MARYLAND HIGHER EDUCATION COMMMISSION
ACADEMIC PROGRAM PROPOSAL

PROPOSAL FOR:

__X__ **NEW INSTRUCTIONAL PROGRAM**

_____ **SUBSTANTIAL EXPANSION/MAJOR MODIFICATION**

_____ **COOPERATIVE DEGREE PROGRAM**

_____ **WITHIN EXISTING RESOURCES or __X__ 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.)

Mount St. Mary's University
Institution Submitting Proposal

Spring 2019
Projected Implementation Date

Post Baccalaureate Certificate
Award to be Offered

Risk Management and Cybersecurity for Professionals
Title of Proposed Program

Suggested HEGIS Code

11.1003
Suggested CIP Code

Math and Computer Science
Department of Proposed Program

Dr. Melanie Butler
Name of Department Head

Dr. Boyd Creasman, Provost	b.creasman@msmary.edu	301-447-5218
Contact Name	Contact E-Mail Address	Contact Phone Number

1/24/2018
Signature and Date — President/Chief Executive Approval

1/15/18
Date — Date Endorsed/Approved by Governing Board

MOUNT ST. MARY'S UNIVERSITY

OFFICE OF THE PROVOST
16300 OLD EMMITSBURG ROAD
EMMITSBURG, MARYLAND 21727

301.447.5218
FAX: 301.447.5863

January 24, 2018

Dr. James Fielder, Secretary
Maryland Higher Education Commission
6 North Liberty Street, 10th floor
Baltimore, MD 21201

Dear Dr. Fielder,

I am writing to submit the enclosed proposal for a Post-Baccalaureate Certificate (PBC) program in Risk Management and Cybersecurity to be offered at Mount St. Mary's University.

The goal of the PBC is to develop risk and cybersecurity awareness across a broad spectrum of the workforce. Individuals within Computer Science and Information Technology have been the target audience for many associate, baccalaureate, and post-baccalaureate educational programs developed across the country. While a focus on increasing technology skillsets for those individuals is a valuable direction for the nation, the knowledge gap between the technical and non-technical workforces related to risk management and cybersecurity has increased. This gap is significant because individuals who are unaware of the risks associated with their individual technology decisions may inadvertently increase their vulnerability. When those decisions are part of a small business or larger corporate structure involving customers, the risk increases dramatically.

The intention of the PBC is to provide the background critical for professionals, technical and non-technical, to adapt decision-making with a risk management and cybersecurity focus. Individuals who are comfortable as users of technology frequently lack the deeper understanding beneficial for protection of critical computing and data resources. A trained workforce with risk management and cybersecurity awareness will ensure decisions made at all levels occur within a risk-centric thought process.

The proposal details the requirements and specifics of the program. Thank you for your time and consideration.

Sincerely,

Boyd Creasman, Ph.D.
Provost

Mount St. Mary's University

Proposal for a New Post-Baccalaureate Certificate Program

Risk Management and Cybersecurity for Professionals

Developed by the Department of Mathematics and Computer Science

A. Centrality to Institutional Mission and Planning Priorities

Program Description

The Department of Mathematics and Computer Science at Mount St. Mary's University proposes a Post-Baccalaureate Certificate (PBC) in Risk Management and Cybersecurity for Professionals. The goal of the PBC is to develop risk and cybersecurity awareness across a broad spectrum of the workforce. Individuals within Computer Science and Information Technology have been the target audience for many associate, baccalaureate, and post-baccalaureate educational programs developed across the country. While a focus on increasing technology skillsets for those individuals is a valuable direction for the nation, the knowledge gap between the technical and non-technical workforces related to risk management and cybersecurity has increased. This gap is significant because individuals who are unaware of the risks associated with their individual technology decisions may inadvertently increase their vulnerability. When those decisions are part of a small business or larger corporate structure involving customers, the risk increases dramatically.

The intention of the PBC is to provide the background critical for professionals, technical and non-technical, to adapt decision-making with a risk management and cybersecurity focus. Individuals who are comfortable as users of technology frequently lack the deeper understanding beneficial for protection of critical computing and data resources. A trained workforce with risk management and cybersecurity awareness will ensure decisions made at all levels occur within a risk-centric thought process. Professionals that would benefit from focused training specific to risk management and cybersecurity include among others:

- Entrepreneurs
- Small business operators
- Executive leaders

- Litigators
- Medical transcriptionists
- Healthcare providers
- Educators
- Procurement officers
- HR personnel
- Law enforcement and intelligence professionals
- Communications professionals in digital, printed, and broadcast media

According to the 2016 US Census, Frederick County, Maryland is among the fastest growing suburbs of the Baltimore-Washington metropolitan area, projected to grow 38% beyond current census by the year 2040. Employers within the county include government, research, and financial spectrums as well as many startup high-technology companies including biotechnology and cybersecurity. Additionally, many of the residents of the county are employed across an equally broad spectrum of careers within the larger Baltimore-Washington metropolitan area.

The background of PBC participants will span a broad range of disciplines including computer science, science, business and humanities. MSMU graduates with the newly-approved Entrepreneurship major will especially find that a Risk Management and Cybersecurity PBC provides a strong advantage for their future direction.

Mount St. Mary's University has the curriculum experience related to bringing technical information to a non-technical audience and has significant experience teaching cybersecurity and risk management across several disciplines. A Cybersecurity minor has been in existence since 2014, and MSMU recently began offering a Cybersecurity major along with a Forensic Accounting major. The Department of Sociology and Criminal Justice and the Bolte School of Business offer cybersecurity curriculum to students in technical and non-technical majors. Many non-computer science majors regularly enroll in introductory computer science courses to expand their knowledge base.

While certification exams and credentials are common in the technology sector for a variety of skillsets, achieving professional certification is not the designed goal of this proposed certificate program. However, aligning with the formal structure of cybersecurity certification curriculum will enable participants to choose to complete certification if credentialing aligns with their future direction. Given the high number of individuals employed within government and government-related sectors in this geographic area, alignment with a certification structure rooted in the government system provides a meaningful framework for PBC participants. The Risk Management Framework (RMF) provides this structure for federal information systems including DoD systems. Additionally, the $(ISC)^2$ (International Information Systems Security Certification Consortium, Inc) provides an early cybersecurity career certification based on RMF through the Certified Authorization Professional (CAP) certification. As such, the combined structure of the RMF and the CAP certification provide a solid foundation for the proposed PBC curriculum. Participants who successfully complete the PBC will be prepared to sit for the CAP exam. Those participants who choose not to pursue additional certification beyond the PBC garner significant risk management perspective for use in all future endeavors. This perspective will set these professionals apart from others in their chosen professions.

The PBC curriculum consists of four (4) courses, each a prerequisite for subsequent PBC courses. The first course provides a high-level perspective on the risk inherent within computer systems, and a means by which to categorize that risk based on information utilization. This course focuses on the Categorize portion of RMF with some security baseline discussion. The second course expands knowledge into security concepts at a computer-system level as standalone utilization as well as related to online activity. All six (6) RMF elements (Categorize, Select, Implement, Assess, Authorize, and Monitor) are discussed within the context of the individual computer usage in this course. Upon completion, participants will have experience with end-to-end RMF application specific to the computer setup. The third course expands on the knowledge base from the second course to consider RMF elements applied within a more complex network environment (intranet and internet). The final course is a capstone course that provides participants opportunity to demonstrate their understanding by completing an end-to-end assessment of risk within their work or personal computing environment.

Initially, the curriculum sites will involve a combination of MSMU's Emmitsburg and Frederick campus locations with integration of online elements throughout. Potential for partnerships with local employers and school systems also exists that could result in satellite locations specific to targeted audiences. Utilizing MSMU's Frederick and Emmitsburg campuses for alternating cohorts will enable the program to reach a geographically disparate population. Collaborating with employers in the geographic area will provide a risk and security savvy work force for those employers. Educating the educators will provide a trained set of individuals capable of bringing comparable knowledge to their students from elementary to middle to high school levels. Students attending part-time will be able to complete the certificate in 1-2 years.

Relationship of Proposed Program to the University's Mission

The proposed program is designed to be consistent with and to support the University's mission:

> *Mount St. Mary's is a Catholic university committed to education in the service of truth; we seek to cultivate a community of learners formed by faith, engaged in discovery, and empowered for leadership in the Church, the professions, and the world.*

As a testament to the university mission, MSMU has an established history of offering curriculum, including technology curriculum, within a structure of smaller, student-focused, class sizes, fully integrated within an ethics-focused framework. The proposed certificate program builds on this success in order to empower participants to develop skills and insights necessary to be ethical leaders within their individual professions. The focus of the curriculum is to build the skills to measure and assess risk, and to do this with full recognition of the significant individual impact that occurs when technology risk implications are ignored.

The program curriculum is based on many existing MSMU courses, thus enabling the program to inherit from the existing structure. Basing the PBC curriculum on proven material ensures alignment with the University's mission statement specific to formation of students. Participants of the certificate program will develop as risk and cybersecurity literate professionals well

prepared to function professionally and ethically within a high technology world. The capstone course provides a means for participants to demonstrate their mastery of certificate topics.

As technology solutions continue to shape the world around us, it is imperative that universities, like Mount St. Mary's University, participate in the preparation of professionals who "see and seek to resolve the problems facing humanity, and commit themselves to live as responsible citizens." Participants who successfully complete the certificate program will think intellectually as well as morally related to the utilization of technology in their career direction. The program will develop not only the technical skills specific to understanding the risk, but will challenge participants to never lose sight of the ethical implications of decisions made and potential impacts to the individuals.

Relationship to Strategic Goals

As a university community, Mount St. Mary's has been participating in a comprehensive effort to refine our mission and strategic plan. The initial revisions are on track for completion by the fall of 2017. As part of these activities, the President in conjunction with the full university community developed shared priorities for AY 2016-17. The following are excerpts from those shared priorities:

1. Improve the excellence of our educational experience by engaging the entire Mount community.
    a. Continue to improve the integration of curricular and co-curricular programs.
    b. Increase online learning courses available at both the Emmitsburg and Frederick campuses
2. Prioritize and develop the most promising areas for growth consistent with our core values as a Catholic institution of higher education.
    a. Research and develop new undergraduate and graduate programs that meet the current and future needs of students and employers

In support of these efforts, a committee established in fall of 2016 under direction of the Provost's Office was charged with identifying potential new academic programs for consideration. That committee composed of administration, faculty, and student representatives reviewed numerous proposals from faculty and selected a few representative of the desired future direction for the university. The proposed cybersecurity certificate was one of the proposals selected by the review committee as providing value in alignment with the university direction.

Additionally, as part of the larger comprehensive effort related to the mission and strategic plan, insights for relevant new programs were sought from Board members specific to their own industry experiences. Data, informatics, and related security topics were a common theme in those discussions. The certificate program as proposed is designed to provide a common thread that can be integrated into many of the new curricula regardless of a STEM or non-STEM discipline area.

B. Adequacy of Curriculum Design and Delivery

Program Requirements

Purpose

The certificate in Risk Management and Cybersecurity is designed for professionals from diverse backgrounds and disciplines to gain critical technology skills intended to augment and enhance their subject area expertise. Participants will gain the knowledge and skills necessary to contribute with a risk-focused thought process within a world that is highly dependent on technology. Participants will develop skills related to security processes, along with an ability to assess and mitigate risk within key technology areas. There are no presumed prior technology knowledge expectations.

Admission Requirements

Candidates for admission into the risk management and cybersecurity awareness PBC program must have completed a bachelor's degree and must satisfy the following criteria:

- 2.75 minimum cumulative undergraduate or graduate grade point average (GPA)
- International students must also submit a TOEFL score with their application.

Course List (4 courses, 12 credits)

Required Courses (4 courses, 12 credits)

CYBER 5XX: Introduction to Risk Management and Cybersecurity for a Digital World (3 cr.) – Students will be introduced to the study of risk assessment and cybersecurity with an in-depth development of concepts behind "cybersecurity" and "risk". Course develops understanding for the integration between computer architecture, operating systems and application programs. In-depth coverage of network concepts including common network topologies; historical and technological foundations of the Internet; risks associated with connectivity are included. Additional topics include security concepts related to computer, network, and data; role of security models and architecture in risk mitigation; security categories; common threat and vulnerability challenges; state and federal laws related to cybersecurity; basic steps to secure privacy, data, and computer; risk assessment; risk mitigation; security and risk planning.

CYBER 5XX: Technology Risk and Security for the Individual (3 cr.) – Students will gain deeper understanding of risk specific to computer hardware, operating systems, and application programs. The course focuses on risk and security concerns for the individual computer, and the elevated risks that result to computer and data when the computer accesses the Internet. Topics include authentication; logging; auditing controls; virtualization; managing and securing data and files; safe online practices; role of security certificates; email protocols; common email hacking techniques; public key encryption.

RMF (Risk Management Framework) elements covered include Categorization, Select, Implement, Assess, Authorize, and Monitor within the context of individual computers and online activity. *Prerequisite CYBER 5XX: Introduction to Risk Management and Cybersecurity for a Digital World*

CYBER 5XX: Technology Risk and Security for Networked Computers (3 cr.) – Students will gain deeper understanding of risk specific to inter- and intra-networking of individual computer systems. The course focuses on risk and security related to small networks, and the connection of those networks to the broader Internet. Concepts covered include switches and routers; basics of IP addressing and subnets; DNS servers; firewalls; authentication and authorization; basic secure network configuration and systems administration; managing data; disaster recovery; backup recovery; change and configuration management practices. RMF (Risk Management Framework) elements covered include Categorization, Select, Implement, Assess, Authorize, and Monitor within context of networked computers including connections to Internet. *Prerequisite CYBER 5XX: Technology Risk and Security for the Individual*

CYBER 5XX: Risk Management and Cybersecurity Capstone (3 cr.) – This course is a culmination of the Risk Management and Cybersecurity for Professionals sequence enabling the student to demonstrate skills learned within a project area of interest for their future or current direction. All project proposals are reviewed by a faculty panel prior to project initiation. Final project completion is reviewed and approved by a faculty panel for successful completion. *Prerequisite CYBER 5XX: Technology Risk and Security for Networked Computers*

Educational Objectives and Student Learning Outcomes

The PBC in Risk Management and Cybersecurity is designed to provide key technology, network and data knowledge for professionals to adapt security focus in their individual and company practices. Completion of the certificate will provide students with:

- A detailed understanding of the risks within individual computers, networked computers, and the Internet
- Working knowledge of key technology skills commonly utilized within individual, enterprise and Internet security
- Detailed knowledge of security practices with high potential to improve safe practices within an organization or related to online activity
- Hands-on experience assessing and managing technology risk
- An ethical foundation to be leveraged in decision-making that involves implementation of technology whether stand-alone or on the Internet

Discuss how general education requirements will be met, if applicable.

Not applicable.

Specialized accreditation or graduate certification requirements

Not applicable

Contracting with another institution or organization

Not applicable.

C. Critical and compelling need as identified in the 2013 State Plan

The proposed certificate is aligned with many of the goals stated in the Maryland Ready 2013-2017 Maryland State Plan for Post-Secondary Education. Specific goals are identified and aligned with the certificate program objectives below.

- Quality and Effectiveness Goal:

  As part of the overall curriculum of Mount St. Mary's University, the certificate program will garner the same benefits as the overall university curriculum in terms of assessment processes, and faculty professional development funding. The program will be continuously assessed and evaluated against formal plans to ensure the courses and program align with learning goals and objectives, and with the mission of the university. Those results will be used to provide constant improvement to the material and delivery mechanisms leveraged.

  The faculty focused on delivering courses within this certificate are full-time members of the faculty, have significant experience teaching in the subject areas, and for several, bring industry experiences to their students as well.

  As a combination of hybrid and online delivery, this program will follow the successful approaches of similar delivery across the Mount curriculum. Mount St. Mary's has made a concerted effort to collaborate across the faculty related to successful online and hybrid delivery practices and approaches. A faculty committee is in place to oversee those guidelines in collaboration with the School of Education resources.

- Access, Affordability and Completion Goal:

  The primary participants in this certificate program are anticipated to be adult learners who are attempting to augment their current career path with relevant technology skills. Small business owners and entrepreneurs who complete the PBC will have a marketing tool to separate themselves from competition specific to risk and online security awareness. The design of the courses with a hybrid and online focus is intended to minimize impact to the busy lives of participants by providing a flexible delivery mechanism to the maximum extent possible. This follows the success models across current MSMU graduate programs related to evening courses and the flexibility of online/hybrid delivery.

Additionally, it is understood that many of the certificate participants will come into the program with minimal advanced experience in technology and security practices. No assumptions related to readiness within the subject area is assumed, which deviates from other programs regionally as well as many online curriculum. The program is designed to build these skills for all participants regardless of previous experiences.

Exposure to current security and risk practices for individual, networked, and online computer technology will be an integral part of the full educational experience within the program. As much of the technology industry relies heavily on open source technology, the intent of the program will be to leverage comparable open source technology as much as possible including Cloud web service capabilities. This will enable participants to gain experience with specific toolsets while also keeping participant costs manageable.

Affordability is a key element for successful recruitment of certificate participants. While Cybersecurity advanced curriculum is readily available in the state of Maryland, the focus of those programs is on advanced training for technology professionals. Program costs for these programs are reflected below as a basis for comparison. In section E, a side-by-side comparison is provided specific to curriculum. Additionally, the total cost for certificate completion has been included below.

Inst.	Graduate Program	$ Per Credit Hour	$ Per Course (3 Cr.)	Cost of Completed Certificate
MSMU	Science – Graduate Level	$635	$1905	4 courses, total $7620
Hood	Cybersecurity Certificate	$500	$1500	5 courses, total $6000
UMUC	Cybersecurity Management and Policy Graduate Certificate	$694; courses 6 credits each	$4164	3 courses, total $12,492
UMD	Cybersecurity Certificate in Department of Engineering	$932	$2796	4 courses; total $11,184
UMBC	Graduate Certificate in Professional Studies: Cybersecurity Strategy and Policy	$753 in-state; $1179 out of state	$2259	4 courses; $9036
UMBC	Graduate Certificate in Professional Studies: Cybersecurity Operations	$753 in-state; $1179 out of state	$2259	4 courses; $9036
Loyola University of Maryland	Managerial Approach to Cybersecurity Certificate	$950	$2850	5 courses, total $14,250
Johns Hopkins	PMC Engineering for Professionals: Cybersecurity	Per course tuition	$4055	PMC 6 courses, total $24,330
Johns Hopkins	PBC: Science, Technology, International Security	Per course tuition	$3673	PBC 5 courses, total $18,365
Towson University	Cybersecurity Specialist (undergraduate level)	N/A	N/A	N/A

- Innovation Goal:

  The strength of this proposed certificate is its innovative nature. Traditionally, cybersecurity skills are taught to individuals with existing computer science and information technology skills. The target participants for this PBC program are not this group of high technology professionals, but rather individuals who in interest of advancing careers or business interests seek knowledge related to risk management and cybersecurity awareness. For these individuals, the gap to be bridged to anticipate future careers that heavily rely on technology can be daunting. Certificate and graduate programs require substantial training and expertise in the technology field. The program is designed to provide skills the non-technical participants need.

  Additionally, leveraging a combination of online/hybrid structure in conjunction with current faculty and course curriculum ensures delivery of a proven framework in a format desirable for our target participants. Online certificates in cybersecurity can be found through universities throughout the United States; online education has become more mainstream. Many of these programs however have significant prerequisite requirements related to computer architecture, networking, computer programming and mathematical maturity levels. Participants in these programs often have fairly advanced technology skills as well. The innovative approach with this program is to leverage instructor-led online elements in conjunction with classroom experiences that enable individuals with primarily user-centric technology skillsets to develop sufficient technology skills to be fully successful in an online technology environment.

  The technology skills taught within PBC are highly desirable skills in the marketplace today including among technical employees. Participants who successfully complete the certificate program will have knowledge sufficient to participate in risk assessment planning/oversight in conjunction with technology professionals. Participants will learn how to continue learning within the subject area by continually leveraging online resources integrated throughout the course curriculum.

- Economic Growth and Vitality Goal:

  As highlighted in the State Plan,

  > *"...students...must have access to high-caliber and effective training that meets the evolving needs of the workplace..."*
  >
  > *"Science, technology, engineering, and mathematics (STEM) occupations have been identified as an area of high need in Maryland..."*

  The Mathematics and Computer Science department and the School of Natural Science and Mathematics at MSMU have a long-standing history of placement of graduates with top STEM employers in the region. Within the last three years, MSMU Mathematics and Computer Science graduates have been employed by Northrup

Grumman, Raytheon, Lockheed Martin, Johns Hopkins Advanced Physics Laboratory, Patuxent River Naval Air Station, NSA, SAIC, and Booz Allen Hamilton among many others. The proposed certification program will benefit from the existing advisory boards as some individuals seek opportunity for more advanced cybersecurity training and employment by building on the PBC foundation. Basing the foundational courses on the existing Cybersecurity minor and major courses ensures that many of the same high-demand cybersecurity skills MSMU graduates obtain are also obtained by the certificate participants.

With the prevalence of technology and data utilization across all disciplines, the demand for risk and cybersecurity literate professionals extends beyond the traditional computational STEM career paths. The goal of this certificate program is to provide a foundation in STEM concepts to certificate program participants regardless of prior technology background. As the target participants will be from diverse discipline backgrounds, the program leverages comparable advisory relationships beyond the School of Natural Science and Mathematics to include the College of Liberal Arts, the Bolte School of Business, and the full university structure.

Each course within the program curriculum builds on previous courses in order to establish the knowledge and confidence of security details from the computer to network to internet. Utilizing a capstone format, participants will also have opportunity to create a portfolio that can be shared for professional advancement as well as with prospective future clients related to the level of knowledge within risk and cybersecurity practices.

D. Quantifiable Evidence of Market Supply & Demand

In a May 2017 article, the Harvard Business Review discussed the widening gap in filling cybersecurity roles, and the individuals trained to fill those roles. This resource availability gap continues to widen despite a focus across the country on expanding cybersecurity curricula. The article additionally references a report from Frost & Sullivan and the $(ISC)^2$, the International Information Systems Security Certification Consortium, Inc, related to the global cybersecurity workforce. An estimated 1.5 million positions will be unfilled by the year 2020 while the security industry is expected to grow to $101 billion of opportunity in that same timeframe. The article conjectures a primary reason for the gap is that businesses as well as college degree programs have focused on training individuals with prior technology expertise. An alternative thought process is raised to consider addressing this widening gap with individuals from non-technical disciplines, as not all cybersecurity roles require the same level of technical training.

IBM has begun to create "new collar" jobs with cybersecurity as a focus area. The intent is to teach the skills needed to enable individuals from a variety of backgrounds to get initial positions, and then continue to develop their training as they progress into more technical roles with time and experience. Focus is to identify individuals with the right thought process and ethics driven background as a foundation. Inside Counsel in a 2015 article highlighted the

"market advantage" that litigators with cybersecurity expertise could garner. These articles demonstrate the need for a change in thought process across the country related to the target audience for risk and cybersecurity related training.

Cybersecurity experts continually highlight that the primary vulnerability with all cybersecurity risk planning and mitigation remains the people within the enterprise. Articles abound supporting this viewpoint including Harvard Business Review in September 2016, and Forbes Magazine in May 2016. In a TripWire white paper, a survey of C-level executives (CEO, CIO, CTO, CSO, etc) indicates that many feel "outside their comfort zone when it comes to decisions on cybersecurity risk". These executives also indicated low confidence that "cybersecurity briefings presented to the board accurately represented the urgency and intensity of cyber threats targeting their organizations".

Frederick County is the third fastest growing county in Maryland with a .9% increase in population from July 2015 to July 2016. With its location equi-distant to the Washington as well as the Baltimore metropolitan areas, the county has many professionals working in those regions across a broad spectrum of careers. Government is a big presence in both metropolitan areas, and a large employer of residents within Frederick County. Mount St. Mary's University is well positioned with a Frederick and Emmitsburg campus to reach the non-traditional adult students within the Frederick County communities. Additionally, government locations like FEMA in Emmitsburg, and Ft. Detrick in Frederick are local employers with heavy reliance on data as well as risk and cybersecurity-literate professionals.

According to the Frederick County Office of Economic Development, 98% of companies in Frederick County are small businesses with less than 100 employees. These companies have critical need to leverage technology for marketing, for product delivery, for customer contacts, for tracking customer data, for payroll and human resource functions, among many other needs. Individuals running these companies frequently do not have the budget to hire the top cybersecurity experts, and instead need to rely on their own ability to make prudent decisions. Small business owners and key employees within these companies are the largest target audience specific to this proposed PBC program.

Educational and Training Needs

Focus in most educational institutions has been on providing the highly technical training required for cybersecurity professionals. With people as the largest security vulnerability, and with the significant number of non-technical employees within the workforce, a need clearly exists for training specifically within this non-technical sector. These positions do not require the level of knowledge that cybersecurity professionals require in the intricacies of defining and establishing an enterprise-level security architecture. Instead, these positions need sufficient understanding of the risks, how to assess the risks, and mitigation steps that can alleviate existing cybersecurity threats.

The proposed PBC addresses these gaps. Program participants receive a level of training in the technology skills critical to prepare them as a valuable employment asset within their segment of the workforce. As explained in more detail in section E below, there are no comparable

certificate programs within Maryland. The majority of programs that exist focus on the advanced technical expertise, or at the management level knowledge. The focus is not on the individuals who have responsibility for the smaller companies, or the full end-end accountability.

According to a combination of U.S. Census Bureau data as well as Maryland Report Card data, Frederick County has a 92% high school graduation rate; second in the state of Maryland behind Howard County at 95%. Thirty-nine (39) % of residents have a bachelor's degree or higher; third in the state of Maryland. Of Frederick County high school graduates, 76.7% enroll in college within 24 months of high school graduation; 71% of the population age 16 or older are in the civilian work force. Data support the focus that career education and advancement represent to Frederick County residents. Web sources referenced include 2016 Maryland Report Card and TownCharts.

Estimating potential student populations is difficult as Risk Management and Cybersecurity programs in alignment to this proposal are not common at this time, and enrollment numbers are not easily obtained as a basis for comparison. Census data indicates that by the year 2020, Frederick County will have 67,351 individuals in the non-traditional college age bracket (age 25-44). Applying the percent of residents with college degree against this population, we obtain 26,267 individuals in Frederick County with educational background to participate in certificate program. The program aims to enroll 30 students in initial courses representing .1% of the total number of eligible individuals.

We also anticipate internal demand for this certificate program related to current graduate students across the MSMU curriculum; a population of 341 graduate students is currently enrolled.

E. Reasonableness of Program Duplication

A search of the Maryland Higher Education Commission site indicates there are several post-baccalaureate certificate programs in Cybersecurity, and one post-masters certificate. Program requirements for each are summarized in the table below.

The UMBC Graduate Certificate in Professional Studies: Cybersecurity Operations and the Johns Hopkins PBC are the closest in alignment to the proposed program. Prerequisites for the UMBC certificate program involve technical expertise and knowledge. Focus for the Johns Hopkins PBC is preparation for technical roles.

Specific to the western Maryland area with Frederick County, there is no duplication of program. While Hood College has a Cybersecurity PBC, that certificate program has technical prerequisites that the proposed MSMU PBC program does not. No programs target non-technical individuals related to risk and cybersecurity awareness training without requiring some level of technical expertise expectations.

The table below compares the proposed MSMU PBC curriculum to existing cybersecurity PBC certificate programs within the state of Maryland. This table highlights the differences related to

target audience and prerequisite requirements as well as overall requirements to complete certificate.

Inst.	Graduate Program	Post-Baccalaureate Certificate Option	Program Comparison	Certificate Course Requirements
MSMU	Science – Graduate Level	Proposed	Bachelor's degree in any discipline, no programming, network, or security prerequisites	1) Introduction to Risk Management and Cybersecurity in a Digital World 2) Technology Risk and Security for the Individual Professional 3) Technology Risk and Security for Networked Computers 4) Risk Management and Cybersecurity Capstone Focus on preparing individual for $(ISC)^2$ CAP (Certified Authorization Personnel) certification aligning with DoD Risk Management Framework
Hood	Cybersecurity Certificate	Yes	Solid background in computer science or information technology, including database and telecommunications concepts, either through formal study or professional experience	5 courses with focus on preparing individual for $(ISC)^2$ CISSP (Certification Information Systems Security Professional) certification. This certification requires 5 years of practical experience related to cybersecurity
UMUC	Cybersecurity Management and Policy Graduate Certificate	Yes	Designed for midcareer professionals or those new to field. Recommended background in computing/programming with options to address skills gaps in preparation for program.	3 6-credit courses with focus on preparing participants to pursue positions managing cybersecurity functions
UMD	Cybersecurity Certificate in Department of Engineering	Yes	Provides full admission for individuals with engineering, computer science, applied mathematics, physics backgrounds, or provisional admission for individuals from related major such as information systems along with existing IT or cyber certification.	4 courses including potentially Secure Programming in C, an advanced programming concept
UMBC	Graduate Certificate in Professional Studies: Cybersecurity Strategy and Policy	Yes	Understand basic concepts and operation of the Internet, networked information systems, and have a basic familiarity with information security	4 courses which provide participants with advanced knowledge of strategy, policy, analytic aspects of cybersecurity, enabling them to fill critical roles in operational cybersecurity missions

			concepts and/or practices. Can satisfy requirements with courses or documented professional experience.	
UMBC	Graduate Certificate in Professional Studies: Cybersecurity Operations	Yes	Understand basic concepts and operation of the Internet, networked information systems, and have a basic familiarity with information security concepts and/or practices. Can satisfy requirements with courses or documented professional experience.	4 courses which provide participants broad exposure to cybersecurity principles, best practices, and technologies
Loyola University of Maryland	Managerial Approach to Cybersecurity Certificate	Yes but not currently accepting applications	Quantitative background	5 courses; strategy, policy, and planning focus
Johns Hopkins	PMC Engineering for Professionals: Cybersecurity	No, PMC	N/A	N/A
Johns Hopkins	PBC: Science, Technology, International Security	Yes	No stated prerequisites that would prevent non-technical from applying	5 courses; 3 CORE and 2 elective selected from long list of options Focus on developing participants for roles in science and technology related to national or international security
Towson University	Cybersecurity Specialist (undergraduate level)	Bachelors level certification for industry certification exams	N/A	N/A

F. Relevance to Historically Black Institutions (HBIs)

1. Potential impact on high-demand programs at HBI's

Not applicable. The proposed program does not duplicate or compete with programs at any of the regional HBIs.

2. Potential impact on the uniqueness and missions of HBIs

Not applicable. The proposed program does not duplicate or compete with programs at any of the regional HBIs.

G. Evidence of the Principles of Good Practice for Online Programs

Not applicable.

H. Adequacy of Faculty Resources

The Cybersecurity certificate program will be housed administratively within the Mathematics and Computer Science Department. The faculty who will teach foundational courses in the program will come primarily from that department, with potential augmentation from Criminal Justice and Forensic Accounting. These faculty have already demonstrated their ability to teach computer science and cybersecurity concepts within the curriculum. A computer scientist, with graduate degree and cybersecurity experience, will be hired to provide additional knowledge and expertise related to this program going forward.

The majority of the faculty listed below have terminal degrees in their field and all are full-time members of the university faculty.

Cybersecurity Certificate Courses

Athar Rafiq – Mr. Rafiq has many years' experience with enterprise-level security implementations, risk assessment and cybersecurity mitigation, and IT project management as the head of a successful Cybersecurity consulting practice. Prior to joining Mount St. Mary's University, Prof. Rafiq was the lead in upgrading Howard Community College Cybersecurity teaching and laboratory systems and equipment. Prof. Rafiq teaches across the Cybersecurity curricula.

Brian Heinold, Ph.D. in Mathematics – Dr. Heinold has taught across the Mathematics, Computer Science and Cybersecurity curricula [Associate Professor Mathematics and Computer Science, Full-time]

Frederick J. Portier, Ph.D. in Mathematics– Dr. Portier has taught across the Mathematics, Computer Science and Cybersecurity curricula including Windows/Linux Operating Systems, and Operating Systems Design [Professor Mathematics and Computer Science; Full-time]

Scott Weiss, M.S. in Computer Science– Mr. Weiss has taught across the Computer Science curricula including Operating Systems, Computer Architecture, Computer and Network Security [Assistant Professor Computer Science, Full-time]

Rebecca Portier, M.S. in Computational Mathematics – Ms. Portier has many years' experience with enterprise-level application systems, risk assessment and mitigation as a technology manager with Wells Fargo and Chevy Chase Bank. Prof. Portier teaches across the Computer Science curricula. [Assistant Professor Computer Science, Full-time]

I. Adequacy of Library Resources

Mount St. Mary's University's Hugh J. Phillips Library currently contains about 200,000 bound volumes and a rapidly expanding collection of scholarly information databases that provide convenient access to e-books, journal articles and a variety of data sources. Included in our e-library are more than 25,000 professional and scholarly journal publications that are carefully chosen to support each of the University's academic programs.

The library has an excellent E-resources collection that includes discipline specific databases including the complete JSTOR back files. Content from Sage, EBSCO, ProQuest, Duke e-journals, ATLA and many others is available from the library's website http://libguides.msmary.edu/phillipslibrary. The library recently implemented the *EBSCO Discovery Service* that performs a single search of all library resources from one search interface. Computer Science, Applied Mathematics, Statistics, and many discipline specific subscriptions are currently available. Requests for additional resources can be made each year.

Our library staff includes four faculty librarians who provide research assistance and information literacy instruction to individuals and groups. A faculty librarian with theological training maintains the theology collection of approximately 46,000 volumes. Our main desk services, resource acquisitions, cataloging and interlibrary loans are provided by four student/faculty-focused employees, with the help of several dedicated student assistants.

The Phillips Library is a founding member of the Maryland Interlibrary Consortium and collaborates with Hood College, Baltimore International College, Washington Adventist University (formerly Columbia Union College), Loyola College-Notre Dame University Library, and Stevenson University. Through this consortium, Mount students and faculty have direct access to the collections of each member library through electronic and physical delivery services. The average delivery time for print materials is within 24hours.

Table 1. 2015-16 Library Expenditures	
Volumes	149,287
Per FTE student	72
Journal Titles-Paper	233
Journal Titles-Digital	26,544
Librarian Research Transactions	1.068
Participation in Instruction Services	1,210
Databases	130
Videos	1,500
Total Library Expenditures	$862,061
Library expenditures per FTE student	$ 413

Source: Mount St. Mary's Factbook 2017

J. Adequacy of Facilities, Infrastructure and Instructional Equipment

The Risk Management and Cybersecurity for Professionals PBC will be offered through MSMU's Emmitsburg and Frederick Campus locations. As part of the Mathematics and Computer Science department, the certificate program will have access to the Coad Science Building facilities utilized by the program. Coad is a 48,000 ft^2 building that holds classrooms, faculty and staff offices, specialized laboratories, a vivarium, a computer lab, and a greenhouse. Existing computer laboratory space was recently renovated to expand utilization for the new Cybersecurity major. Those renovations were completed with cybersecurity, data science, computer science and mathematics needs in mind, and will provide access to servers for any custom software or data access needs by the program.

The Frederick Campus is a 25,000 ft^2 facility with classrooms, offices, large conference room, two dining areas, chapel, and kitchen. The facility has some unused capacity in terms of classroom space so it will support the 1-2 additional courses per term that the PBC program will introduce. Although it is a technical program, laboratory facilities are not needed at this site. Faculty instructors have access to the full resources of the facility including photocopiers, scanners, audio-visual equipment, phones, and office supplies. Administrative assistants provide administrative support and faculty also may avail themselves of the resources of the MSMU Career Center, Learning Services, Information Technology Support Center, and Health and Wellness Center.

Numerous online resources are available and will be leveraged throughout the curriculum. Participants will be expected to provide their own computer. Any software or technology tools leveraged will be predominately open source.

In summary, this program can be offered with existing institutional facilities, infrastructure, and instructional equipment.

K. Adequacy of Financial Resources

TABLE 2: RESOURCES					
Resources Categories	**Year 1 (2017-2018)**	**Year 2 (2018-2019)**	**Year 3 (2019-2020)**	**Year 4 (2020-2021)**	**Year 5 (2021-2022)**
1. Reallocated Funds	$0	$0	$0	$0	$0
2. Tuition/Fee Revenue **(c+g)**	$0	$109,872	$161,760	$224,856	$257,400
a. # F.T. Students					
b. Annual Tuition/ Fee Rate (Discounted rate)					
c. Annual Full Time Revenue **(a x b)**					
d. # Part Time Students	0	14	20	27	30
e. Credit Hour Rate	$635	$654	$674	$694	$715
f. Annual Credit Hours	0	12	12	12	12

g. Total Part Time Revenue **(d x e x f)**	$0	$109,872	$161,760	$224,856	$257,400
3. Grants, Contracts, & Other External Sources					
4. Other Sources					
TOTAL (Add 1-4)	**$0**	**$109,872**	**$161,760**	**$224,856**	**$257,400**

Academic year 2017-2018 will be primarily a year of preparation because we will not have time to recruit students. After a strong recruiting and marketing effort in 2017-18, we expect to admit a first cohort of 14 students in the fall of 2018. We expect to grow by about 40% after the first cohort, and leveling off at about 30 students.

Credit Hour Rate: The rate for 2016-17 is $635 per credit. We project an increment of 3% per year which is a typical amount of increase at MSMU.

Total Resources: The resources available are projected to be $0 in year 1, increasing to $257,400 in year 5.

TABLE 3: EXPENDITURES					
Expenditure Categories	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**
1. Faculty **(b+c below)**	0	$113,900	$116,178	$118,502	$121,485
a. # FTE	0	1	1	1	1
b. Total Salary	$0	$85,000	$86,700	$88,434	$90,203
c. Total Benefits	$0	$28,900	$29,478	$30,068	$31,282
2. Admin. Staff **(b+c below)**					
a. # FTE					
b. Total Salary					
c. Total Benefits					
3. Support Staff **(b+c below)**	$3,350	$3,417	$3,485	$3,555	$3,626
a. # FTE	0.05	0.05	0.05	0.05	0.05
b. Total Salary	$2,500	$2,550	$2,601	$2,653	$2,706
c. Total Benefits	$850	$867	$884	$902	$920
4. Equipment					
5. Library		$2000	$2100	$2200	$2300
6. New or Renovated Space					
7. Other Expenses (see Table 3)	$10,200	$9,700	$9,700	$9,700	$9,700
8. TOTAL (Add 1 – 7)	**$13,550**	**$129,017**	**$131,463**	**$133,957**	**$137,111**

Faculty: By AY2018-2019, we will hire a full-time, tenure-track faculty member in computer science with cybersecurity experience to assist in teaching courses along with courses in support of existing computer science programs. This will result in a full teaching load (21 credits per year). The range of median salaries cybersecurity engineers is $60,199 - $133,795 (Payscale; Bureau of Labor Statistics). The national average for Asst. Professor Computer Science faculty (first-year) is $84,281 (Inside Higher Ed). In order to be able to attract and retain an experienced individual in this field a

salary of $85,000 is recommended. A portion of time has been allotted in AY2017-2018 for current faculty to begin development of curriculum in preparation for course offerings in fall of 2018.

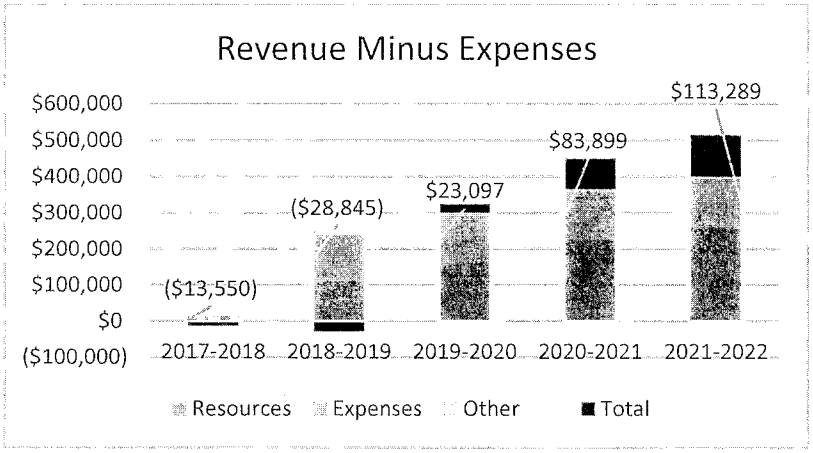
Support Staff: We estimate a time commitment equivalent to 5% of a person's workload in the Communications Office for marketing and promotion. A salary of $50,000 was assumed and benefits are 34% of the salary. The salary was incremented by 2% per year.

Library: To purchase some additional journal subscriptions, $2,000/year should be added to the Library budget. This amount was incremented by 5%/year to account for inflation.

Other Expenses: See table 3 below.

TABLE 3: OTHER EXPENSES					
Promotional items	$1,000	$500	$500	$500	$500
Printed brochures/flyers	$200	$200	$200	$200	$200
Advertising/Marketing expenses	$5,000	$3,000	$500	$300	$300
Faculty development		$2,000	$2,000	$2,000	$2,000
Memberships	$1,500	$1,500	$1,500	$1,500	$1,500
Conferences/travel	$1,500	$1,500	$1,500	$1,500	$1,500
Networking/outreach	$1,000	$1,000	$1,000	$1,000	$1,000
Subtotal	**$10,200**	**$9,700**	**$7,200**	**$7,000**	**$7,000**

The "Other Expenses" include operating expenses for the program such as promotional items (pens, lanyards, etc.), printed brochures, and marketing and advertising (such as online advertising). Funds will be available for faculty development (e.g., travel to conferences) so that they will remain up-to-date on current practices. Department will obtain membership in relevant societies and will have funds for traveling to conferences. Finally, funds for networking and outreach will enhance recruitment.



Budget Summary: In the first 2 years of the program, the program runs at a loss while marketing and building full cohort. In year 3, there is a profit, while revenue far exceeds expense in all subsequent years.

L. Adequacy of Provisions for Evaluation of Program

The program will leverage significant curriculum from the existing cybersecurity major and minor in order to tailor curriculum for the graduate certificate. The program will be part of the Middle States Accreditation of the university. Course evaluations will be completed for each course as designated by the College/School in which the course resides and the university. Full-time faculty are reviewed at least every five years. Part-time faculty are reviewed on a course/semester basis. Each program is reviewed every five years, using an outside consultant. The following table details department Learning Outcomes to be assessed at least once in a five-year period.

Learning Outcome	Assessment	Benchmark	Timing
LO1: demonstrate an understanding of the basic concepts of risk management and cybersecurity	Department-designed cybersecurity exam	TBD	Every spring in Capstone
LO2: have the ability to apply the concepts of risk management and cybersecurity to effectively assess risk for individual and network computer setup	Rubric assessment of projects within capstone	TBD	Every spring in Capstone
LO3: have the ability to communicate technical ideas from cybersecurity with precision and clarity	Rubric assessment of communication	TBD	Every spring in Capstone
LO4: understand the legal context and the ethical issues that constitute the cybersecurity profession so that they are prepared for success	One and five-year surveys of alumni	TBD	Every spring

M. Consistency with the State's minority student achievement goals

The Risk Management and Cybersecurity for Professionals certificate program at MSMU will be promoted along with other graduate programs in SNSM. In 2015-16, the proportion of students of color was 20% in the graduate programs and 30% in the undergraduate programs. Our commitment to diversity is evidenced by a recent S-STEM award from the National Science Foundation that provides scholarship funding for underrepresented students in STEM majors with high financial need.

Nondiscrimination Statement
It is the policy of Mount St. Mary's University not to discriminate on the basis of race, color, national or ethnic origin, political or religious opinion or affiliation, age, sex or handicapping condition in the recruitment or admissions of students, or in the administration of the university's educational policies, admissions policies, scholarship and athletic programs, and other university-administered activities and programs.

Center for Student Diversity
The Center for Student Diversity was established to aid Mount St. Mary's University in its efforts of fostering inclusion, collaboration, and relationship building across campus. The Center provides academic, social, and transitional support in addition to programming, leadership training and inclusive workshops for ALL students and promotes exchange and dialogue between individuals of diverse backgrounds.

The Center for Student Diversity oversees the intercultural development programs, the Horning Fellowship, student support programs (including Third Century Scholars program and the American Indian program), and cultural programs. The office also supports cultural organizations, conducts diversity awareness programs, assesses the needs and climate of diverse groups and advocates on behalf of underrepresented students.

N. Relationship to low productivity programs identified by the Commission

Not applicable. There are no identified low productivity programs at MSMU.

Addendum

Risk Management and Cybersecurity Tables

K. Adequacy of Financial Resources

TABLE 2: RESOURCES					
Resources Categories	**Year 1 (2017-2018)**	**Year 2 (2018-2019)**	**Year 3 (2019-2020)**	**Year 4 (2020-2021)**	**Year 5 (2021-2022)**
1. Reallocated Funds	$47,720	$24,602	$0	$0	$0
2. Tuition/Fee Revenue **(c+g)**	$0	$117,720	$161,760	$208,200	$321,750
a. # F.T. Students	$0	$0	$0	$0	$0
b. Annual Tuition/ Fee Rate (Discounted rate)	$0	$0	$0	$0	$0
c. Annual Full Time Revenue **(a x b)**	$0	$0	$0	$0	$0
d. # Part Time Students	0	12	16	24	30
e. Credit Hour Rate	$635	$654	$674	$694	$715
f. Annual Credit Hours	0	15	15	15	15
g. Total Part Time Revenue **(d x e x f)**	$0	$117,720	$161,760	$249,840	$321,750
3. Grants, Contracts, & Other External Sources	$0	$0	$0	$0	$0
4. Other Sources	$0	$0	$0	$0	$0
TOTAL (Add 1-4)	**$47,720**	**$142,322**	**$161,760**	**$208,200**	**$321,750**

Academic year 2017-2018 will be primarily a year of preparation because we will not have time to recruit students. After a strong recruiting and marketing effort in 2017-18, we expect to admit a first cohort of 12 students in the spring of 2019. We expect to grow by about 30% after the first cohort, and 50% in subsequent years, leveling off at about 30 students.

Reallocated Funds: Funds will be reallocated in the first year to support current faculty in development of the curriculum, and to cover marketing expenses related to program initiation. Reallocation at a lower level for the second year, and no additional reallocation needed beyond the second year.

Credit Hour Rate: The rate for 2016-17 is $635 per credit. We project an increment of 3% per year which is a typical amount of increase at MSMU.

Total Resources: The resources available are projected to be $24,120 in year 1, increasing to $294,233 in year 5.

TABLE 3: EXPENDITURES					
Expenditure Categories	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**
1. Faculty **(b+c below)**	$34,170	$113,900	$116,178	$118,502	$121,485
a. # FTE	.3	1	1	1	1
b. Total Salary	$25,500	$85,000	$86,700	$88,434	$90,203
c. Total Benefits	$8,670	$28,900	$29,478	$30,068	$31,282
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)**	$3,350	$3,417	$3,485	$3,555	$3,626
a. # FTE	0.05	0.05	0.05	0.05	0.05
b. Total Salary	$2,500	$2,550	$2,601	$2,653	$2,706
c. Total Benefits	$850	$867	$884	$902	$920
4. Equipment	$0	$0	$0	$0	$0
5. Library		$2000	$2100	$2200	$2300
6. New or Renovated Space	$0	$0	$0	$0	$0
7. Other Expenses (see Table 3)	$10,200	$9,700	$9,700	$9,700	$9,700
8. TOTAL (Add 1 – 7)	**$47,720**	**$129,017**	**$131,463**	**$133,957**	**$137,111**

Faculty: By AY2018-2019, we will hire a full-time, tenure-track faculty member in computer science with cybersecurity experience to assist in teaching courses along with courses in support of existing computer science programs. This will result in a full teaching load (21 credits per year). The range of median salaries cybersecurity engineers is $60,199 - $133,795 (Payscale; Bureau of Labor Statistics). The national average for Asst. Professor Computer Science faculty (first-year) is $84,281 (Inside Higher Ed). In order to be able to attract and retain an experienced individual in this field a salary of $85,000 is recommended. A portion of time has been allotted in AY2017-2018 for current faculty to begin development of curriculum in preparation for course offerings in spring of 2019.

Support Staff: We estimate a time commitment equivalent to 5% of a person's workload in the Communications Office for marketing and promotion. A salary of $50,000 was assumed and benefits are 34% of the salary. The salary was incremented by 2% per year.

Library: To purchase some additional journal subscriptions, $2,000/year should be added to the Library budget. This amount was incremented by 5%/year to account for inflation.

Other Expenses: See table 3 below.