MOUNT
ST. MARY'S
UNIVERSITY

Academic Program Proposal

for a

BACHELOR OF SCIENCE IN CYBERSECURITY

Revision 2

2 August 2016

Developed by the Cybersecurity Committee:

Melanie Butler (co-chair), Virginia McGovern (co-chair), Barbara Palmer, Jeffrey Simmons, Brian Heinold, Timothy Stanton, Simon Y. Blackwell, David King, David Scibelli

Approved by the Faculty on 28 April 2016

A. ***Centrality to institutional mission statement and planning priorities:***

   1. *Provide a description of the program, including each area of concentration, and how it relates to the institution's approved mission.*
   2. *Explain how the proposed program supports the institution's strategic goals and provide evidence that affirms it is an institutional priority.*

The planned major in Cybersecurity will include existing Computer Science courses, new Computer Science courses, new Cybersecurity courses, and electives from Criminal Justice, Business, Mathematics, and Forensic Accounting. This major seeks to foster the development of graduates well-skilled in the analytical, practical, and ethical issues associated with internet technology.

Our mission statement enjoins us in the formation of students who "undertake free and rigorous inquiry" in a manner that prepares them for engagement in the world around them. Consonant with this, it is a mission that prepares our students to "see and seek to resolve the problems facing humanity, and [to] commit themselves to live as responsible citizens." The BS in Cybersecurity, in concert with the core curriculum, helps fulfill the undergraduate mission of the university by preparing students for challenging and meaningful careers that aid in the cyber defense of this and other nations. In particular, the cybersecurity program will develop strong skills in quantitative reasoning, logic, problem-solving, and design along with versatile communication skills and the ability to apply an ethical lens to a broad spectrum of information technology issues. The particular emphasis of this program is on Cybersecurity at the programming and operating systems level, while also stressing communication and ethics. The program will contribute to the undergraduate mission of the Mount by encouraging students to think intellectually and morally about access to information and responsible use of internet technology. In addition, students will develop the technical skills to help protect the dignity of all individuals who use internet technology. In this way, students will be working to solve real-world issues and dilemmas.

To develop the courses for the major, a committee held several phone conferences with a diverse group of people working in industry in Cybersecurity. Email feedback from this industry group on an initial proposal was used to make further modifications to the major. In addition, there are many possible certifications and designations in the field. Content in each required course in the proposed major was mapped to several of these programs. In particular, the Cybersecurity major was designed to help prepare students for the Global Information Assurance Certification Security Leadership Certificate (GIAC SLP). The major was also designed by mapping content to the CompTIA Security+ certification and the Center for Academic Excellence in Cyber Operations Core Knowledge Units and Optional Knowledge Units.

Those consulting on the new major repeatedly emphasized the need for Cybersecurity graduates to have strong communication skills and ethics background. For this reason, the Mount is in an especially unique position to offer this major and to help solve the overwhelming issues in the Cybersecurity field. Communication and ethics are emphasized throughout our core program, so the core and the major complement each other in a very important way. In fact, this complementarity is integral to the field, will set our program apart from other degrees, and calls us to help fill this need. Furthermore, the required major courses will incorporate communication and ethics throughout and especially in the writing-intensive and capstone requirements. The required senior-year capstone course will build on the *Veritas* core ethics course that students take in the junior year. In this way, the proposed major contributes to Priority 1, Initiative 1: The University will strengthen formation in Catholic mission (2013-15 Strategic Plan).

The new major differs from the existing program in Computer Science by requiring students to take practical courses on network administration, Windows and UNIX operating systems, and other new Cybersecurity courses, including a capstone. In addition, the Cybersecurity major allows students to take electives from Criminal Justice, Business, Mathematics, Data Science, and Forensic Accounting. Students will also use skills and knowledge from the *Veritas* core, such as the ability to research and write well, an understanding of ethics, and a knowledge of government. Although there are some undergraduate cybersecurity programs in the region, there are few liberal arts schools that offer such a major; graduates from the Mount's program will have a unique skill set because of our strong core program. While we currently offer a Cybersecurity minor which is attractive and beneficial to current students, the Cybersecurity major has the potential to attract many new students to the Mount. This proposal fits into Priority 2, Initiative 2 of the 2013-15 Strategic Plan: The University will strengthen academic quality.

Students in the Cybersecurity major will meet the following Goals and Objectives of the Undergraduate Program:

3. Master the skills of analysis, interpretation, communication, and problem solving.
   To fulfill this goal, Mount St. Mary's expects students to:
   a. Fully understand the characteristics, principles, and challenges that make up the framework for a secure worldwide information system.
   b. Communicate ideas from cybersecurity with precision and clarity to diverse audiences.

5. See and seek to respond with justice and solidarity to all in the global community, to protect human dignity, to work for peace and freedom, and to respect the integrity of creation.
   To fulfill this goal, Mount St. Mary's expects students to:
   a. Discover the ethical uses of the internet and learn how to protect the system from malevolent individuals or groups.
   b. Preserve the dignity and human rights of all that use this technology.

B. *Adequacy of curriculum design and delivery to related learning outcomes consistent with Regulation .10 of this chapter:*

- *Provide a list of courses with title, semester credit hours and course descriptions, along with a description of program requirements.*
- *Describe the educational objectives and intended student learning outcomes.*
- *Discuss how general education requirements will be met, if applicable.*
- *Identify any specialized accreditation or graduate certification requirements for this program and its students. (not applicable)*
- *If contracting with another institution or non-collegiate organization, provide a copy of the written contract. (not applicable)*

The curriculum draws upon regular course offerings from Computer Science and Criminal Justice, and includes new course offerings in Computer Science and Cybersecurity. Students who complete the Cybersecurity major will be required to take twelve courses (36 credits) in Computer Science and Cybersecurity. An additional 12 credits of electives complete the major. In order to graduate, all students must complete the core curriculum (49 credits) plus 23 credits of free electives to meet the requirement of 120 credits. The table below lists requirements and electives. Courses marked with * are new courses. Full course descriptions follow the table.

Requirements for the B.S. in Cybersecurity degree

Major Requirements (36 credits)			**36**
*CYBER 160	Networking Administration	3	
*CYBER 161	UNIX and Windows Operating Systems	3	
*CYBER 201	Secure Systems Design and Risk Management	3	
*CYBER 210	Systems Operations Management	3	
*CYBER 400	Cybersecurity Capstone	3	
CMSCI 120	Introduction to Computer Science I	3	
CMSCI 125	Introduction to Computer Science II	3	
CMSCI 277	Computer Architecture	3	
CMSCI 355	Network Systems and Design	3	
CMSCI 356	Operating Systems and Design	3	
*CMSCI 357	Network Security	3	
CMSCI 358	Computer Security I	3	
Cybersecurity Electives (12 credits)			**12**
(Pick four classes, one of which must be MATH)			
CJUST 120	Sociology of Cybercrime	3	
CJUST 314	Cybersecurity	3	
CJUST 319	Cyber Forensics	3	
BUWI 270	Cyberethics	3	
ACCT 311	Forensic Accounting and Fraud Investigation	3	

ACCT 312	Forensic Accounting and Litigation Advisory Services	3	
MATH 285	Applied Statistics	3	
MATH 228	Discrete Mathematics	3	
CMSCI 359	Database Management Systems	3	
*CMSCI 459	Computer Security II	3	
*CYBER 492	Practicum	3	
General Education Requirements (49 credits)			**49**
FSYM 101	First-Year Symposium	3	
PHIL 103	Foundations of Philosophy	3	
WCIV 102	Origins of the West	3	
MATH 211	Mathematical Thinking	3	
PHIL 203	Philosophy in the Modern Age	3	
WCIV 201	The Modern Western Imagination	3	
THEOL 220	Belief in Today's World	3	
THEOL 320	Encountering Christ	3	
THEOL/PHIL 300	Ethics & the Human Good	3	
AMER 202	America in the World	3	
ENGL/FAAR 373	Literature, the Arts and the Human Condition	3	
XXXX 101^	World Languages I	3	
XXXX 102^	World Languages II	3	
XXGE 3XX	One Global Encounters course *(selected from offerings from various departments)*	3	
XXXX 1XX	One Foundations in Social Science Course *(selected from ECON,PSYCH,SOC,EDUC,PSCI)*	3	
GNSCI 1XX	One Laboratory Science Course	4	
Free Electives (23 credits)			**23**
		Total Credits[#]:	**120**

^Selected from SPAN, FREN, GER, LAT, ITAL

[#] Students must complete 120 credits in order to graduate.

COURSE DESCRIPTIONS

Major Requirements (36 credits)

*CYBER 160 Networking Administration (3)
This hands-on course focuses on building and maintaining computer networks. Topics include network architecture and topologies; network hardware such as cabling, switches, and routers; basics of IP addressing and subnets; network address translation; network configuration; and basic network security. (Fall)

*CYBER 161 UNIX and Windows Operating Systems (3)
In this course, students will study Windows and UNIX operating systems in depth and in a hands-on way. Topics include OS installation; configuration; working at the command

line; managing users and groups; authentication; updates; logging; auditing; managing system services; backups; virtualization; and host-based security. (Spring)

*CYBER 201 Secure Systems Design and Risk Management (3)
Students in this writing intensive course will be introduced to the study of risk assessment and compliance. Topics include security models, architecture, and design principles; threat and vulnerability analysis; risk assessment; risk remediation; incident handling and disaster recovery; laws affecting cybersecurity; compliance including PCI, HIPAA, and FERPA; privacy; protecting data; physical security; measuring reliability and availability; capacity planning; adversaries and targets. (Fall)

*CYBER 210 Systems Operations Management (3)
In this course, students will study managing systems in an enterprise environment. Topics include systems administration; database administration; RAID management; virtualization in enterprise; cloud security; enterprise systems programming; disaster recovery; backup recovery; redundant systems; change and configuration management practices; deploying systems and applications in an enterprise; and managing data. (Spring)

*CYBER 400 Cybersecurity Capstone (3)
This capstone to the Cybersecurity major focuses on the ethics of cybersecurity at enterprise, national, and international levels by examining relevant stories and case studies from the news. This course follows and will reference the junior level ethics course from *Veritas*. Applications in accounting, criminal justice, business, and education are discussed. Students will complete a major project reflecting integration, application, and communication of key elements of cybersecurity. Oral and written communication skills will be emphasized throughout the course and, in particular, in the presentation of the final project. (Spring)

CMSCI 120 Introduction to Computer Science I (3)
This is an entry-level course in computer science that covers problem-solving methods and the development of algorithms. Students are taught how to design, write, edit, test, debug and document simple computer programs. Principles of modularity and information hiding, good programming style and elementary data representation are covered. (Fall and Spring)

CMSCI 125 Introduction to Computer Science II (3)
A continuation of programming techniques from CMSCI 120, this course emphasizes the object-oriented paradigm. Students learn about class design, inheritance, input and output to files, and arrays. Prerequisite: CMSCI 120. (Fall and Spring)

CMSCI 277 Computer Architecture (3)
This is an introduction to the architecture and organization of modern computer systems. Topics are selected from processor and multiprocessor design, instruction set

architectures, addressing, number system representation and computer arithmetic, control structures, microprogramming, memory management, memory hierarchies, and input output structures, assembly-level programming. Prerequisite: CMSCI 120 or permission of instructor. (Fall, even years)

CMSCI 355 Network Systems and Design (3)
The fundamental communications concepts leading to a study of the topology and communication protocols for computer networks are examined. The class focuses on protocols for Internet communication. Topics include application-layer protocols, TCP/IP, DNS servers and e-mail protocols. Prerequisites: CMSCI 125 or permission of the instructor. (Fall, odd years)

CMSCI 356 Operating Systems and Design (3)
This course is an examination of modern operating systems. Topics include dynamic procedure activation, system structure, evaluation, memory management, process management, recovery procedures, and systems software. UNIX and MS Windows are the primary examples. Prerequisites: CMSCI 125 and CMSCI 277 or permission of the program director or department chair. (Spring, odd years)

*CMSCI 357 Network Security (3)
Students will study both the theory and practice of network security. Topics include firewalls; intrusion detection/prevention systems; proxies; VPNs; packet analysis; honeypots; network and vulnerability scanning; secure network configuration; and wireless network security. (Spring, even years)

CMSCI 358: Computer Security I (3)
This course covers cryptography as well as some network and application security topics. Cryptography topics include public key and symmetric key cryptography; public key infrastructure; hashing; digital signatures; SSL/TLS; steganography; and attacks on cryptography. Network and application security topics include botnets; denial of service attacks; buffer and numerical overflows; cross-site scripting; SQL injection; session hijacking; malware such as viruses, trojans, backdoors, and rootkits. (Fall, even years)

Cybersecurity Electives (12 credits)

Pick four classes, one of which must be MATH:

CJUST 120 Sociology of Cybercrime (3)
This course examines the motivations of cyber criminals and victims. The class focuses on why individuals, businesses, and governments engage in cybercrime. It also will address the concerns of victims, what they do about protecting their identity, and how being a victim changes their behavior. (Spring)

CJUST 314 Cybersecurity (3)

This course examines the development of the internet, how it has been used for licit and illicit purposes and by whom, and how government, corporate, and military organizations manage online security. (Fall)

CJUST 319 Cyber Forensics (3)
With nearly everyone and everything now hooked up to the internet, a new wave of illegitimate behavior has changed the investigative playing field and necessitates highly skilled individuals to retrieve lost data and also to find data that has been intentionally misplaced or misused. This course provides individuals with the skills for the investigation of these types of computer-related crimes. Students will learn how to retrieve lost data and protect digital evidence from alterations, damage, or corruption. Digital evidence has been utilized in cases ranging from illegal downloading of music and movies and in the investigation of homicides. (Spring)

BUWI 270 Cyberethics (3)
This very relevant course will explore the ethical ramifications of the computer age, including the Internet, the Web, privacy, computer monitoring, intellectual property, personal information, freedom of speech, computer crime, computers in the workplace and profession ethics and responsibilities. This course may be taken by any interested student. (Spring)

ACCT 311 Forensic Accounting and Fraud Investigation (3)
This course provides an introduction to the practice and various disciplines of forensic accounting and explores investigating fraudulent financial reporting, misappropriation of assets, tax reporting fraud and indirect methods of reconstructing income, money laundering, and cybercrime frauds. The course examines and utilizes various techniques and computer-based tools used by forensic accountants to detect and investigate various frauds. Students will study actual case studies and apply the principles learned to the fraud schemes perpetrated. Prerequisites: ACCT 101-102.

ACCT 312 Forensic Accounting and Litigation Advisory Services (3)
This course explores the other disciplines of forensic accounting including litigation services and expert testimony provided by forensic accountants, commercial damages and how forensic accountants compute economic losses and damages, and business valuations. The course also explores proper evidence management, investigating electronic evidence, digital forensic analysis, and cybercrime management and loss valuations. Students will study actual case studies and apply the principles learned related with these forensic disciplines. Prerequisites: ACCT 101-102.

MATH 285 Applied Statistics (3)
This course is an introduction to the principles and techniques of data analysis and statistical models. Topics include the methods of exploratory data analysis, the design of experiments, sampling, hypothesis testing, simple and multiple regression, and the analysis of variance. Prerequisite: MATH 247 or permission of instructor. (Spring, odd years)

MATH 228 Discrete Mathematics (3)
This course introduces the basic techniques and methods of reasoning for discrete problem solving. Topics include induction, set theory, elementary combinatorics, and graph theory. Applications to computer science are emphasized. This course satisfies the writing intensive *Veritas* program requirement. Same as MAWI 228. (Fall and Spring)

CMSCI 359 Database Management Systems (3)
The design, organization, and implementation of database systems are studied. Topics include the relational model, entity-relationship modeling, normalization, SQL, and database programming. Prerequisite: CMSCI 125. Strongly Recommended: CMSCI 254. (Fall, odd years)

*CMSCI 459 Computer Security II (3)
Primary topics include secure programming techniques, low-level programming, reverse engineering, and penetration testing. In particular, topics include database security; mobile device security; processes for developing secure software; avoiding common security flaws; C and assembly language programming; disassemblers and debuggers; techniques used by malware; penetration-testing tools and techniques. Prerequisites: CMSCI 256 and CMSCI 358. (On a rotating basis)

*CYBER 492 Practicum (3)
Practicum presents an opportunity to gain practical experience through a one semester internship. The nature of the work experience must be approved in advance by the department chair. (As needed)

General Education Requirements (49 credits)
All students at MSMU are required to complete the core curriculum that consists of 49 credit hours of sequential, integrated coursework in the humanities, social sciences, mathematics, and natural sciences. More specifically, the core curriculum includes over 20 credit hours of arts and humanities, 3 credit hours of English composition, 3 credit hours of social and behavioral sciences, 3 credit hours of Mathematics, and 4 credit hours of biological and physical sciences. As such it meets the requirements for general education as listed in COMAR 13B.02.02.16.E.(2).

Educational Objectives
The Cybersecurity degree prepares students for entry level professional practice in cybersecurity in a variety of areas including securing networks and devices, programming, cryptography, information security, software design, and network operations. The program also provides solid preparation for graduate-level study in these same areas. Graduates of the program will find that they are well-prepared for challenging and meaningful careers in the cybersecurity field.

Educational objectives of the program are:

a. To develop content knowledge in the field of cybersecurity

b. To prepare students to work in organizations that secure computer and network systems against theft, fraud, and other malicious acts
c. To prepare students to analyze, defend, and design computer systems
d. To develop an understanding of legal and ethical issues in cybersecurity
e. To develop oral and written communication skills that prepare students to effectively communicate technical ideas to diverse audiences

Student Learning Outcomes

The Cybersecurity major graduates students who:

LO1: demonstrate an understanding of the basic concepts of computer science, criminal justice, and cybersecurity

LO2: have the ability to apply the tools and techniques of cybersecurity to effectively investigate and solve technical problems

LO3: have the ability to communicate technical ideas from cybersecurity with precision and clarity

LO4: understand the legal context and the ethical issues that constitute the cybersecurity profession so that they are prepared for success in a career or graduate study.

C. Critical and compelling regional or Statewide need as identified in the State Plan:

1. Demonstrate demand and need for the program in terms of meeting present and future needs of the region and the State in general based on one or more of the following:

a. The need for the advancement and evolution of knowledge;
b. Societal needs, including expanding educational opportunities and choices for minority and educationally disadvantaged students at institutions of higher education;
c. The need to strengthen and expand the capacity of historically black institutions to provide high quality and unique educational programs.

Provide evidence that the perceived need is consistent with the Maryland State Plan for Postsecondary Education (pdf)

Maryland is a highly-educated state. Thirty five percent of Marylanders have at least a bachelor's degree (DLLR Division of Workforce Development and Adult Learning, Occupational projections-2008-2018, p. 43). Maryland ranks third behind Massachusetts and Colorado in percent of population with advanced degrees. According to the Maryland Department of Labor, Licensing and Registration (DLLR), in short term projections for job growth for 2014-2016, "computer and mathematical occupations" will be "faster than usual" high-growth areas. In every sector, from computer systems analysts to network and computer system administrators, the expectation of growth is high (DLLR Division of Workforce Development and Adult Learning, Occupational projections 2014-2016 and 2012-2022 and Commission on Maryland Cybersecurity Innovation and Excellence, Sept 1, 2014).

Our proposed program makes Mount students competitive in a rapidly growing market (Maryland Commission on Cybersecurity Innovation and Excellence, September 1, 2014). The development of the BS in Cybersecurity by Mount St. Mary's University addresses the critical and compelling statewide need of workforce development. According to the Maryland state plan,

> "It is critical that Maryland state and local governments adopt laws and policies that endorse and encourage cyber education in Maryland's high schools, colleges, and universities. The emphasis on cyber related education, recruitment, and workforce development will not only increase the cybersecurity of Maryland, but it will allow Maryland the opportunity to be a leader in this emerging and vital field" (p. 22).

In addition, according to the United States Department of Labor, Bureau of Labor Statistics the nationwide growth rate for Cybersecurity Operations analysts will be 37% from 2012-2022. These jobs require a bachelor degree and have a median salary of $86,170 per year or $41.43 per hour. In Maryland, the need is even greater because of the high concentration of Cybersecurity firms operating in and around Washington, D.C. Furthermore, the degree plan has an internship opportunity, affording students opportunities to contribute to their communities while learning.

D. *Quantifiable & reliable evidence and documentation of market supply & demand in the region and State:*

1. *Present data and analysis projecting market demand and the availability of openings in a job market to be served by the new program.*

Currently, the demand for cybersecurity professionals is very high. In the private sector the cybersecurity market was valued at $46 billion in 2015 and is in a rapid growth phase (Figure 1). Government spending is similarly large and growing largely in response to the escalating number of cyber attack incidents (Figure 2). The number of federal cybersecurity incidents has grown from 5,500 in 2006 to 67,000 in 2014.

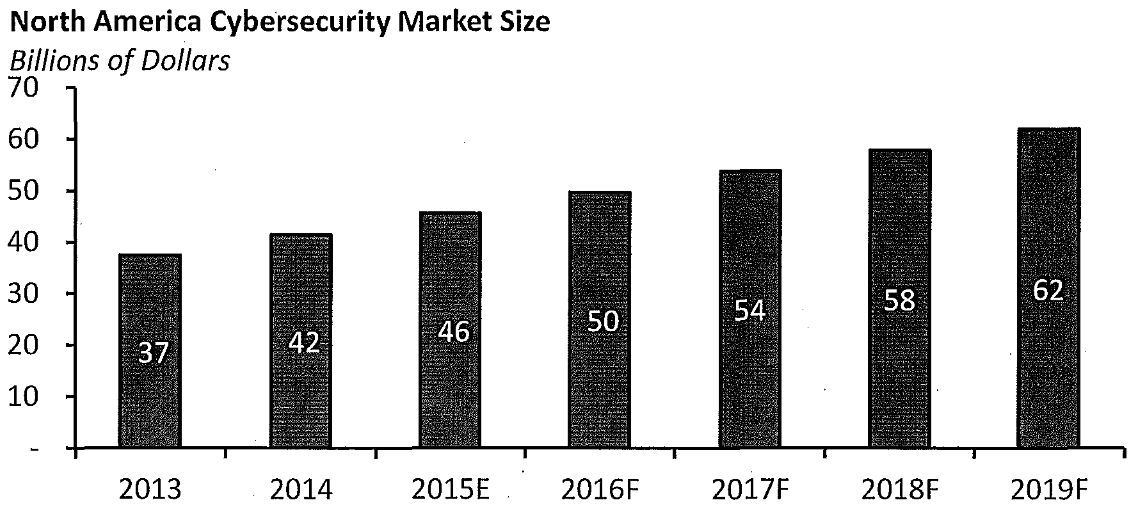

Figure 1. Steady growth in cybersecurity market size is expected through the end of the decade. Source: MicroMarketMonitor, http://www.micromarketmonitor.com/market-report/cyber-security-reports-7651948375-2.html

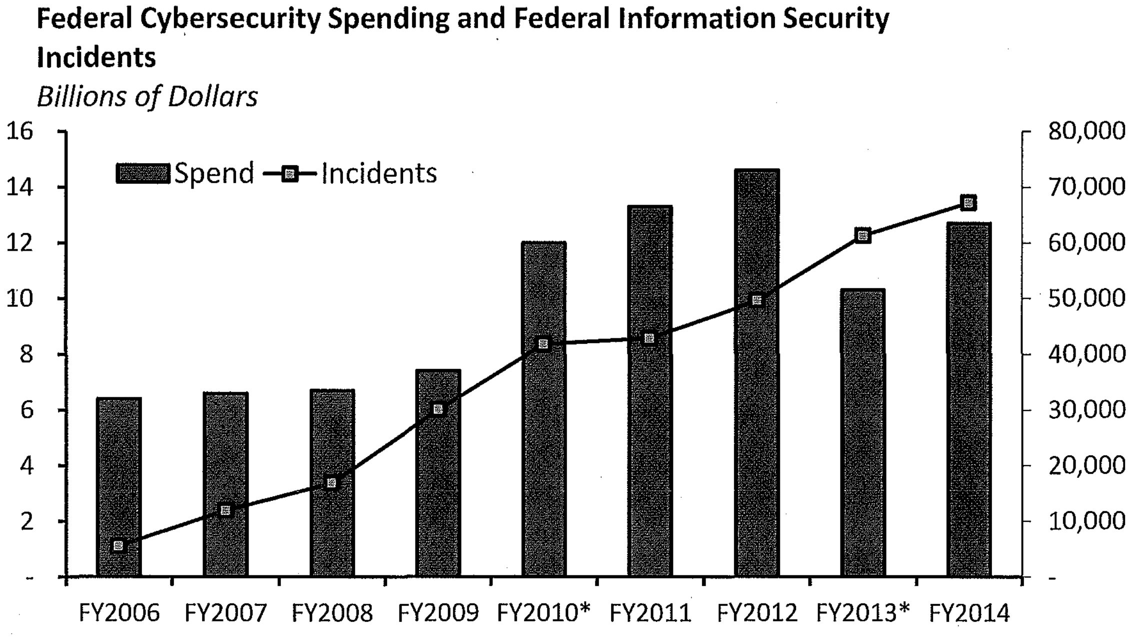

Figure 2. Federal cybersecurity spending has been steadily growing in parallel to the number of attacks on government agency systems. Note: * OMB calculation methodology changed in these years. Sources: Government Accountability Office, Peninsula Press (Stanford), CS Monitor.

The number of cybersecurity employees has doubled over the past decade from a nationwide total of 260,000 in 2005 to 524,000 in 2014 (Figure 3). A large fraction of those positions are located within MSMU's "catchment area," defined here as the eight states from which 93% of our students come (MD, PA, NJ, VA, NY, DE, FL, CT). Six of those eight states are ranked in the top 15 states for cybersecurity job postings in 2014 (Table 1). The total number of job postings in those states alone was 69,631 which indicates a tremendous demand for cybersecurity graduates within this region.

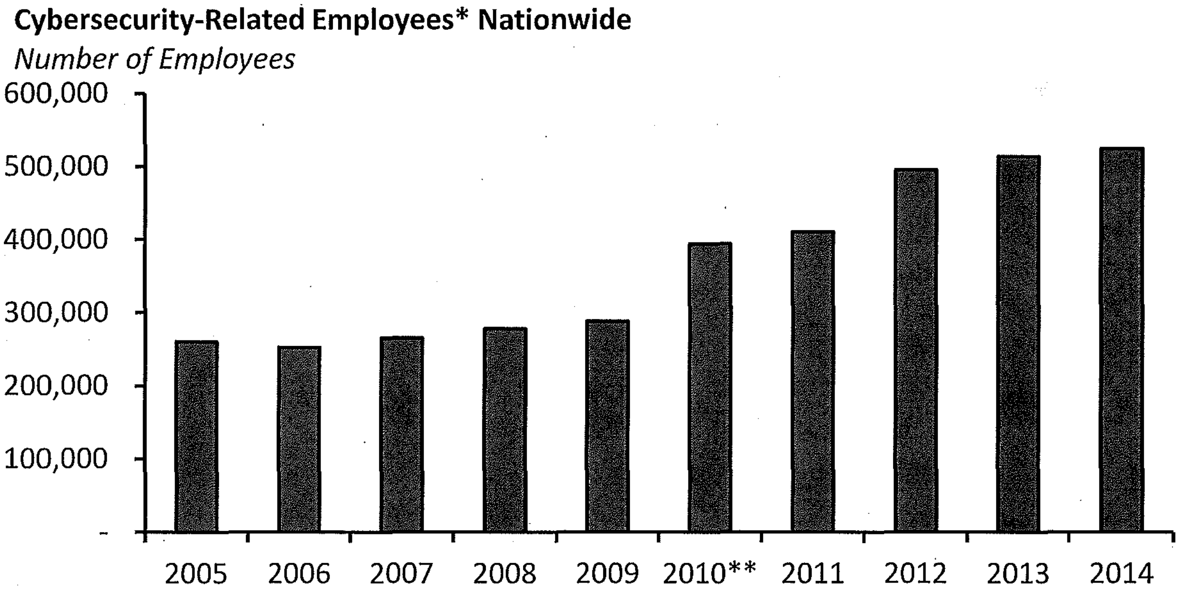

Figure 3. The number of cybersecurity-related employees nationwide has grown rapidly since 2010. Note: *Systems Managers, Database Administrators, and Information Security Analysts; **2010 CIP code reclassification Source: Bureau of Labor Statistics

Table 1. States within MSMU's catchment area that are ranked within the top 15 states for total cybersecurity job postings. The percent growth in job postings from 2010 to 2014 is also listed. Source: Burning Glass Technologies.

Rank	State	Total Postings	% Growth (2010-2014)
2	Virginia	20,276	38%
4	New York	14,089	104%
6	Maryland	11,406	39%
7	Florida	9,847	135%
9	New Jersey	8,268	80%
14	Pennsylvania	5,745	69%
	Total	69,631	

Over the next decade, cybersecurity is projected to be a fast growing profession. Case in point, the industry market size is projected to increase by 35% by 2019 (Figure 1). Cybersecurity is not listed as a profession in the Bureau of Labor Statistics' (BLS) Occupational Outlook Handbook but similar occupations within computer science show ten-year growth rates of 8 – 18% which exceeds the average projected growth rate for all occupations (7%; Table 2). BLS estimates that 200,900 new positions will be created in these fields across the U.S. Within Maryland the picture is very similar. Rapid expansion in several computer science fields is anticipated at least through the year 2022 with growth rates ranging from 5 to 41% (Table 3).

Table 2. Number of employees nationwide in cybersecurity-related professions in 2014 and estimated for 2024. Source: U.S. Bureau of Labor Statistics, Employment Projections program.

Occupational Title	Employment, 2014	Projected Employment, 2024	Change, 2014-24	
			Percent	*Numeric*
Network and computer systems administrators	382,600	412,800	8	30,200
Computer and information systems managers	348,500	402,200	15	53,700
Information security analysts	82,900	97,700	18	14,800
Database administrators	120,000	133,400	11	13,400
Computer support specialists	766,900	855,700	12	88,800
Totals	**1,700,900**	**1,901,800**		**200,900**

Table 3. Number of Maryland employees in cybersecurity-related professions in 2012 and estimated for 2022. Source: MD Dept. of Labor, Licensing and Regulation, http://www.dllr.state.md.us/lmi/iandoproj/maryland.shtml.

Occupation	2012	Projected, 2022	Change, 2012-22	
			Percent	*Numeric*
Computer and Information Research Scientists	3,492	4,099	17.4	607
Computer Systems Analysts	11,935	14,589	22.2	2,654
Information Security Analysts	3,375	4,764	41.2	1,389
Software Developers, Systems Software	14,020	17,124	22.1	3,104
Database Administrators	3,420	3,976	16.3	556
Network and Computer Systems Administrators	10,094	11,516	14.1	1,422
Computer Network Architects	4,940	5,739	16.2	799
Computer Network Support Specialists	5,093	5,365	5.3	272
Totals	**56,369**	**67,172**		**10,803**

In summary, all indicators of current and projected demand for cybersecurity graduates in the state, region, and nation agree that the cybersecurity job market is strong and undergoing rapid growth. With cyber attacks on the rise, more and more companies are hiring security specialists to protect against and respond to attacks. Likewise, government agencies, such as the National Security Agency and Department of Defense, are expanding their cybersecurity workforce to deal with these cyber threats.

2. *Discuss and provide evidence of market surveys that clearly provide quantifiable and reliable data on the educational and training needs and the anticipated number of vacancies expected over the next 5 years.*

In March 2014, an online survey was distributed to 136 representatives of local companies and organizations who are members of the Frederick County Chamber of Commerce. The survey was solicited by the Advisory Board of the Center for Research and Education in Science and Technology (CREST) and was conducted by MGT, Inc. The survey's (hereinafter CREST survey) target audience was developed using a purposeful rather than random sample of major local employers across a variety of industry sectors and supplemented with a set of smaller employers. Employers invited to participate represent a cross-section of business categories. The survey remained open for six weeks. Multiple follow-up appeals for participation to the sample of employers yielded 41 completed surveys (30% response rate).

Cybersecurity was featured prominently in this report. It was one of the educational programs that employers believed should be offered in the county at the certificate and bachelor's level but at that time no such programs existed. When asked in which fields current or future employees were likely to need training over the next 3-5 years, 37% of employers selected "computer information and support services" as one of the responses. Business owners also estimated the number of employees they would need over the next 3-5 years with a bachelor's degree in a cybersecurity-related field (Table 4). The total was 192 but we must keep in mind that this estimate comes from just a sampling of businesses in the region. The actual need is undoubtedly much higher. Finally, in the conclusion of the report, cybersecurity was listed as one of six educational programs that should be considered for implementation in this region.

Table 4. Local educational needs requiring Bachelor's degrees according to the CREST employer survey of 41 businesses conducted in 2014 in the Frederick, MD area.

Academic Discipline	No. of Current and Future Employees Needing Training	Is Program Available in the Local Market?
Computer and Information Sciences	53	Y
Computer Systems Networking and Telecommunications	35	N
Management Information Systems and Services	32	Y
Communications Technology Technician	29	N
Computer Programming	24	N

Computer/Information Technology Administration and Management	19	Y
Total	**192**	

The need for cybersecurity graduates can also be inferred from general employment information. Figure 3 shows the huge and growing number of cybersecurity employees nationwide and Table 1 lists the large number of job postings for cybersecurity positions in Maryland in 2014 (11,406). Although these numbers apply to the workforce demand on a larger scale, there is no reason to believe that they would not be representative of Frederick County and the surrounding region. Within 50 miles of Frederick County are several major federal agencies that rely on cybersecurity professionals (e.g., National Security Agency, National Institute for Standards and Technology, and Department of Defense) as well as major cybersecurity companies (e.g., Lockheed Martin, Northrop Grumman, and Patriot Technologies). In fact, last year 14 Maryland companies were added to the Cybersecurity 500, a global list of the world's leading cybertechnology companies (http://open.commerce.maryland.gov/it-and-cybersecurity/). Clearly, Maryland's current strengths in cybertechnology and technology in general will lead to increasing demand for cybersecurity professionals in the coming decade.

3. *Data showing the current and projected supply of prospective graduates.*

Strong government and corporate demand have driven the creation and expansion of Cybersecurity degree programs, which have attracted a large number of new students across degree levels (Figure 4). Within the surrounding states, there are 12 institutions with Bachelor degree programs in cybersecurity (that graduate more than 10 students per year) and in 2014 they awarded 672 degrees in those programs. This is a robust indication of strong interest in this type of program among undergraduates.

One indicator of current MSMU student interest in cybersecurity is the number of students who are taking the required courses for the minor, which was instituted in Fall 2014. The three courses offered between Fall 2014 and Fall 2015 were all filled to capacity (25 students in each). Such strong enrollment in just the 2nd year of the program suggests that there is student interest in this field. Part of the success of this minor probably is a result of the robust Criminal Justice program which comprises about 95 majors (sophomores, juniors and seniors; 2016 FactBook). Cybersecurity sits squarely between computer science and criminal justice and may draw some students (e.g., double majors) from those populations.

Finally, we intend to establish articulation agreements with regional community colleges that will encourage students with Associate's degrees to pursue a Bachelor's degree at MSMU. We have such agreements with community colleges already and they provide a reliable stream of students in particular areas. Table 5 shows the large number of Associate degree programs in the state from which we could draw transfer students.

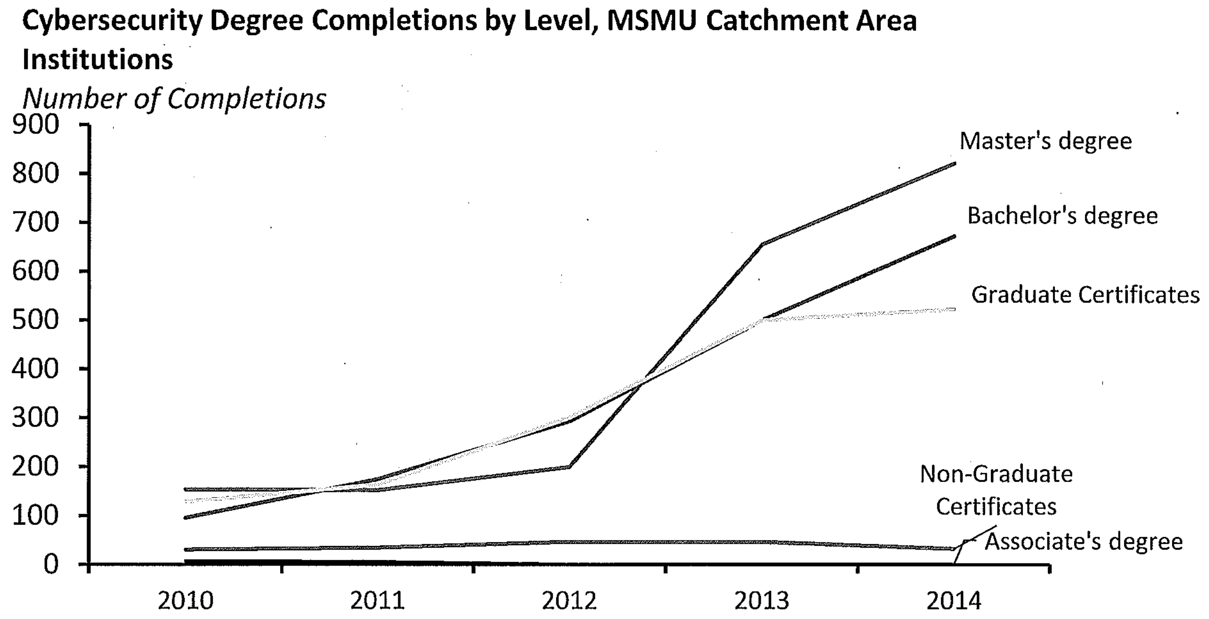

Figure 4. The number of cybersecurity degrees awarded at higher education institutions in MD and surrounding states (PA, NJ, NY, DE, VA, and DC) has increased rapidly since 2011.

Table 5. List of associates degree programs in cybersecurity within Maryland that could serve as sources of students for our program by establishing articulation agreements. Source: MHEC list of academic programs, accessed 20-Feb-2016; http://www.mhec.state.md.us/utilities/search_CIP.asp.

Institution	Program Name	Degree Offered
Anne Arundel Community College	CYBERCRIME	Associate Degree
Anne Arundel Community College	INFORMATION ASSURANCE & CYBERSECURITY	Associate Degree
Baltimore City Community College	CYBER SECURITY AND ASSURANCE	Associate Degree
Cecil College	CYBERSECURITY	Associate Degree
Frederick Community College	CYBERSECURITY	Associate Degree
Garrett College	CYBERSECURITY	Associate Degree
Hagerstown Community College	CYBERSECURITY	Associate Degree
Hagerstown Community College	CYBERSECURITY	Associate Degree
Montgomery College-All Campuses	CYBERSECURITY	Associate Degree
Prince George's Community College	CYBERSECURITY	Associate Degree

E. Reasonableness of program duplication:

1. *Identify similar programs in the State and/or same geographical area. Discuss similarities and differences between the proposed program and others in the same degree to be awarded.*

Within Maryland there are only three institutions that offer Bachelor degrees in cybersecurity — Capitol Technology University, Frostburg State University, and University of Maryland University College (Table 6). Towson University and the University of Maryland, College Park offer a cybersecurity track within their computer science programs. The proposed program at MSMU will be unique and will complement the other full cybersecurity programs. First the UMUC cybersecurity programs are 100% online, whereas the MSMU program is offered primarily onsite. Moreover, we expect very little overlap in terms of the population of interested prospective students. UMUC is a very large, public institution while MSMU is a small, private, liberal arts university.

Capitol Technology University (CTU) offers two Cybersecurity programs. The Management of Cyber and Information Technology focuses on the administration and business aspects of information management which is very different from the MSMU program. CTU's Cyber and Information Security program has a few similarities to the MSMU program in terms of being technology focused. However, the combination of our sequenced and integrated general education curriculum (61 credits) and our multidisciplinary cybersecurity program provides a much broader liberal arts foundation than Capitol Technology University's program.

The Secure Computing and Information Assurance program at Frostburg State focuses mainly on the technical side of cybersecurity with most of the courses being housed in the Computer Science Department. In contrast, the MSMU program is more multidisciplinary, incorporating coursework in criminal justice and ethics and our general education program is more extensive.

Table 6. List of bachelor degree and associates degree programs in cybersecurity within Maryland. The bachelor programs are potential competitors but the associate programs could serve as sources of students for our program with the help of articulation agreements. Source: MHEC list of academic programs, accessed 20-Feb-2016; http://www.mhec.state.md.us/utilities/search_CIP.asp.

Institution	Program Name	Degree Offered
Capitol Technology University	CYBER AND INFORMATION SECURITY	Bachelor's Degree
Capitol Technology University	MANAGEMENT OF CYBER & INFO TECHNOLOGY	Bachelor's Degree
Frostburg State University	SECURE COMPUTING & INFO ASSURANCE	Bachelor's Degree
Univ. of Maryland University College	CYBER SECURITY (online)	Bachelor's Degree
UMD, College Park	COMPUTER SCIENCE (computer security track)	Bachelor's Degree
Towson University	COMPUTER SCIENCE (cybersecurity specialization)	Bachelor's Degree

2. *Provide justification for the proposed program.*

In summary, the MSMU program is unique because the curriculum has a focus on Cybersecurity at the software and operating systems level and is complemented by a robust and integrated general education program. The other programs in the state are more narrowly focused and are technology heavy. We also are leveraging our strength in Criminal Justice and our location near federal security agencies to incorporate an emphasis on cybercrime. Finally, the proposed MSMU program is offered in an educational setting that is different from the others: an onsite program at a small, private, liberal arts institution.

The proposed program meets a strong workforce demand in the state and region and contributes to Maryland's drive to become a technology leader in the nation. With many computer technology, information technology and cybersecurity companies in and around Washington, DC, a program such as this is extremely valuable.

F. Relevance to Historically Black Institutions (HBIs)

1. *Discuss the program's potential impact on the implementation or maintenance of high-demand programs at HBI's.*

We do not anticipate any impact on programs at HBI's.

2. *Discuss the program's potential impact on the uniqueness and institutional identities and missions of HBIs. Not applicable.*

We do not anticipate any impact on HBI's.

G. 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 entirely on-site.

H. Adequacy of faculty resources (as outlined in COMAR 13B.02.03.11).

Provide a brief narrative demonstrating the quality of program faculty. Include a summary list of faculty with appointment type, terminal degree title and field, academic title/rank, status (full-time, part-time, adjunct) and the course(s) each faulty member will teach.

The Cybersecurity program will be housed administratively within the Mathematics and Computer Science Department. The faculty who will teach courses in the program will come from several departments. The majority of the faculty listed below have terminal degrees in their field and many are experienced Associate and Full Professors. These faculty have already demonstrated their ability to collaborate through the Cybersecurity minor that was instituted two years ago. A computer scientist, with graduate degree and cybersecurity training or experience, will be hired to take a lead role in this program.

List of current faculty (and areas of expertise) who will teach in the program.

Business Course

Bruce E. Yelovich, MS in Information Systems, M.Div., M.L.S.; Assistant Professor of Information Systems; Full-time; Courses: Information Systems, Cyberethics

Computer Science and Mathematics Courses

Brian Heinold, Ph.D. in Mathematics; Associate Professor of Mathematics and Computer Science; Full-time; Courses: Software Development, Network Systems and Design, Introduction to Computer Science I and II, Computer Security I and II, Discrete Mathematics

Frederick J. Portier, Ph.D. in Mathematics; Professor of Mathematics and Computer Science; Full-time; Courses: Database Management Systems, Introduction to Computer Science I and II, Introduction to Data Science I

Scott Weiss, M.S. in Computer Science; Assistant Professor of Computer Science; Full-time; Courses: Introduction to Computer Science I and II, Computer Architecture, Operating Systems and Design

Criminal Justice Courses

Dr. Virginia McGovern, Ph.D. in Criminology and Social Psychology; Associate Professor and Department Chair of Sociology and Criminal Justice; full-time; Courses: Cybersecurity, Sociology of Cybercrime, White Collar Crime

Dr. David Scibelli: Ph.D. in Science; Adjunct Professor, part time. Courses: Cybersecurity, Cyber Forensics

I. Adequacy of library resources (as outlined in COMAR 13B.02.03.12)

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 supports Education, Business, Theology and Sociology. The collection includes all the major databases in each of these disciplines 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/databases. The library recently implemented the *EBSCO Discovery Service* that performs a single search of all library resources from one search interface. Funding is being requested for some new cybersecurity-related subscriptions.

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 highly competent, 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 7. 2013-2014 Library Expenditures	
Volumes	147,503
Per FTE student	*71*
Journal Titles-Paper	308
Journal Titles-Digital	15,850
Librarian Research Transactions	654
Participation in Instruction Services	512
Databases	125
Videos	1,422
Total Library Expenditures	$838,413
Library expenditures per FTE student	$ 403
Source: Mount St. Mary's Factbook 2015	

J. Adequacy of physical facilities, infrastructure and instructional equipment (as outlined in COMAR 13B.02.03.13)

Provide an assurance that physical facilities, infrastructure and instruction equipment are adequate to initiate the program, particularly as related to spaces for classrooms, staff and faculty offices, and laboratories for studies in the technologies and sciences. If the program is to be implemented within existing institutional resources, include a supportive statement by the President for adequate equipment and facilities to meet the program's needs.

Cybersecurity professionals must apply what they know to the herculean task of protecting information by anticipating and preventing problems, trouble-shooting, and creating and managing computer networks. Thus, extensive hands-on training in a variety of platforms and network systems, an abundance of simulations and problem-solving exercises, and opportunities for students to pursue their own projects are critical for solid preparation of future cybersecurity professionals. Therefore, a well-equipped computer lab is an essential component of our new cybersecurity program.

One of our current computer laboratories (Coad 111) will be upgraded to include hardware (e.g., servers, workstations) to create multiple independent networks. Students will need to have the experience of building and managing a computer network using a variety of platforms and equipment, and setting security protocols. They need to learn how to set up firewalls and how to prevent hackers from accessing their system. Faculty will use the lab to set up simulations for class exercises and to provide specialized software to students.

With the exception of the computer lab, we have adequate classroom space and office space for the faculty involved. The program will be housed in the Coad Science Building and within the Department of Mathematics and Computer Science. 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.

K. Adequacy of financial resources with documentation (as outlined in COMAR 13B.02.03.14).

1. Complete Table 8: Resources (pdf) and Table 9: Expenditure (pdf). Finance data(pdf) for the first five years of program implementation are to be entered. Figures should be presented for five years and then totaled by category for each year.
2. Provide a narrative rational for each of the resource category. If resources have been or will be reallocated to support the proposed program, briefly discuss the sources of those funds.

TABLE 8: RESOURCES						
Resources Categories	Year 0 (2016-17)	Year 1 (2017-18)	Year 2 (2018-19)	Year 3 (2019-20)	Year 4 (2020-21)	Year 5 (2021-22)
1. Reallocated Funds	$15,000	$32,700	0	0	0	0
2. Tuition/Fee Revenue (c+g below)	$0	$172,250	$268,710	$372,611	$484,395	$604,524
a. # F.T. Students	0	10	15	20	25	30
b. Annual Tuition/ Fee Rate (Discounted rate) from 2015 Fact Book		$17,225	$17,914	$18,631	$19,376	$20,151
c. Annual Full Time Revenue (a x b)	$0	$172,250	$268,710	$372,611	$484,395	$604,524
d. # Part Time Students						
e. Credit Hour Rate						
f. Annual Credit Hours						
g. Total Part Time Revenue (d x e x f)						
3. Grants, Contracts, & Other External Sources						
4. Other Sources						
TOTAL (Add 1-4)	**$15,000**	**$204,950**	**$268,710**	**$372,611**	**$484,395**	**$604,524**

Explanation of Resources

Academic year 2016-17 (Year 0) will be a year of preparation because we will not have time to recruit students. After a strong recruiting and marketing effort in 2016-17 we expect to admit a first cohort of 10 students in Fall 2017. Thereafter, we expect to grow by approximately 5 students per year, leveling off at about 30 students. Some of these students will be transfer students from two-year institutions. The net tuition and fees revenue was obtained from the 2015 FactBook and was incremented by 4% per year which is a typical rate of tuition increase for MSMU.

TABLE 9: EXPENDITURES						
Expenditure Categories	Year 0 (2016-17)	Year 1 (2017-18)	Year 2 (2018-19)	Year 3 (2019-20)	Year 4 (2020-21)	Year 5 (2021-22)
1. Faculty	0	$120,700	$122,978	$125,302	$127,672	$130,089
a. # FTE	0	1	1	1	1	1
b. Total Salary		$85,000	$86,700	$88,434	$90,203	$92,007
c. Total Benefits		$28,900	$29,478	$30,068	$30,669	$31,282
d. PT Adjunct Salary		$6,800	$6,800	$6,800	$6,800	$6,800
2. Admin. Staff						
a. # FTE						
b. Total Salary						
c. Total Benefits						
3. Support Staff	$0	$0	$0	$0	$0	$0
a. # FTE						
b. Total Salary						
c. Total Benefits						
4. Equipment	0	$48,250	$48,250	$20,000	0	$20,000
5. Library	0	$2,000	$2,100	$2,205	$2,315	$2,431
6. New or Renovated Space	0	0	0	0	0	0
7. Other Expenses (software and materials)	$15,000	$34,000	$19,000	$34,000	$19,000	$34,000
8. TOTAL (Add 1 – 7)	$15,000	$204,950	$192,328	$181,507	$148,987	$186,520

Explanation of Expenditures

1. **Faculty**

   By Year 1, we will hire a full-time, tenure-track faculty member in cybersecurity to teach most of the new cybersecurity courses (CYBER 201, 210, 400; CMSCI 358, and 492 every year and CMSCI 357, 359, and 459 every other year) and some computer science courses which will result in a full teaching load (21 credits per year). Because this new program is outside the realm of expertise of our current faculty and because this is a rapidly-changing field, it absolutely critical that we hire an expert in the field who can lead the program and remain up to date on cybersecurity issues. The range of median salaries for mid-level cybersecurity professionals is $80,000 - $100,000 (Payscale; Bureau of Labor Statistics). The national average for Asst. Professor Computer Science faculty (first-year) is $82,500 (Inside Higher Ed). In order to be able to attract and retain an expert in this field a salary of $85,000 is recommended.

   Two courses annually will be taught by part-time adjunct faculty (CMSCI 160, 161; 6 credits total/yr). The total expense for adjunct faculty would be $3,400/course * 2 courses = $6,800 per year.

2. **Equipment**

   The existing computer lab will be upgraded to support the coursework in the new program, including hands-on activities, system design and construction, network troubleshooting, simulations and cyber competitions. Three servers (Cisco Poweredge r420, $9,600 each) will be purchased for a total of $28,800. Fifteen new desktop workstations and monitors will be purchased (e.g., HP Z640, $2,500 each for a total of $37,500) that allow access to the internal workings, easy reconfiguration, and have the computing power necessary for the program's goals. These workstations are necessary for the success of the proposed project because students need to be able to work on modern hardware in the hands-on, simulation-rich curriculum. Three firewalls (two Meraki MX84 with 3-yr license, $5,500 and Cisco ASA 5516, $3,600) and four switches (two Cisco 3850 Layer 3 for $4,500 each and two 2960 Layer 2 for $3,300 each) will be purchased. The total for these one-time purchases is $ 96,500. It is important to note that the current computer lab is long overdue for an upgrade; we already need to invest at least $40,000 in an upgrade to the lab within the next few years for the existing programs which use the facility. These programs include the Computer Science major, Computer Science minor, Mathematics major, and Cybersecurity minor. Thus, the proposed upgrade for $96,500 will meet a need for both Cybersecurity and existing programs.

3. **Library**

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

4. New or Renovated Space

Not applicable.

5. Other Expenses

$15,000/yr in years 0 and 1	**Marketing Resources:** For this program to be successful, we need to actively recruit new students from a different population than our current pool of prospects; specifically, students with high aptitude in mathematics and computer science. These funds will be added to the Marketing and Communications budget for two years to provide that office with resources for conducting market research, developing a marketing plan and implementing that plan. For example, the office could try to identify special populations like STEM schools and charter schools. It is expected that after two years of this active research and planning, the implementation can be integrated into the normal operations of the Marketing and Communications office. The funds may be used for compensation for a part-time employee, to hire a market research firm, and/or for marketing materials such as brochures, mailings, and video segments for the website.
$4,000/yr	**Travel and Supplies:** The Mathematics and Computer Science departmental budget will need to be adjusted to accommodate the additional faculty member. Specifically, the standard $2,000/yr for faculty development and $2,000/yr in educational supplies (cables, routers, adaptors, tools, challenge competition supplies, etc.).
$15,000/yr	**Software:** The Mathematics and Computer Science departmental budget will need up to $15,000/yr for software and firewall licenses. Much of this software can also be used by the Computer Science program.
$15,000 in yrs 3 and 5	**Technology Upgrades:** To remain up-to-date with industry standards and with technology changes, the computer lab hardware, including workstations, will need to be updated or replaced on a rotating basis.

By subtracting total expenditures (Table 9) from total revenue (Table 8) we arrive at the net "profit" for the program. This is not truly a profit for the University as the cybersecurity students will be taking other courses and using other resources at the University. However, this exercise does show that the tuition revenue from the students is far greater than the costs of the program, including personnel, infrastructure, and equipment/materials. During the 2016-17 and 2017-18 years, there is expected to be a net loss because of the large investment in equipment and personnel compared to relatively few students. VP for Finance, Bill Davies, has confirmed that the University can absorb that amount of loss for two years (personal communication to Jeff Simmons). In year 2 and thereafter, the revenue far surpasses the expenses.

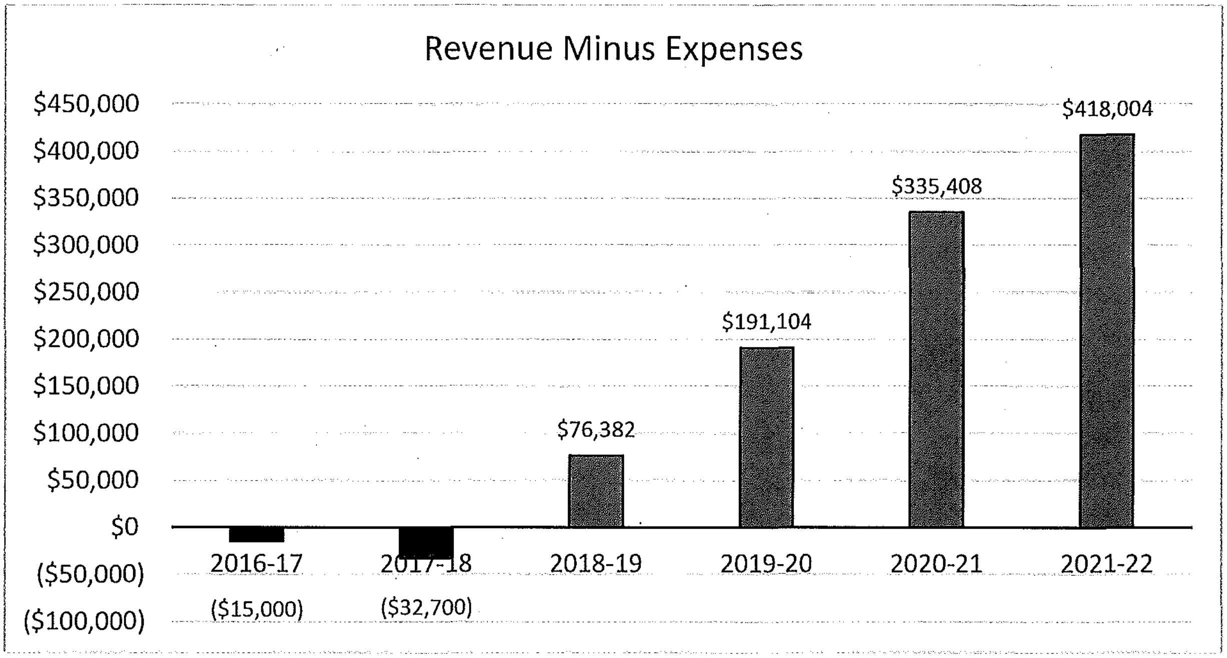

Figure 5. The difference in revenue (from net tuition of new cybersecurity majors, excluding "reallocated funds") and expenses (of the proposed cybersecurity program) from 2016-17 through 2021-22.

L. Adequacy of provisions for evaluation of program (as outlined in COMAR 13B.02.03.15).

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

1. Middle States Accreditation
2. Course evaluations
3. Faculty reviews
4. Program assessment and five-year reviews

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 the department assessment for the program, with each Learning Outcome being assessed at least once in a five-year period.

Learning Outcome	Assessment	Benchmark	Timing
LO1: demonstrate an understanding of the basic concepts of computer science, criminal justice, and cybersecurity	Department-designed computer science and cybersecurity exam with input from Criminal Justice	TBD	Every spring in Capstone
LO2: have the ability to apply the tools and techniques of cybersecurity to effectively investigate and solve technical problems	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 in a career or graduate study	One and five-year surveys of alumni	TBD	Every spring

M. Consistency with the State's minority student achievement goals (as outlined in COMAR 13B.02.03.05 and in the State Plan for Postsecondary Education).

Discuss how the proposed program addresses minority student access & success, and the institution's cultural diversity goals and initiatives.

The BS in Cybersecurity degree at MSMU will be promoted along with all the other undergraduate programs. For a Catholic institution of our size, our minority population is relatively high. In the 2015-16 academic year, minorities made up 29.5% of the undergraduate population. Our commitment to diversity is evidenced by a recent S-STEM award from the National Science Foundation that will provide scholarship funding for 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, 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:

No low productivity programs have been identified by the Commission at Mount St. Mary's University. Therefore, this section is not applicable.