulation .15 of this chapter;

Discuss procedures for evaluating courses, faculty and student learning outcomes.

SLOAP's focus is the primary mission of the college: to provide quality opportunities for intellectual development that result in student learning. The SLOAP outlines the process of collecting information to determine whether CSM's academic offerings are having the appropriate educational impact on students. Student Learning Outcomes Assessment (SLOA) is defined as the systematic collection of information about academic offerings and analysis thereof, for the purpose of improving student learning.

Program Assessment at CSM is a cyclical process that includes:

1. Program Reviews conducted every five-six years, or more often as needed.
2. Academic certificate programs are included within the review of degree programs.
3. Program Monitoring conducted every other year (except in the year of a Program Review).
4. Program Assessments of Student Learning conducted on a cycle established by faculty.

In addition, CSM conducts course evaluations every semester or, more often when deemed necessary.

N. Consistency with the Commission's minority student achievement goals; and

One of CSM's Values/Guiding Principles is Diversity. The Institutional Equity and Diversity Office works to "create an environment that instills an appreciation and understanding of the diverse qualities each of us brings to this campus; where our students, staff, and faculty mirror the community we serve and are free from discrimination and harassment."

Additionally, CSM defines civility as "the demonstration of respect for others through basic courtesy and the practice of behaviors that contribute toward a positive environment for learning and working."

As is true of CSM, the Cybersecurity program is open to all students with no restrictions reference to age, gender, or ethnic background. As such, any student meeting the eligibility requirements of the college admissions process is entitled to enroll in this discipline of study. Furthermore, CSM, the Business & Technology Division, and representatives of the Cybersecurity program all participate in events, programs, orientations, and information sessions sponsored internally or by external advocates in order to reach all students seeking information on the college's programs and the professional opportunities that result from that education and training.

CSM's marketing department is developing a comprehensive marketing plan for this new program. These resources include the designing and printing of brochures, assistance with marketing campaigns (web and traditional news media), and development of other recruitment materials. CSM is committed to ensuring new programs are marketed to diverse populations, as demonstrated by the organizational values, which include valuing diversity. Marketing plans will include activities specifically designed to market the program to the diverse population of the tri-county region.

Diversity and multiculturalism are vitally important issues for future leaders. As such, the representatives of this new program at CSM intend to make contact with multiple professional associations, national, regional and local employers, secondary and postsecondary institutions to create partnerships that will lead to the diversity of our student population and graduates of our programs.

O. Relationship to low productivity programs identified by the Commission.

The proposed program is not directly related to an identified low productivity program identified by the Commission.

P. If proposing a distance education program, please provide evidence of the Principles of Good Practice (as outlined in COMAR 13B.02.03.22C)

The proposed program is not designed as a distance education program as less than 50% of the courses will be offered online.

References

College of Southern Maryland. (2017). *Student Characteristics*. Retrieved from https://www.csmd.edu/Assets/AboutUs/PIER/student_characteristics_credit_sp17.pdf

College of Southern Maryland. (2015). *College of Southern Maryland 2015-2018 Strategic Plan*. Retrieved from https://www.csmd.edu/Assets/AboutUs/Strategic-Plan/StrategicPlan2015-2018_R2.pdf

Cyber Pathways Across Maryland. (n.d.). Cybersecurity in Maryland. Retrieved from http://cyberpathwaysacrossmd.com/cyberinmaryland.html

Department of Labor, Licensing and Regulations (DLLR). (2017). *Spotlight on Cybersecurity*. Retrieved from https://mwejobs.maryland.gov/admin/gsipub/htmlarea/uploads/SpotlightCybersecurity_newLMI.pdf

ISACA. (2017). *Cybersecurity Nexus (CSX) Fact Sheet.* Retrieved from https://www.isaca.org/cyber/Documents/Cybersecurity-Nexus-Fact-Sheet_pre_Eng_0117.pdf

Kauflin, J. (2017). The fast-growing job with a huge skills gap: cybersecurity. *Forbes*. Retrieved from https://www.forbes.com/sites/jeffkauflin/2017/03/16/the-fast-growing-job-with-a-huge-skills-gap-cyber-security/#4f79e3285163

Maryland. (2017). *Maryland IT & Cybersecurity Story*. Retrieved from https://open.maryland.gov/it-and-cybersecurity/

Maryland Higher Education Commission. (2014). *Maryland Ready: 2013-2017 Maryland State Plan for Postsecondary Education*. Retrieved from http://mhec.maryland.gov/institutions_training/Documents/acadaff/acadproginstitapprovals/MHECStatePlan_2014.pdf

Maryland Higher Education Commission. (2009). *2009 Maryland State Plan for Postsecondary Education. Retrieved from* http://mhec.maryland.gov/Documents/2004Plan/JUNE_2009_FinalEdited.pdf