Office Use Only: PP#

MHEC
Creating a state of achievement

Cover Sheet for In-State Institutions
New Program or Substantial Modification to Existing Program

Institution Submitting Proposal	University of Baltimore

Each action below requires a separate proposal and cover sheet.

- (●) New Academic Program
- ( ) New Area of Concentration
- ( ) New Degree Level Approval
- ( ) New Stand-Alone Certificate
- ( ) Off Campus Program
- ( ) Substantial Change to a Degree Program
- ( ) Substantial Change to an Area of Concentration
- ( ) Substantial Change to a Certificate Program
- ( ) Cooperative Degree Program
- ( ) Offer Program at Regional Higher Education Center

JB 028660

Payment Submitted: (●) Yes ( ) No | Payment Type: (●) R*STARS ( ) Check | Payment Amount: $850 | Date Submitted: 12/6/18

Department Proposing Program	Merrick School of Business
Degree Level and Degree Type	Master of Science
Title of Proposed Program	Cyber Security Management
Total Number of Credits	30 - 33
Suggested Codes	HEGIS: 0799-11 CIP: 11.1003
Program Modality	(●) On-campus ( ) Distance Education (*fully online*) ( ) Both
Program Resources	(●) Using Existing Resources ( ) Requiring New Resources
Projected Implementation Date	(●) Fall ( ) Spring ( ) Summer Year: 2019
Provide Link to Most Recent Academic Catalog	URL: http://www.ubalt.edu/academics/uploads/catalogs/18-19_grad_catalog/18-19GRCatalogFINAL.pdf
Preferred Contact for this Proposal	Name: Dr. Candace Caraco Title: Assistant Provost Phone: (410) 837-5243 Email: ccaraco@ubalt.edu
President/Chief Executive	Type Name: Dr. Darlene B. Smith, Executive Vice President and Provost Signature: Darlene B. Smith Date: 11/28/2018
	Date of Approval/Endorsement by Governing Board:

Revised 11/2018

November 26, 2018

The Honorable James D. Fielder, Jr., Ph.D.
Secretary of Higher Education
Maryland Higher Education Commission
6 N. Liberty St.
Baltimore, MD 21201

Dear Secretary Fielder,

The University of Baltimore seeks approval to offer a Master of Science (MS) in Cyber Security Management. The program will be based in the Merrick School of Business but is interdisciplinary, drawing on expertise not only in technical elements of cyber security, but also in organizational management, psychology, and digital forensics.

Thank you for your consideration. Please let me know if you have any questions.

Sincerely,

Kurt L. Schmoke
President

cc: Dr. Darlene B. Smith, EVP and Provost
Dr. Antoinette Coleman, USM

Office of the Executive
Vice President and Provost

UNIVERSITY OF BALTIMORE
ubalt.edu

1420 N. Charles St.
Baltimore, MD 21201

T: 410.837.5244
F: 410.837.5249

UNIVERSITY SYSTEM OF MARYLAND INSTITUTION PROPOSAL FOR

X	New Instructional Program
	Substantial Expansion/Major Modification—existing program going online
	Cooperative Degree Program
X	Within Existing Resources, or
	Requiring New Resources

University of Baltimore
Institution Submitting Proposal

Master of Science in Cyber Security Management
Title of Program

Master of Science	**Fall 2019**
	Projected Implementation Date
0799-11	**11.1003**
Program HEGIS Code	Program CIP Code
Department of Information Systems and Decision Science, Merrick School of Business	Danielle Fowler Department Chair; Candace Caraco Office of the Provost
Department in which program will be located	Department Contact
410-837-5243	ccaraco@ubalt.edu
Contact Phone Number	Contact E-Mail Address
Barbara B Smith	10-8-2018
Signature of President or Designee	Date

New Instructional Program

The University of Baltimore requests approval for the creation of a Master of Science (MS) in Cyber Security Management. UB is proposing the first AACSB-accredited master's in cyber security management program in Maryland, building on the business school's proven history of delivering quality management education in preparing students to take senior leadership roles in the management of information security.

The program features a customized, inter-disciplinary curriculum that will leverage existing expertise across three schools (Business, Public Affairs, and Arts & Sciences), and complement existing graduate specializations and programs in the area, including those from the business school (MBA specializations in Leadership, Managing Financial Performance, Data Analytics and Cybersecurity & Organizational Resilience), the Yale Gordon College of Arts and Sciences (MS in Applied Psychology - Industrial/Organizational Psychology), and the College of Public Affairs (MS in Forensic Science: High-Tech Crime).

A. **Centrality to Mission and Planning**

The proposed Master of Science (MS) in Cyber Security Management program will prepare graduates for the unmet demand for cyber security expertise both nationally and regionally by instilling knowledge of leadership, strategy and information security management, as well as incorporating important inter-disciplinary perspectives from criminal justice and psychology.

The program's professional career focus fits with the mission of the University of Baltimore (UB), which is to offer career-focused education for aspiring and current professionals, making excellence accessible to traditional and nontraditional students motivated by professional advancement. The student population at UB is diverse ethnically, racially, and in age, attracting a high proportion of both first-generation degree-seekers and first-generation citizens: all qualities prized in the cyber security field.

As a degree housed primarily within the business school, it also fits the Merrick School of Business' mission to use our urban education hub to offer practical, career-minded and globally engaged business education that inspires professional and entrepreneurial growth. The location of the campus next to Penn Station provides easy access both to students and to industry expertise throughout the Baltimore-DC region.

In addition to the expertise of the business school faculty, the program will draw on the inter-disciplinary expertise available from the Colleges of Public Affairs and of Arts and Sciences and will extend and complement the existing programmatic capacity at UB in the area of cyber, including:

- B.S. in Applied Information Technology (Information Security and Assurance track)
- B.S. Information Systems and Technology Management

- M.S. in Forensic Science – High-Tech Crime
- MBA specialization in Cyber Security and Organizational Resilience

Building out programmatic capacity in cyber across UB will also enable the University to pursue certifications such as National Center of Academic Excellence in Information Assurance / Cyber Defense status from the National Security Agency and the Department of Homeland Security. While there are other institutions in Maryland with NSA certifications, cyber fields remain in high demand, particularly in Maryland with its high concentration of government and defense industry employers.

B. Regional and Statewide Needs as Identified in the State Plan

The State's 2017-2021 postsecondary education plan, *Increasing Student Success with Less Debt,* points out that most students are not traditional college students and that higher education has to meet the needs of this growing segment of students in higher education. The University of Baltimore has historically focused its programming, both undergraduate and graduate, on professionally ambitious students who are often working while attending school. UB endeavors to make its education affordable and as a public institution, maintains a reasonable cost for most students. This 30-credit master's degree will not charge premium rates and will schedule courses compatible with working adults.

One of the three thematic pillars of the current State Plan is innovation, with strategies directed at workforce readiness, research partnerships, and developing a culture of experimentation. This program uses innovative methods to extend the reach of students' educational and professional opportunities. It specifically notes the need for more cyber security workers in Maryland, placing special emphasis on workforce development as an element of economic growth and vitality. Its unique interdisciplinary structure will equip students to solve problems using a variety of lenses—technical, managerial, and psychological. The program will provide advanced professional education for individuals working in cyber security in the region's government agencies and contract organizations as well as private sector businesses who are moving into management ranks, and defense and military cyber specialists moving into industry positions.

C. Evidence of Market Supply and Demand in the Region and State

The national and regional demand for technical cyber security experts in the USA has been well documented, but there is now recognition of a growing need for graduate education for mid-career technical specialists as they advance into more senior organizational roles. This proposed program aims to serve primarily this population: those who have some technical skills already and who seek to advance in management, whether moving from the military to the private sector or moving from a technical position to a more senior management position within the private or government sector.

UB commissioned the Educational Advisory Board (EAB) to prepare an analysis of demand for cyber management jobs. Their analysis shows regional employer demand for master's-level cyber management professionals increased 68 percent between late2013 and early 2017 (i.e., 340 to 570 job postings per year), but in the last year the number has almost doubled, to over 1000 jobs[1].

The cybersecurity job market is thriving and continues to grow rapidly, particularly in the greater Washington D.C.-area. Burning Glass reports that cybersecurity job postings have grown 74% from 2007-2013—twice as fast as all IT jobs. On average, cybersecurity salaries offer a premium of over $15,000 over the salaries for IT jobs overall[2].

The *Baltimore Business Journal* reported last year that "more than 200,000 U.S. cybersecurity jobs are currently unfilled, and the shortage is projected to grow to more than 1.5 million unfilled positions by 2019. The talent shortage is particularly an issue for Maryland, which has more than 12,000 IT and cybersecurity companies."[3] Many of these companies are small and support larger businesses or agencies like the National Security Agency and the U.S. Cyber Command. The Maryland Department of Labor, Licensing and Regulation issued EARN (Employment Advancement Right Now) grants last November to target cyber and green industries. As the sector grows, more management positions within the cyber space will be needed and for companies of varying sizes.

The Bureau of Labor Statistics Occupational Outlook Handbook does not list cyber security managers per se. Computer and information systems manager openings are expected to grow faster than average (at 12%), with median wages at over $139,000.[4] This more general category, which includes various kinds of project managers, is broad enough to include cyber security managers.

The rapid growth in the sector and the increasingly clear impact on business and government points to a demand for an AACSB-accredited, high-quality MS in Cyber Security Management program in the state of Maryland. We respectfully suggest that we have the expertise and resources to administer such a program.

References

1. Data Snapshot: Employer Demand for Master's-level Cyber Management Professionals. Educational Advisory Board, 2016. *(Agreement with EAB does not allow UB to have this published statewide but can be made available to MHEC upon request.)*
2. Burning Glass. http://burning-glass.com/research/cybersecurity/
3. "Maryland cyber group aims to decrease number of unfilled industry jobs," Baltimore Business Journal. https://www.bizjournals.com/baltimore/news/2017/08/22/maryland-cyber-group-aims-to-decrease-number-of.html
4. https://www.bls.gov/ooh/management/computer-and-information-systems-managers.htm

D. Reasonableness of Program Duplication

Given the large market demand for a wide variety of positions in the cybersecurity space, and given the specifically interdisciplinary nature of the proposed program, there is no persuasive evidence that this proposed degree duplicates any of the cyber master's degrees offered in Maryland. Consequently, there should be no adverse effect on programs from other schools. The proposed UB program is unique in its inter-disciplinary focus and builds on an existing inventory of expertise available at UB, particularly

in business, psychology and criminal justice. These characteristics will be leveraged to create a unique academic program suited to the broadening cyber job market, particularly in Maryland.

According to the State Program Inventory, the schools noted below are approved to offer graduate cyber degrees of some kind in Maryland:

Analysis of UB Program vs. Capitol Technology University

Capitol Technology University has three graduate degrees in cyber security, none of which have the interdisciplinary focus of UB's proposed program. The two master's degrees offered at Capitol are an MS in Cyber Analytics and an MS in Cyber and Information Security, and Capitol offers a DSc in Cybersecurity. All are online degrees, although the DSc requires students to come to campus twice a In terms of curriculum it is focused tightly on information assurance, with elective streams in network engineering, project management and writing, and software assurance. There is a course on cyber security principles that covers "the overarching security architectures and vectors of information assurance from a management perspective", but there are no courses on general business competencies such as leadership or financial performance, nor is there an inter-disciplinary focus including criminal justice or psychology. The MS in CIS is focused primarily on preparation for mid - management careers within the information systems security role (such as information systems security office or security manager), although it also lists CIO and CSO as destination jobs, so in that respect it overlaps with this program. But the core courses and elective pathways are distinct from the proposed UB program.

The MS in Cyber Analytics has minimal overlap with the data analytics theme available in this program, with courses that cover specific applications such as securing healthcare information or mobile medical devices (not business or financial analytics applications). There is no coverage of accounting, management, leadership, cyber crime or psychology. A list of the core courses for the MS in CIS shows how different the curricula are: Access and Identity Management, Secure Information and Identity Management, Vulnerability Management, Healthcare Info Systems Security, Mobile Device/Application Security, Web Analytics, Analytics and Decision Analysis, Applied Statistics and Visualization for Analytics, and Big Data Warehousing and Analytics Systems.

Analysis of UB Program vs. Hood College MS in Cyber Security

The Hood College program is located within the Computer Science and Information Technology Department. The program does not assume a technical background (though it is preferred), and much of the program is dedicated to programming. There are no courses in management, accounting, or psychology. There are courses in programming, hardware, and systems engineering. The post-baccalaureate certificate (PBC) offered at Hood is within this master's degree, and the same issues apply.

Loyola College PBC – appears to be inactive per Loyola website (program not listed)

Analysis of UB Program vs. Morgan State University programming

Morgan State has the following graduate offerings in the area of cyber security:

1. Post-Baccalaureate Certificate in Cyber Security (Graduate)
2. Master of Science in Electrical Engineering with a Concentration in Signal Intelligence (Graduate)
3. United States Navy/ Morgan State University Master of Engineering (ME) in Cyber Engineering

The Morgan offerings are not duplicative with the proposed program as they have a fundamentally different disciplinary approach. All three programs focus on technical cyber security topics, particularly network security or signals intelligence. They are also offered out of the engineering school (all are EEGR courses), rather than their business school. The only managerial course is EEGR583 Introduction to Security Management. The Cyber Engineering program is open only to those employed by the Navy.

The proposed UB Master of Science (MS) in Cyber Security Management program is quite distinct from these offerings. It has a business focus, preparing students for senior management and leadership positions in information security, as well as providing exposure to a wide and inter-disciplinary set of skills and knowledge that are important in understanding how cyber security fits into the wider functioning of a business, particularly at a strategic level. The focus is on knowledge of leadership, strategy and information security management, as well as incorporating important inter-disciplinary perspectives from criminal justice and psychology. There is no overlap in content with the offerings from MSU.

Analysis of UB Program vs. UMES

The University of Maryland Eastern Shore offers a master's degree in Cyber Engineering. This program is entirely online and consists of five six-credit topics courses. It is narrower in scope and has a different delivery mechanism.

Analysis of UB Program vs. UMBC

UMBC offers several specializations in the area of cyber management through its master's in professional studies:

- Master's of Professional Studies: Cybersecurity (30 credits)
- Post-Baccalaureate Certificate in Professional Studies: Cybersecurity Strategy and Policy (12 credits)
- Post-Baccalaureate Certificate in Professional Studies: Cybersecurity Operations (12 credits)

Many of the courses in these offerings are related to technological issues such as firewall design and coding best practice. There is some overlap in topics in the area of risk assessment, cyber security operations management, and cyber law, but the UMBC programs do not have the inter-disciplinary

focus of the proposed program. Their focus is primarily from an information systems and computer science perspectives: there is no leadership, analytics, financial expertise, or psychology content. Further, the degree is an MPS, a general program, rather than a program approved specifically for cybersecurity.

Analysis of UB Program vs. UMCP

The University of Maryland is very active in cyber security and houses the Maryland Cybersecurity Center (MC2), but their offerings are not focused on cyber management and are a collaboration of the School of Engineering, the College of Computer, Mathematical and Natural Sciences, and the Institute for Advanced Computer Studies.

Analysis of UB Program vs. UMUC Programs

UMUC has several program offerings in cyber security, but only one with a focus on management issues: the MS in Cyber Security Management and Policy. From the UMUC Program Website (http://www.umuc.edu/academic-programs/masters-degrees/cybersecurity-management-policy-ms.cfm):

> *"The Master of Science in cybersecurity management and policy at University of Maryland University College can help you gain the tools you need to join the management track in cyber security so that you can establish, implement, and oversee a cyber security policy structure for an organization. Learn how to create a security approach that combines technology, governance, and compliance perspectives. Gain advanced knowledge in organizational structures, communication, operational business processes, and the legal framework for cyber security policy.*

The program consists of 6 x 6 credit courses:

- CBR600 communications, problem solving and leading in cybersecurity
- CMP610 foundations in cybersecurity management
- CMP620 organizational cybersecurity management
- CMP630 public sector cybersecurity management
- CMP640 international cybersecurity management
- CYB 670 capstone

Course descriptions suggest the program is focused on governance and policy, applied to different sectors both public and private. In terms of the management of organizational security, our program differs in its broad and inter-disciplinary focus. Specifically, the UMUC program has no apparent coursework on financial operations, analytics, forensics, or psychology. Listed topics include business process design, operations management, organizational structures, communication, and a digital framework for cyber.

We believe the inter-disciplinary nature of our program is a point of distinction. We give a grounding in analytics, increasingly important in cyber management, and we bring a strong interdisciplinary focus, particularly in psychology which appears to be absent from any other cyber management program in MD. This interdisciplinary focus gives technical personnel a broader appreciation of their field in addition to preparation for advancement.

Analysis of UB Program vs. Towson Programs

Towson has two programs in this area. One is an Information Security & Assurance Post-Baccalaureate Certificate. This certificate is focused on securing the software development process and network security, and hence has a technical cyber security focus.

The second is an M.S. in Integrated Homeland Security Management, which is an online-only program. The specializations in Information Assurance and Security Policy have some limited management coverage, specifically leadership and risk management. Their overall focus however is on securing critical infrastructures and wider physical security concerns such as bioterror preparedness, which is a very different focus than the proposed program.

Analysis of MS in Cyber Security Management Degree vs.
the UB MBA Specialization in Cyber Security & Organizational Resilience

While the proposed master's program makes use of a number of existing UB MBA courses, the program has an identity distinct from the MBA program. The MBA is a generalist degree, designed to take students from a wide variety of backgrounds, and confer skills and knowledge from all of the major areas of business. The MS in Cyber Security Management is designed for students with technical security backgrounds, and provides both a deeper understanding of the information / cyber security field, and the skills needed to advance through an organization to leadership positions such as CSO and CISO (Chief Security Officer, and Chief Information Security Officer).

Relevance to High-Demand Programs at Historically Black Institutions

As mentioned above, Morgan State has program offerings in cyber security but they are housed within the school of engineering, not the business school, and are focused on technical cyber security topics such as signals intelligence. The proposed program is a business-focused, inter-disciplinary program that focuses on managerial competencies such as leadership, managing human behavior and decision making, as well as information security management issues such as governance and business continuity. There is no overlap in content area.

E. **Relevance to Identity of Historically Black Institutions**

Cyber security is not the unique domain of any HBI. Morgan State University's programming in cyber security, as mentioned above, is technical-/ engineering-based rather than management-focused, is not run out of the business school, and does not take the inter-disciplinary approach of the UB program.

F. **Adequacy of curriculum design & delivery to related learning outcomes consistent with Regulation**

1. Provide a list of courses with title, semester credit hours and course descriptions, along with a description of program requirements.

The program curriculum can been seen in the figure below.

MS in Cyber Security Management

	Leadership & Human Behavior	Decision Making / Analytics	Business Fundamentals	Ethics / Law	Information Security Mgmt
Foundation (3)		Opre 505+506 Stats I+II			
Core (19.5)	Mgmt 605 (1.5) Leading with Integrity	Opre 605 (1.5) Business Analytics	Acct 505 (1.5) Accounting Essentials	PSCS601 (3) Legal Issues in High Tech Crime	Inss 605 (3) IT for Bus Transformation
	Appl 603 (3) Learning & Cognition				Inss 703 (3) Principles of Info. Sec Mgmt
	OPM 615 (3) Innovation & Project Mgmt				
Electives (7.5)	Mgmt 615 (3) Managing in a Dynamic Env. Mgmt 730 (3) Leadership, Learning & Change	Inss 611 (1.5) Data Science Toolkit I Inss 612 (1.5) Data Science Toolkit II	Acct 601 (3) Forensic Acct Principles	Acct 604 (3) Litigation Support Acct 701 (3) Accounting Ethics	
	Appl 641 (3) Organizational Psychology Appl 642 (3) Motivation, Satisf. & Ldrsp	INSS 722 Visual Business Intelligence	Inss 621 (1.5) Digital Innovation Inss 622 (1.5) Digital Transformation		
Capstone (3)	INSS 753 (3) Info Sec & Bus Continuity				

The program is a 30-credit degree that can be completed through 30 credits of coursework. The program focuses on 5 areas of competence:

1. Leadership and human behavior
2. Decision making and analytics
3. Business fundamentals
4. Ethics and Law
5. Information Security Management

The program requires no new courses to be created, as it leverages courses offerings already in place, although there is scope to develop additional specialized electives. The structure and course offerings are detailed below.

Foundation (3 credits, waivable):

OPRE 505 Fundamentals of Statistics (1.5)
Emphasizes applications of descriptive statistics in business. Topics include basic probability concepts, summary measures of location and dispersion, discrete and continuous probability distributions,

sampling distribution of mean, and introductions to confidence interval estimation and hypothesis testing. Excel-based software is used for computer implementation. Prerequisite: graduate standing.

OPRE 506 Managerial Statistics (1.5)
Emphasizes applications of inferential statistics in business. Topics include confidence interval estimation, hypothesis testing, analysis of variance, simple linear regression and an introduction to multiple regression. Excel-based software is used for computer implementation. Prerequisite: OPRE 505.

Core Courses (19.5 credits):

ACCT 505 Accounting Essentials (1.5)
Introduces students to the basics of corporate financial reporting and financial statement analysis from the manager's perspective. Emphasizes the analysis of financial statements and provides an overview of U.S. Generally Accepted Accounting Principles (GAAP) and International Financial Reporting Standards (IFRS) rules for most critical accounting items. Prerequisite: graduate standing.

APPL 603 Learning and Cognition (3)
Study of the major theories and models of human learning from both the traditional behaviorist perspective and the contemporary cognitive perspective and an experiential overview of how people acquire, store and use information. Theoretical and empirical information is applied to the understanding of human behavior in a wide variety of settings. Prerequisites: None.

FSCS 601 Legal Issues in High Technology Crime (3)
Examines the general regulations, general and computer-related law, and ethics and business policies associated with high technology crime. Areas of major focus include description of legal issues facing management and administration, traditional search and seizure as well as privacy issues, manager and supervisor responsibilities, criminal issues and definitions, chain of custody and ethical considerations. Problem-oriented course that focuses on applying the holdings of cases and analyses of statutes to different criminal fact patterns. Prerequisites: None.

INSS 605 IT for Business Transformation (3)
Examines the key roles that information systems and technologies play in the current business environment as well as the disruptive and innovative nature of information systems in promoting the fundamental transformation of industries, businesses and society. Covers current major issues in the field of management of information systems, such as social computing, cybersecurity, big data and mobile technologies. Prerequisites: graduate standing.

INSS 703 Principles of Information Security Management (3)
Awareness and management of information security has become critical to the management of any organization. This course focuses on the need for businesses to adapt to the changing security landscape, and provides an introduction to the different domain areas in information security from a managerial perspective. Topics will include security governance, legal regulations and compliance, environmental security, operations security, access controls, network security, disaster recovery response, and cryptography. Prerequisites: INSS 605.

MGMT 605 Leading with Integrity (1.5)
Focuses on leadership, integrity and core management principles. Provides an overview of concepts and practices essential to managerial effectiveness, including developing a vision for the organization in a

complex business environment, setting objectives, planning, motivating others, managing for results, and a grounding in ethics at the individual and organizational level. Prerequisite: graduate standing.

OPM 615 Innovation and Project Management (3)
Covers the essentials of innovation and project management from project selection through implementation, monitoring, control and termination. Topics covered include: product/process innovation, project identification, risk and uncertainty in project management, project planning and budgeting, selecting the project team, resource allocation, implementation and control, and project evaluation and termination. Prerequisite: OPM 505 or permission of instructor.

OPRE 605 Business Analytics (1.5)
Explores business analytics and its applications to management decision-making for a range of business situations. Covers problem structuring; big data; data mining; optimization; computer simulation; decision analysis; and predictive modeling. Prerequisite: OPRE 505 and OPRE 506 or permission of the M.B.A. program director.

Electives (7.5 credits)

ACCT 601 Forensic Accounting Principles (3)
Provides an overview of the field of forensic accounting, focusing on the roles, responsibilities and requirements of a forensic accountant in both litigation and fraud engagements. Examines basic litigation and fraud examination theory, identifies financial fraud schemes, explores the legal framework for damages and fraud and damage assessments and methodologies, and reviews earning management and financial reporting fraud. Other topics include computer forensics and corporate governance and ethics. Actual litigation and fraud cases are used to highlight the evolving roles of forensic accounting. Pre-requisite: ACCT 505 or equivalent.

ACCT 604 Litigation Support (3)
Addresses the relationship between the forensic accounting professional and the litigation process in which he or she may play a role. Specifically, this course covers the litigation process, the legal framework for damages and fraud, damage assessment methodologies, issues related to the presentation of evidence through expert testimony, practices used in supporting divorce cases and basic rules of evidence as they apply to forensic accountants. Prerequisite: ACCT 505 or equivalent.

ACCT 701 Accounting Ethics (3)
Considers business ethics issues within an accounting context from a multiple stakeholder perspective. Ethical theories, codes of ethics relevant to accountants, corporate governance and professional and corporate social responsibility are covered. The course emphasizes the application of concepts such as professionalism, integrity, independence and objectivity to individual decision-making. Prerequisite: graduate standing.

APPL 641 Organizational Psychology (3)
Studies how principal theories and empirical findings from research in organizational psychology are used to improve employee performance and satisfaction. Emphasizes the interactive effects of situational and individual difference variables as they influence organizational behavior. Overview includes motivation, leadership, employee morale, group dynamics and interpersonal communication. Students apply theoretical and empirical findings to solutions of work-related problems in case studies. Lab fee may be required.

APPL 642 Motivation, Satisfaction And Leadership (3)
Critical and in-depth examination of the research evidence for theories of leadership and job satisfaction. Using motivation as a central concept, students gain an understanding of how group dynamics and personal, environmental and cultural factors influence organizational behaviors. Students work in teams to solve performance-related problems presented in case studies. Lab fee may be required. Prerequisite: APPL 641 or approval of program director.

INSS 611 Data Science Toolkit I (1.5)
This course will introduce the basis of using the python programming language in data science, specifically to collect and manipulate data in preparation for exploratory data analysis and prediction. No prior programming experience is required. Topics will include python data structures, program logic and libraries, as well as data wrangling and data management. Types of data sources covered will include databases as well as unstructured data sources such as social media feeds. Prerequisites: graduate standing.

INSS 612 Data Science Toolkit II (1.5)
The effectiveness of business analytics depends on the quality of the data fed into the analytics models used. Data scientists can spend as much as 60% of their time cleaning and organizing data. This course focuses on preparing data for analytics tasks, to improve the accuracy and reliability of the results. Using python students will learn to "wrangle" (clean, transform, merge and reshape) data. Techniques will include data parsing, data correction, and data standardization. Prerequisites: INSS 611.

INSS 621 Digital Transformation (1.5)
Digital technologies are playing a transformative role in the modern world. The changes associated with digital innovations such as social media, block-chain technology and smart embedded devices are rapidly disrupting a variety of industries across the globe and challenging institutions, organizational structures, and most importantly, the skillset needed for a successful workforce. This course focuses on bleeding-edge technologies and digital business transformation. It enables students to understand the challenges and opportunities of the dynamic complex and disruptive technological business environment of the digital age. Prerequisites: INSS 605.

INSS 622 Digital Innovation (1.5)
The digital revolution is constantly challenging businesses and managers to adapt to new realities. Many organizations are establishing market leadership in today's competitive environment by mastering digital innovation. This course is designed to assist students in understanding that the fundamental nature of digital innovation is not about information technology, but is about thinking differently about how to organize to create value. It aims to equip students to competently identify technological and organizational opportunities, lead digital initiatives and develop new business models for existing and emerging organizations. Topics include digital disruption and innovation, digital platforms, digital business models and digital product and service development. Prerequisites: INSS 605.

INSS 722 Visual Business Intelligence (3)
This course will introduce students to the use of data visualization and visual business intelligence in a business environment. Students will develop a framework and language for analyzing and critiquing the visualization of data, and learn to use data visualizations to effective support decision making. Topics will include data abstraction and validation, and how to handle different types of data, dataset and attribute types. Students will use software tools to create visualizations. Prerequisites: INSS 605.

MGMT 615 Managing in A Dynamic Environment (3)
Covers the processes and necessary skills for leading and managing people in organizations that compete in dynamic environments. Emphasizes leading and motivating diverse employee populations in global organizations, and human resource management issues, including evaluation, rewards, and employment law. Prerequisites: MGMT 605 or MGMT 600.

MGMT 730 Leadership, Learning and Change (3)
Based on the idea that the deeper we go into the exploration of organizational leadership, learning and change, the more we need to deal with the dimensions of the sense-making, connection-building, choice-making, vision-inspiring, reality-creating roles of leaders. The course involves a series of workshops designed to help students learn something that cannot be taught: leading, learning and changing "from within." Readings, assignments and Web forum interactions are designed to inspire "practices of deep inflection": storytelling, historical inquiry, reflective reading and writing, dialogue and action research. Prerequisites: graduate standing.

Capstone Course (3 credits)

INSS 753 Information Security and Business Continuity (3)
This course focuses on information security at a strategic level, particularly information security governance and risk management, and business continuity. The key issues associated with protecting business information assets will be examined, including how risk and security assessments should be done in terms of impact on systems, staff, reputation and market share. Topics will include information security management, disaster recovery response, governance and compliance frameworks, and information security policy. Prerequisites: INSS 605.

2. **Describe the educational objectives and intended student learning outcomes.**

The MS in Cyber Security Management has the following program Learning Goals and corresponding Student Learning Objectives:

Goal 1: Analytical and Critical Thinking Skills—Graduates will possess the analytical and critical thinking skills needed by information / cyber security professionals.

> **Learning Objective 1.1:** Students will understand and apply the concepts surrounding the regulatory environment of different business sectors with respect to information security.
>
> **Learning Objective 1.2:** Students will analyze data and interpret their findings to identify information security issues such as fraud or security breaches.

Goal 2: Information Analysis – Graduates will use appropriate methods from a variety of disciplines in order to identify and mitigate business risk and ensure business continuity.

> **Learning Objective 2.1:** Students will be able to define the information needs pertaining to a strategic business problem arising from cyber security issues.

Learning Objective 2.2: Students will demonstrate the ability to analyze and suggest changes to business continuity processes.

Goal 3: An Ethical Perspective—Graduates will incorporate ethical considerations in their decision-making.

Learning Objective 3.1: Students will identify and analyze ethical dilemmas raised by cyber security issues and recommend appropriate resolutions.

Goal 4: Effective Communication Skills—Graduates will have the skills to communicate both tactical and strategic information security problems and solutions persuasively, professionally, and in a clear and concise manner.

Learning Objective 4.1: Students will prepare effective written reports, using appropriate data, analysis, and conclusions.

Goal 5: Leadership—Graduates will have the skills to lead an organization in its preparedness and response to cyber security threats.

Learning Objective 5.1: Students will analyze the factors and behaviors associated with effective leadership.

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

Not applicable as this is a graduate program

4. **Identify any specialized accreditation or graduate certification requirements for this program and its students.**

The primary home of the proposed degree, UB's Merrick School of Business, is accredited by AACSB, the international accrediting body of choice for schools of business. Some courses in the proposed program will be available online, and AACSB expects institutions to demonstrate assurance of learning comparability across platforms.

If contracting with another institution or non-collegiate organization, provide a copy of the written contract.

Not applicable

G. Adequacy of Articulation

Students with an undergraduate degree in information technology or related discipline, and experience in the cyber security industry should be well prepared to complete this degree.

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

1. 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 majority of courses in the MS in Cyber Security Management will be taught by full-time faculty.

From the Merrick School of Business

- **Anil Aggarwal,** professor, received a Ph.D. from the University of Houston. His research and teaching interests are in the areas of business intelligence, databases, could computing and decision making among distributed groups. He has edited books on cloud computing and big data.
- **Regina Bento**, professor, has a Ph.D. from the Sloan School of Management at MIT, and an MD from the Federal University of Rio de Janeiro. Her teaching interests include leadership and organizational behavior. Her research interests include performance appraisal and rewards, stigma, leadership, and management education.
- **Danielle Fowler,** associate professor, received a Ph.D. from Swinburne University in Australia. She is the chair of the Department of Information Systems and Decision Science. Her research and teaching interests include cyber education, e-commerce and requirements engineering.
- **Rajesh Mirani,** associate professor, received a Ph.D. from the University of Pittsburgh. His research and teaching interests cover management information systems, including applications to healthcare and business-information technology alignment, as well as governance and public sector information technology initiatives.
- **Joel Morse,** professor, earned his Ph.D. at the University of Massachusetts at Amherst. His research and teaching interests are in the areas of investments, corporate finance, and business valuation, with a particular focus on goodwill impairment, volatility investing and derivatives. He has been a course designer of online graduate teaching material and courseware since 1998.
- **Eusebio Scornavacca,** associate professor, received his Ph.D. from Victoria University of Wellington. He holds the Dean Clifford James Chair for Distinguished Teaching and the John and Margaret Thompson Professorship. His research and teaching interests are in the areas of mobile and ubiquitous information systems, disruptive innovation, and information security as a component of digital business.
- **Jaya Singhal**, professor, earned her Ph.D. at the University of Arizona. She has won the USM Board of Regents faculty award for scholarship, and she holds the Frank Baker Chair for Research Excellence. Her research focuses on topics in Management Science, Supply Chain Management, and Operations Management.

- **Kalyan Singhal,** professor, has a D.B.A from Kent State university. He is one of the founders of the Production and Operation Management Society (POMS), and serves as the Editor-in-Chief of the Production and Operation Management Journal. His research interest is in Trade-and-Innovation Dynamics and its science.
- **Lisa Stickney,** associate professor, received her Ph.D. from Temple University. Dr. Stickney's research interests include anger in organizations, emotional contagion, gender studies, and management pedagogy. Her research has been published in Human Relations, Sex Roles: A Journal of Research, The Journal of Management Education and in Research in Emotions in Organizations among others.
- **Lourdes White,** professor, received a doctoral degree from Harvard University in business with an accounting concentration. Her research and teaching interests are in the areas of management accounting and control, including performance management, cost and control systems, and accounting ethics. She has also published in the areas of quality assurance and student engagement in online education, and has presented her work on the scholarship of online education at national and international academic conferences.

From the College of Public Affairs:

- **Pat Hall**, lecturer, is an attorney and director of the MS. in Forensic Science and High Tech Crime. Attorney Hall has more than 30 years of experience with the legal process and criminal investigation of cybercrime in both corporate and public-sector organizations. Her expertise includes the CFAA and other business and organizational regulations. She has participated in various incident response teams representing the legal implications and evidence preservation.
- **Debra Stanley**, professor, earned her Ph.D. from the University of Maryland. She is currently executive director of the School of Criminal Justice. Her research focuses on victimology, domestic violence, substance abuse and crime, violence prevention and program evaluation. Her teaching areas include Research Techniques in Criminal Justice, Advanced Criminology, and Administration of Justice.

From the College of Arts and Sciences:

- **Sharon Glazer**, professor, earned her Ph.D. from Central Michigan University. She is currently Chair of the Division of Applied Behavioral Sciences, and an affiliate Research Professor at the University of Maryland Center for Advanced Study of Language (CASL) and Department of Psychology. She is a cross-cultural organizational psychologist who studies the role of culture in individuals' organizational ABCs (affects, behaviors, and cognitions), changes in (organizational and national) cultures due to domestic policies in a globalizing world, and differences and similarities between (national and organizational) cultures on individuals, teams, and organizations' ABCs.

- **John Donahue**, assistant professor, earned his Psy.D from LaSalle University. His area of interest is the field of emotion regulation, and his expertise includes a clinical internship in the Federal Bureau of Prisons and research fellowship at the Portland VA Medical Center.
- **Thomas Mitchell,** associate professor, earned his Ph.D. from Virginia Commonwealth University. His expertise is in the area of industrial and organizational psychology, and his research has focused on understanding how applicant faking on personality tests affects job performance.

A mapping of faculty to course offerings is below:

Foundation (3 credits, waivable)		**Faculty**	**Status**	**Qualifications**
OPRE 505	Fundamentals of Statistics (1.5)	Jaya Singhal	Professor	Ph.D., Univ of Arizona
OPRE 506	Managerial Statistics (1.5)	Jaya Singhal	Professor	Ph.D., Univ of Arizona
Required Core (19.5 credits)				
ACCT 505	Accounting Essentials (1.5)	Jessica Kaufman	Adjunct	MBA Univ Baltimore, CPA
APPL 603	Learning And Cognition (3)	John Donahue	Assist Prof	Psy.D. LaSalle Univ
FSCS 601	Legal Issues in High Technology Crime (3)	Pat Hall	Lecturer	JD, Esq. Practicing Attorney,
INSS 605	IT for Business Transformation (3)	Rajesh Mirani	Assoc Prof	Ph.D. Univ of Pittsburgh
INSS 703	Principles of Information Security Management (3)	Eusebio Scornavacca	Assoc Prof	Ph.D. Victoria Univ (NZ)
MGMT 605	Leading with Integrity (1.5)	Lisa Stickney	Assoc Prof	Ph.D. Temple University
OPM 615	Innovation & Project Management (3)	Kalyan Singhal	Professor	D.B.A Kent State
OPRE 605	Business Analytics (1.5)	Jaya Singhal	Professor	Ph.D., Univ of Arizona
Elective Courses (7.5 credits)				
ACCT 601	Forensic Accounting Principles (3)	Robert Carter	Adjunct	MS. Acct Bus Advis, CPA
ACCT 604	Litigation Support (3)	Joel Morse	Professor	Ph.D. Umass Amherst
ACCT 701	Accounting Ethics	Lourdes White	Professor	D.B.A. Harvard
APPL 641	Organizational Psychology (3)	Thomas Mitchell	Assoc Prof	Ph.D. Virginia Commonwealth Univ
APPL 642	Motivation, Satisfaction And Leadership (3)	Thomas Mitchell	Assoc Prof	Ph.D. Virginia Commonwealth Univ
INSS 611	Data Science Toolkit I (1.5)	Danielle Fowler	Assoc Prof	Ph.D. Swinburne Univ (Aus)
INSS 612	Data Science Toolkit II (1.5)	Danielle Fowler	Assoc Prof	Ph.D. Swinburne Univ (Aus)

INSS 621	Digital Transformation (1.5)	Eusebio Scornavacca	Associate Prof	Ph.D. Victoria Univ (NZ)
INSS 622	Digital Innovation (1.5)	Eusebio Scornavacca	Associate Prof	Ph.D. Victoria Univ (NZ)
INSS 722	Visual Business Intelligence (3)	Anil Aggarwal	Professor	Univ of Houston
MGMT 615	Managing in a Dynamic Environment (3)	Regina Bento	Professor	Ph.D. MIT; MD Federal Univ of Rio de Janeiro
MGMT 730	Leadership, Learning and Change (3)	Regina Bento	Professor	Ph.D. MIT; MD Federal Univ of Rio de Janeiro
Capstone (3 credits)				
INSS 753	Information Security And Business Continuity (3)	Danielle Fowler	Assoc Prof	Ph.D. Swinburne Univ (Aus)

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

As the program uses existing course offerings, the program has sufficient library resources through the Bogomolny Library to meet its needs. The UB library is a member of the University System of Maryland and Affiliated Institutions library consortium, which provides among the most robust interlibrary loan services in the country. Faculty and students have remote access to research database searches and electronic journals, and there is 24/7 reference help available. The library moved into a completely refurbished building in June of 2018.

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

The Merrick School of Business is housed in the William Thumel Business Center, a five-story academic building with the classroom and technology resources to provide courses through a variety of electronic media. Faculty all have computers, there are student computer labs, an advising center, a business incubator, and ample classrooms and faculty offices. The University uses the Sakai learning management system, which has 24/7 support from Sakai, plus support from UB's Office of Technology Services. Faculty are supported in online learning by the Bank of America Center for Excellence in Learning, Teaching and Technology.

As this program is focused on the management of cyber security, not technical proficiency, it has no requirement for specialized lab facilities. If it would suit instructors to demonstrate material in a lab setting, this can be done using the existing information systems lab space in the Merrick School (which includes a virtual lab), or the dedicated cyber security labs in the College of Arts and Sciences.

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

TABLE 1: RESOURCES:

Resource Categories	Year 1	Year 2	Year 3	Year 4	Year 5
1. Reallocated Funds[1]	N/A	N/A	N/A	N/A	N/A
2. Tuition/Fee Revenue (c + g below)	**$360,750**	**$1,103,895**	**$1,501,297**	**$1,722,739**	**$2,147,681**
a. Number of F/T Students[2]	0	0	0	0	0
b. Annual Tuition Rate[3]	$9,612	$9,804	$10,000	$10,200	$10,404
c. Total F/T Revenue (a x b)	$0	$0	$0	$0	$0
d. Number of P/T Students[4]	10	30	40	45	55
e. Credit Hour Rate[5] (3 cr)	$2,405	$2,453	$2,502	$2,552	$2,603
f. Annual Credit Hour Rate[6]	15	15	15	15	15
g. Total P/T Revenue (d x e x f)	$360,750	$1,103,895	$1,501,297	$1,722,739	$2,147,681
3. Grants, Contracts & Other External Sources	N/A	N/A	N/A	N/A	N/A
New students	10	20	20	25	25
Total students		30	40	45	50

[1]The program consists of existing courses within the MBA, MS Applied Psych, and MS Forensic Science-High Tech Crime. MS Cyber students will be integrated with students in these programs.

[2]The target market for the program is part-time students.

[3]The current rate for tuition for full-time, in-state students is used for year 1. Thereafter, a tuition increase of 2% per year is assumed. There are no program specific fees.

[4]See note 2. Enrollments projected to grow with better program identification in the market.

[5]The current tuition rate for part-time, in-state, students for 3 credits is used for year 1. Thereafter, a tuition increase of 2% per year is assumed. There are no program specific fees.

[6]Program designed/marketed for two-year completion rate. Students take 6-7.5cr/term over fall, spring, summer.

TABLE 2: EXPENDITURES:

Expenditure Categories	Year 1	Year 2	Year 3	Year 4	Year 5
1. Faculty (b + c below)	**$261,870**	**$368,445**	**$452,304**	**$461,350**	**$579,284**
a. # FTE[1]	0.5	1	1.5	1.5	2
b. Total Salary[2]	$129,000	$181,500	$222,810	$227,266	$285,362
c. Total Benefits	$132,870	$186,945	$229,494	$234,084	$293,922
2. Academic Support Staff[3]	N/A	N/A	N/A	N/A	N/A
3. Technical Support and Equipment[4]	$5,000	$0	$0	$0	$0
4. Library[5]	$0	$0	$0	$0	$0
5. New or Renovated Space[6]	$0	$0	$0	$0	$0
TOTAL (Add 1 – 6)	**$266,870**	**$368,445**	**$452,304**	**$461,350**	**$579,284**
Net Contribution: Tuition Revenue - Expenses	**$93,880**	**$735,450**	**$1,048,993**	**$1,261,388**	**$1,568,397**

[1] Year 1 FTE represents incremental FTE required to support the program. As enrollments grow, additional adjuncts will be deployed. Assume 2% growth in FT faculty salaries, fringe constant.

[2] Based on Fall 2017 FT faculty salaries plus adjunct salaries

[3] Able to accommodate growth in students with existing academic support over this time period

[4] Software: Cyber security management tools (SIEM) $5,000

[5] Library: no additional journals required

[6] Existing lab and classroom space sufficient

M. 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.

The Merrick School of Business is accredited by AACSB, which requires a self-study process and peer review of assurance of student learning. This accreditation is re-affirmed every 5 years. Faculty scholarship is also part of the review. As the proposed program will be housed and taught primarily by the Merrick School of Business, it will be incorporated into the AACSB review process, ensuring the program meets those standards.

Faculty are also evaluated through student evaluation of courses, annual review, promotion and tenure review, and post-tenure review.

The program faculty will engage in the assessment of program student learning outcomes to satisfy UB, University System of Maryland, and AACSB requirements for program review. Assessment of program learning objectives is conducted every two years, and recommendations for continuous improvement are prepared and implemented by faculty teaching in the program, under the guidance of the program director and the chair of the Department of Information Systems and Decision Science.

The associate dean of the Merrick School coordinates academic assessment for the School. UB uses TaskStream software for academic assessment to track the evaluation of student learning outcomes. The assistant provost for assessment, advising and retention, in conjunction with the Academic Core Assessment Team, oversees academic assessment processes at the university. The assistant provost provides a check to ensure that all academic assessment is on file within the software.

N. 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 University of Baltimore has a majority minority population and is one of the most ethnically and racially diverse institutions in Maryland (see http://www.ubalt.edu/campus-life/diversity-and-culture-center/diversity-profile.cfm and comparative information from the MHEC *Data Book*, 2017). The institution's entire history has been shaped by the goal of helping individuals gain the education they

need to advance professionally and personally; now as in the past, a large percentage of UB students work full- or part-time while earning a degree. This program continues in that tradition by serving working professionals in the cyber industry wanting to advance professionally.

Like all University System of Maryland institutions, UB has goals related to closing the achievement gap between races and income groups. A key factor in completion of degrees is ease of access. It is critically important to keep students enrolled if they are to graduate, both for graduate and undergraduate programs. Providing the program online will facilitate efforts to keep students enrolled in the degree program, through achievement of the CPA credential and on to the degree.

UB has also works to track its impact on social mobility. Providing this program online, and thereby helping more students earn a valuable professional credential, is aligned with UB efforts to increase the incomes and social mobility of its student population.

O. Relationship to low productivity programs identified by the Commission: If the proposed program is directly related to an identified low productivity program, discuss how the fiscal resources (including faculty, administration, library resources and general operating expenses) may be redistributed to this program.

Not applicable