April 2, 2020

The Honorable James D. Fielder, Ph.D.
Secretary of Higher Education
Maryland Higher Education Commission
6 North Liberty Street
Baltimore, Maryland 21201

Dear Secretary Fielder,

The University of Baltimore (UB) is proposing a new Bachelor of Science in Cyber Forensics (proposed CIP 43.0403 and proposed program code 2105-10). This is a 42-credit program that provides an undergraduate degree in an area of study that is already available at the graduate level at UB through the Master of Science in Forensic Science – Cyber Investigations.

This proposed program addresses an area of high need within metropolitan Baltimore, the State of Maryland, and the region. The program was developed in collaboration with community college partners and other units at UB, so students could begin the program at UB or easily transfer in from a Maryland community college and continue this educational pathway.

If you have any questions, please contact me or my staff (410-837-5243).

Sincerely,

Darlene Brannigan Smith, Ph.D.

Encl.
cc: 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

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.

- [x] New Academic Program
- [ ] New Area of Concentration
- [ ] New Degree Level Approval
- [ ] New Stand-Alone Certificate
- [ ] Off Campus Program
- [x] 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

Payment Submitted:	Payment Type:	Payment Amount:	Date Submitted:
○ Yes ○ No	◉ R*STARS ○ Check	$850	

Department Proposing Program	School of Criminal Justice	
Degree Level and Degree Type	Bachelor of Science	
Title of Proposed Program	Cyber Forensics	
Total Number of Credits	42 major in 120-credit degree	
Suggested Codes	HEGIS: 2105.10	CIP: 43.0403
Program Modality	◉ On-campus	○ Distance Education (*fully online*)
Program Resources	◉ Using Existing Resources	○ Requiring New Resources
Projected Implementation Date	◉ Fall ○ Spring ○ Summer	Year: 2020
Provide Link to Most Recent Academic Catalog	URL: http://www.ubalt.edu/academics/uploads/catalogs/19-20_undergrad_catalog/19-20UGCatalog.pdf	
Preferred Contact for this Proposal	Name: Dr. Candace Caraco (for Dr. Debra Stanley)	
	Title: Asst. Provost	
	Phone: (410) 837-5243	
	Email: ccaraco@ubalt.edu	
President/Chief Executive	Type Name: Dr. Darlene Brannigan Smith, Exec VP and Provost	
	Signature: [signature]	Date: 3/16/20
	Date of Approval/Endorsement by Governing Board:	

Revised 3/2019

UNIVERSITY SYSTEM OF MARYLAND INSTITUTION PROPOSAL FOR

X	New Instructional Program
	Substantial Expansion/Major Modification
	Cooperative Degree Program
X	Within Existing Resources, or
	Requiring New Resources

University of Baltimore

Institution Submitting Proposal

B.S Cyber Forensics

Title of Proposed Program

B. S. Cyber Forensics	**FALL 2020**
Award to be Offered	Projected Implementation Date
2105-10	**43.0403**
Proposed HEGIS Code	Proposed CIP Code
School of Criminal Justice College of Public Affairs	Debra L. Stanley, Ph.D.
Department in which program will be located	Department Contact
(410) 837-5243	ccaraco@ubalt.edu
Contact Phone Number	Contact E-Mail Address
Signature of President or Designee	Date

New Instructional Program – University of Baltimore B. S. Cyber Forensics

A. Centrality to Institutional Mission and Planning Priorities

The mission of the University of Baltimore (UB) is to offer career-focused education for aspiring and current professionals, providing the region with highly educated leaders who make distinctive contributions to the broader community. The University's vision is to be the premier regional university for career advancement, where leaders grow, thrive and learn to apply their skills for solving local and global challenges. One of the greatest challenges in our region and globally is the rapidly evolving character and reach of cybercrime.

UB's School of Criminal Justice already offers a highly regarded bachelor's degree in **Forensic Studies**, with options in police science and in forensic sciences, and a growing **Master of Science program in Forensic Science – Cyber Investigations**, which is offered both at the downtown campus and at the Universities at Shady Grove. This graduate program has attracted both professionals working in the field and those who wish to move into cyber forensics. The proposed Bachelor of Science in Cyber Forensics would both leverage the strengths of existing offerings and align with Maryland community college offerings in cyber forensics. The program fills a significant gap in cyber forensics undergraduate education in Maryland. Having been developed in collaboration with community college cybercrime, cybersecurity and cyber forensic technology programs, the B.S. in Cyber Forensics would provide the next level of education for A.A. and A.S. graduates to complete a baccalaureate degree. The proposed program is fully consistent with the UB mission and will help provide the region with needed leaders in the growing field of cyber forensics.

The first B.S. Cyber Forensics degree program beyond an associate degree in Maryland

The proposed BS in Cyber Forensics is a 42-credit major designed to provide students with a broad-based practical understanding of cybercrimes and cyber investigations. The core of the program exposes students to forensic investigation techniques and skills, computer and digital information crimes, fraudulent activities in the use of technology and digital systems, prevention and security management strategies, and legal interventions and resolutions.

It is expected that coursework in the B.S. Cyber Forensics program will enhance students' digital and technology fluency as many courses involve accessing information that is available online. In addition, students will, in some classes, learn to access online data and use software tools designed to sort and make sense of data. It is expected that such fluencies will make graduates more competitive and more marketable for professional opportunities post-graduation.

Program Requirements:

Total number of credits: 42 semester credit hours. The program requires the successful completion of 14 three-credit core courses:

Code	Course Title	Credits	Faculty
FSCS 301	Fundamentals of Cyber Forensics	3	de la Cruz/Xu/Zahadat
FSCS 310	Cyber Crime and the Law	3	Hall/Rosenblatt
FSCS 320	Operating System Forensics	3	de la Cruz/Xu/Zahadat
FSCS 325	Mobile Forensics	3	de la Cruz/Zahadat
FSCS 360	Network Forensics	3	Xu/Zahadat
FSCS 375	Scripting for Cyber Forensics	3	Zahadat/Xu/Leggette
FSCS 380	Fundamentals of Cryptography	3	Xu/Leggette
FSCS 400	Ethical Hacking	3	Xu/Zahadat
FSCS 430	Forensic Investigations	3	de la Cruz/Zahadat
FSCS 445	Forensic Data Analysis	3	Zahadat/Xu
FSCS 480*	Forensic Documentation	3	Everett/Tumosa
FSCS 482*	Moot Court	3	Hall/Rosenblatt
FSCS 487*	Field Internship in Forensic Science	3	All
FSCS 490	Forensic Incident Response-Capstone	3	All
	Total Credits	42	

**Courses already exist in the Forensics Studies – Trace Evidence degree program. Students from both programs will be enrolled in each of these three courses*

Admissions Standards: Students may begin as freshmen at UB or transfer into the program. Transfer students will be expected to have at least a 2.8 grade point average (GPA). Students with a high GPA who have completed an AA or AS in a related cyber forensics discipline will have a clear pathway to advanced studies in their fields with the addition of the Cyber Forensics bachelor's degree.

Preparation for Further Study: UB has a law school, and high GPA undergraduates may be eligible for UB's automatic admit program. And the BS Cyber Forensics graduates would directly feed into the MS in Forensic Science Cyber Investigations should they wish to pursue their education further. Accelerated study options may be available to high GPA students.

Program supports the institution's strategic goals and priorities.

The mission of the University of Baltimore assures that the university's emphasis on career-oriented education attracts students with clear professional objectives and provides them with a broad foundation of knowledge to meet the rapidly changing conditions of today's work environment, as well as equipping them with the latest skills and techniques for productive careers in the public and private sectors. The College of Public Affairs, which houses the School of Criminal Justice, seeks to prepare problem-solvers who will analyze policy and lead public, nonprofit, health-care, and third sector organizations of the future. The proposed program aligns with these institutional goals.

As part of its strategic planning process in 2018, the University developed five Signature Areas of Excellence:

- Law, Justice and Public Service
- Business and Entrepreneurship
- Media, Communications and Design
- Behavioral, Health and Human Services
- Cyber, Gaming and Technology

The proposed program in Cyber Forensics bridges the signature areas of Law, Justice and Public Service as well as Cyber, Gaming and Technology. The proposed program builds on the School of Criminal Justice's history of delivering quality forensic science and cyber investigations education.

The University of Baltimore and the College of Public Affairs excel in the preparation and the delivery of education that has practical application and prepares students for professional careers. The School of Criminal Justice is uniquely situated to provide education to students who seek careers in forensic investigations. The proposed degree program fills a significant gap in undergraduate education in Maryland. The B.S. Cyber Forensics program is a 21st-century reflection of the university's mission to impart knowledge that works and provide students an opportunity to be agents of positive change. The program supports several strategies related to the strategic plan's first goal of focusing on career-oriented professional education.

The proposed B.S. in Cyber Forensics builds on and supports each of the institutional goals set forth by the University of Baltimore and the College of Public Affairs, while also contributing to the university's projected growth goals (plan goal 4). The program will also provide opportunities for the expansion of existing degree programs by attracting students interested in forensic science who might not otherwise pursue undergraduate study at the University of Baltimore. The degree program will develop students' knowledge and skills as experts in the recognition of cybercrimes, thereby preparing them to investigate the expanding area of cyber-related criminal activity. Just as the digital world has grown, cybercrimes are one of the fasted growing areas of criminal behavior in the 21st Century.

Five-Year Funding Plan

a. Ongoing institutional administrative, financial and technical support of the program.
b. Continuation of the program for a period of time sufficient to allow enrolled students to complete the program.

As noted above, UB already offers an undergraduate degree and a graduate degree in related fields. These programs have been operating over five years, and the University is confident that this program will be sustainable. The faculty already on staff at UB can offer the BS in Cyber Forensics, and the prospective program director is tenured. That said, the program will also make additional hires through resources already identified once the program is launched. The physical facilities needed for specialized labs are also already in place. Annual technology needs are

typically funded using course fees and other discretionary funding to ensure the most up-to-date technology is afforded to students.

In addition, this program targets a key area in Governor Hogan's workforce development initiative for expanding degree programs and is approved for FY21 University System of Maryland Enhancement funding that supports that initiative. The Enhancement funds will support technology resources and personnel. AY21 personnel will include a faculty position and full-time Cyber Lab director, and in AY22 an additional faculty position will be hired. The Enhancement funding also will support ongoing technology costs: in AY21 the technology expansion will include both hardware and software updates in the labs and the installation of virtual learning environment technology. This support will facilitate the program becoming self-sustaining through enrollment before the end of year 5. As the program grows and further enrollment demands are needed to support the program, the institution's financial models are designed to support growth and high-enrolled programs. Through this model, additional lab space can be prepared as demanded by enrollments.

The job growth in this field is expected to continue to increase for the next decade. According to the US Bureau of Labor Statistics (2019), there were 112,300 jobs in the field of cyber forensics and security analysts, the job outlook for 2018-2018 is predicted to grow 32 percent, a rate much faster than the average for all occupations, which is at 5 percent. Based on the market analysis, we anticipate enrollments to increase rapidly in the first several years; and while it may taper off a bit, enrollments are expected to maintain at a robust level. The University anticipates that this program will generate enrollments for at least this coming decade.

B. Critical and Compelling Regional and Statewide Need

a) Need for 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

Maryland is one of the top employing regions for forensic science investigators in the US, with the Washington, D.C.-Baltimore metro area ranking fourth in the country (US Department of Labor's Bureau of Labor Statistics, 2019). The job market in the Maryland-Washington, DC region is expected to grow by 8 percent annually, with an annual growth rate of 270 new positions. Forensic investigators may seek employment in local, state and federal governments, corporate and private businesses, financial institutions, hospitals, schools, and non-profit organizations. Today, most organizations and governmental agency require cyber forensics experts to protect and manage cyber technology and systems. The proposed program targets a key area in Governor Hogan's workforce development initiative for expanding degree programs and has been approved for FY21 funding through the University System of Maryland to support State priorities.

The University of Baltimore has one of the state's most diverse student populations, and most students are from the great Baltimore region. The proposed program will help expand educational opportunities in this area in what is a high-demand and high-growth field. The workforce demand for an increase in the number of hires in the area of computer and digital forensic investigators surpasses the current capacity of qualified workers.

UB's program will not infringe on the ability of historically black institutions to offer high quality and unique educational programs.

Evidence that the perceived need is consistent with the Maryland State Plan for Postsecondary Education *(Student Success with Less Debt)*

The BS in Cyber Forensics can provide students with quality postsecondary education at an affordable, public education price. UB attracts a highly diverse student population and is well prepared to provide students with equitable access and to assist them in succeeding in meeting their educational goals. Goal 3 of the State Plan calls for fostering innovation in all aspects of higher education to improve access and student success. The BS in Cyber Forensics is a unique program in an exciting, cutting-edge field. As students at UB as a whole and particularly in the College of Public Affairs tend to be non-traditional students, we anticipate that this program will attract similar students. Training students in a rapid growth, high demand area would enhance UB's national recognition in providing high levels of social mobility to largely non-traditional and widely diverse students.

The curriculum for BS in Cyber Forensics was developed in consultation with programs at community colleges in Maryland. This level of consultation should ensure that the ability of students to transfer seamlessly from community college programs to the BS degree and thereby complete their education faster (State Plan strategy 6). In addition, this program could potentially provide strong students with accelerated routes through a graduate or law program.

As noted above, the program focuses on a key target in Governor Hogan's Workforce Development Initiative and was provided USM Enhancement Funding for FY21. Recognizing the need for practical experience, the BS in Cyber Forensics has a mandatory internship requirement (FSCS 487). This internship requirement will foster development of partnerships between the university, government and the private sector as these internships are developed. (cf. Strategies 7 and 8 of the State Plan).

C. Quantifiable and Reliable Evidence and Documentation of Market Supply and Demand in the region and State

1. Describe potential industry or industries, employment opportunities, and expected level of entry (*ex: mid-level management*) for graduates of the proposed program.
2. Present data and analysis projecting market demand and the availability of openings in a job market to be served by the new program.

3. 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.
4. Provide data showing the current and projected supply of prospective graduates.

The BS in Cyber Forensics program is intended for students interested in pursuing employment in government, private corporations, and nonprofit organizations who desire to advance their competencies in managing advanced technological resources to combat cyber threats, and related crime. It will qualify graduates for positions such as incident response manager, information security supervisor, cyber investigator, forensic analyst, law enforcement, private investigator, corporate security manager, and fraud manager. Job opportunities may include:

Cyber Investigator	Health Care Fraud Management
Forensic Analyst	Intelligence Analyst
Private Security Investigator	Independent or Internal Auditing
Government Accounting	Cybersecurity Investigator/Analyst
Digital Forensic Specialist	Forensic Examiner
Cyber Threat Investigator	Incident Forensics Specialist
Senior Network and Threat Specialist	Intelligence Research Specialist/ Analyst
Forensics Technician	Cyber Defense Forensics Analyst

The program, developed in consultation with the local community colleges, FBI representatives, and statewide law enforcement, is intended for members of private corporations, nonprofit organizations, and governmental agencies who desire to advance their competencies in managing advanced technological resources to combat cyber threats, and cybercrimes. Students who have not yet been employed will benefit from the expertise of other students and will be required to gain job experience in the field through a required internship.

Cybersecurity is a fast-growing market with tremendous career opportunities; cyber-crime is now the number one threat to United States national security (USDOC, 2020). As the number of large-scale data breaches and cyber-attacks continue to rise year after year, there is an increasing need for educated and dedicated cyber professionals to protect our nation, businesses, and individuals from cyber threats. In 2018, the U.S. Department of Commerce estimates that there are approximately 350,000 cybersecurity jobs currently unfilled in the U.S. Cybersecurity Analytics and Cybersecurity Ventures predict that there will be 3.5 million unfilled cybersecurity jobs globally by 2021 (Cybersecurity Ventures, 2017); these estimates are before the new field of cyber forensics and investigations fully develops and new jobs are added to the job listings. The cybersecurity unemployment rate has effectively been at zero percent for the last 8 years. Recent figures indicate that in the past 12 to 24 months, there have been 700,000 to 1 million tech job openings, with cybersecurity positions making up 32-45 percent of all US tech job openings.

Maryland is viewed as the US Headquarters for cybersecurity with more than 110,000 cyber-related jobs, and 40 government agencies with strong cybersecurity programs (Martin, 2019). Maryland leads the US in cyber employment for classified national-state jobs. According

to the Maryland Chamber of Commerce, there are currently, over 15,000 open cybersecurity jobs in Maryland.

The most recent employment data (2019) from the Bureau of Labor Statistics (BLS) affirms the demand for employees in cyber security related work, both within government and in the private sector with 112, 300 jobs available at the bachelor's degree level. The BLS predicts that the job growth rate into 2028 will increase by at least 32 percent, which is much faster than average for all occupations.

The Baltimore-Washington region has one of the highest concentrations of job opportunities in the country for computer forensics and cybersecurity related positions. The average salary for the greater Baltimore-Washington, DC-Northern VA regions, where BLS provides statistics, is over $107, 960. In Maryland, 68,000 people are employed in security-related occupations, and BLS data show that 20,516 jobs are currently vacant in Maryland alone; and another 50,000 in Virginia (Cyberseek, 2020). The Md-DC-VA region has over 14, 540 open jobs; with 2,610 of those jobs in Baltimore-Columbia-Towson, Maryland (BLS, 2019). A recent search of Indeed.com, a jobs website, indicates over 914 job openings at all levels in cyber security in Maryland, with a third of these jobs at starting salaries of $50,000 or more. Linkedin.com reported over 10,000 positions in the Baltimore-Washington region as of July 2019.

The bachelor's-level education this program provides would enable current employees at entry-level positions to move up to positions of greater responsibility and pay, and it would prepare students for professional positions in the field.

References:

Cybersecurity Ventures (2017) https://cybersecurityventures.com/jobs/
Cyberseek (2020) https://www.cyberseek.org/heatmap.html
Martin, James (2019). Top 10 Global Cybersecurity hubs for 2019. CSO – United States. (April). https://www.csoonline.com/article/3390222/top-10-global-cybersecurity-hubs-for-2019.html#slide5
Maryland Chamber of Commerce (2019) https://mdchamber.org/marylands-leading-industries/
Maryland Department of Labor (2020) https://www.dllr.state.md.us/
U.S. Department of Commerce (2020) https://www.commerce.gov/issues/cybersecurity
U.S. Bureau of Labor Statistics (2020) https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

D. 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.

The proposed program does not duplicate any other program in Maryland. It will be the only cyber forensics bachelor's degree program. There are associate degree programs at the

community colleges that will prepare students for the BS in Cyber Forensics. There is one graduate certificate program in Cyber Forensics that was recently approved at UMBC.

While there are several undergraduate bachelor's cybersecurity programs, the curriculum for the undergraduate cybersecurity programs are based on computer security and prevention of security breaches. The proposed program curriculum is based on forensic investigations and evidence collection; therefore, the program focuses on responding to criminal behavior and intentional attacks on computer and digital technology, investigating incidents, and gathering evidence that may be used in court to prosecute offenders. The BS degree program is a uniquely defined area within the forensic discipline because of its emphasis on cybercrime, particularly that which occurs within the workplace. **Currently, there are no cyber forensic bachelor's degree programs offered at any other USM institution, or any private or HBI institution within Maryland.**

2. Provide justification for the proposed program.

This is a unique program in a high-demand area of the workforce. Many of the major national security risks involve technology threats from cyber-espionage, computer and financial crimes, hacktivism, the proliferation of mobile devices, social engineering, phishing and malware, advanced persistent threats and attacks on critical infrastructures. The increasing internationalization of the world's economies, coupled with global networks, electronic commerce, foreign direct investment, and capital flows, has facilitated financial crime and other attacks. Combating cyber threats/attacks effectively requires that we educate investigators and administrators in a "multidisciplinary" manner—i.e., combining several branches of learning into a common forensic studies program - criminal justice, cyber investigations, cybersecurity, incident response management, computer technology, and law and business regulations. A degree in cyber forensics provides the knowledge and skills needed to interpret electronic data to solve crimes; it combines investigative skills with digital technology in the examination and preservation of evidence.

Civil and/or criminal investigations within businesses and public agencies require the same legal understanding and forensic evidence skills and techniques used in traditional criminal investigations. For this reason, forensics will play a critical role as an organizing concept for the development of this program because the systematic collection and presentation of evidence is critical in a court of law. However, knowledge of forensics and criminal justice investigatory techniques alone is not sufficient. We know that law enforcement as well as businesses often lack expertise within their organizations in the fields of computer technology, forensic analysis, incident response management and data privacy protection issues that hamper successful investigations. A new bachelor's degree in this area is well-justified for the State of Maryland.

E. Relevance to High-demand Programs at Historically Black Institutions (HBIs)

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

The proposed program does not duplicate or compete with the implementation or maintenance of high-demand programs at HBI's.

F. Relevance to the Identify of Historically Black Institutions (HBIs)

1. Discuss the program's potential impact on the uniqueness and institutional identities and missions of HBIs.

It does not have any potential impact on the uniqueness and institutional identities and missions of HBIs.

G. Adequacy of Curriculum Design, Program Modality, and Related Learning Outcomes (as outlined in COMAR 13B.02.03.10)

1. Program Establishment and Faculty Oversight

Faculty from the highly successful Master of Science in Forensic Studies—Cyber Investigations met with representatives of Maryland Community Colleges that offer Associate degrees or certificates in Cyber Forensics to design a transfer program at a four-year institution for graduates of these community college programs. [1] This new baccalaureate program will be overseen by the program director of the graduate program and other faculty devoted to both the MS Program in Cyber-Investigations and the Bachelor of Science in Forensic Studies.[2]

The Cyber Forensics program consists of core courses in forensic investigative techniques, cyber investigations, incident management, data protection, legal aspects of management, infrastructure protection and security, computer and digital forensics, forensic investigations, preservation of evidence, cybercrimes, and forensic data analytic techniques. While all courses will be taught in traditional classrooms, the program's applied pedagogy features an interactive virtual learning environment that provides students access to course scenarios and software both in and out of the traditional classroom experience.

2. Educational Objectives:

The major offers an opportunity for students who are interested in advanced cyber forensics to develop knowledge and skills that will allow them to compete for careers in government and private sector corporations for highly evolving jobs in the cybersecurity field.

The degree program includes General Education and Graduation Requirements, each of which has standard student learning outcomes, which are assessed on a regular schedule. The General Education Council, a committee of the University Faculty Senate, assesses courses that are to meet general education requirements. Graduation requirements may be assessed in one of two

[1] As one example, see Howard Community College Programs in Cyber-Forensics (https://www.howardcc.edu/programs-courses/programs/cyber-forensics-tech-aa/index.html)

[2] Courses currently offered in the BSFS program that teach basic principles and skills used in other areas of forensics (such as Moot Court, Forensic Documentation) will be included in the new program.

ways: either by the General Education Council or by the program. Capstones, for example, are reviewed by the academic programs offering them. Student learning outcomes for all general education and graduation requirements are found on the UB website.

Program Outcomes: With the completion of the B.S. Cyber Forensics program, the student should be able to:

- Recognize the many modes of attack through digital space on computer systems and articulate how these relate to criminal acts
- Demonstrate specialized knowledge to remediate such attacks
- Evaluate commercial or governmental programs with regard to criminal attacks
- Design solutions for commercial or governmental programs with regard to criminal attacks
- Effectively manage counter-crime programs

3. Assessment of Learning Outcomes for the Program:

Once approved, the program will fully develop a schedule for assessment and map the level of student competency for each SLO (introduction, intermediate and mastered). The program director will oversee course data collection and program assessment procedures under the direction of the School Executive Director and the Associate Dean. The current graduate program in this area assesses all program SLOs every other year. Adjustments are made to the curriculum and then reassessed in the following year as part of the continuous improvement cycle. It is likely that the undergraduate program will employ a similar format. Results of these assessments will be entered into the university's assessment management software (TaskStream).

As is the case for all USM programs, this program will participate in the 7-year Program Review process that includes a self-study process and external peer evaluation. Finally, as UB is accredited by the Middle States Commission on Higher Education, the overall assessment process at UB was reviewed during the most recent accreditation of the University in 2017. See above for discussion of the assessment of general education and University-wide graduation requirements.

4. Course Descriptions:

The BS in Cyber-forensics is a 42-hour program with all 14 courses being required for successful completion.

FSCS 301 Fundamentals of Cyber Forensics (3)
It provides a basic understanding of cyber Forensics and its relationship with networks and operating systems. Recognize threats to an organization and to infrastructure. Also examines the frameworks, roles, and competencies involved with information Forensics. The fundamentals of cyber Forensics that will be examined include: network and security concepts, attacker techniques, data security, system and applications security.

FSCS 310 Cyber Crime and the Law (3)
Examines terminology and dynamics associated with business policies and civil, criminal and administrative law in high technology crimes. Explores various laws specific to combatting cybercrimes. Examination of statutory and Constitutional laws, regulations, and Acts, pertaining to the possession, extraction, and analysis of electronic evidence. The legal policies established for the prevention, apprehension, and prosecution of cybercrimes are defined. Protocols for evidence gathering, documentation, and presentation through a proper chain of custody are explored.

FSCS 320 Operating System Forensics (3)
Explore the roles of an operating system, its basic functions, and the services provided by the operating system. Learn the forensic analysis of the three major operating systems (Windows, Mac OS X, and Linux) in the real world. Topics include disk acquisition and analysis, file system forensic, memory acquisition and analysis, timeline investigation, as well as tracking and analyzing operating system configuration settings.

FSCS 325 Mobile Forensics (3)
Provides a framework for learning the latest developments in wireless and mobile communications; the characteristics and operations of wireless network technologies. Examines wireless network principles, protocols, and applications and provides basic knowledge necessary to complete a logical acquisition of digital evidence from mobile devices. Demonstrates the use of wireless networks and mobile forensics investigative techniques and tools. Explains mobile forensics procedures and principles, related legal issues, mobile platform internals, bypassing passcode, rooting, logical and physical acquisition, data recovery and analysis. Some of the topics covered will include hand-on extraction using iOS, PDA, Blackberry and Android platforms.

FSCS 360 Network Forensics (3)
Explores the methodology and procedures associated with analyzing and mitigating threats in a network environment; identification of potential risks, inappropriate software activity, and security breaches. Examines the topologies, protocols, and applications required to conduct forensic analysis in networks. Other topics include an overview of the various types of VPNs and the utility of firewalls and limitations of firewalls. Explains network forensic principles, legal considerations, digital evidence controls, and documentation of forensic procedures. Laboratory exercises will reinforce practical applications of course instruction.

FSCS 375 Scripting for Cyber Forensics (3)
Provides advanced elements of regular expressions in Python; explores scripting languages working with databases, files, Unicode and text encoding, and object-oriented coding in scripting language as it relates to forensics. Examines how to test and debug scripting codes. Builds scripts to automate diagnostics and investigations, and ways to visualize data. The course will teach students to use the scripting libraries as an investigative tool.

FSCS 380 Fundamentals of Cryptography (3)
Introduces the historical and modern cryptography to ensure the confidentiality, integrity, and authenticity of data and communication. Study how cryptographic algorithms and protocols work and how to use them. Topics include symmetric cryptography, asymmetric cryptography, hash

functions, as well as various attacks to cryptographic algorithms and protocols. Explores decryption techniques as applied to businesses and to government. Steganography is a process by which information is hidden within other media. Also presents the processes of hiding or encrypting data to inhibit a forensic analysis and of the detection and counter-resolution of hidden information.

FSCS 400 Ethical Hacking (3)
Learn how to apply knowledge of engineering to security evaluations, design and conduct security assessment experiments as well as analyze and interpret the resulting data. Learn various practice techniques for penetration testing and provide various methods of discovering ways of exploiting vulnerabilities to gain access to a system. Understand professional and ethical responsibility. Recognize the need for life-long learning in the quickly changing cybersecurity environment

FSCS 430 Forensic Investigation (3)
Examines the theory, best practices, and methodologies to conduct computer forensics investigations; it includes the ethical issues, evidence collection and preservation, data presentation, and chain-of evidence procedures. Explore current tools and technologies used to analyze, acquire, and organize digital evidence. Case studies are used to illustrate successful and sometimes less successful investigations. An introduction to LAN investigation as well as PC and Mac Forensics will be included.

FSCS 445 Forensic Data Analysis (3)
Learn concepts and techniques related to data analytics and analysis techniques to discover forensic evidence. Applying basic statistical, machine learning, and artificial intelligence tools to describe, visualize, and analyze forensic data collected from computing devices. Focus on detecting anomalies on collected forensic log files.

FSCS 480 Forensic Documentation (3)
Prepares students to document and manage cases properly from inception to successful conclusion. Students gain a basic understanding of investigative and forensic case documentation.

FSCS 482 Moot Court (3)
The skills of courtroom presentation techniques and skills required for qualified expert witnesses, designed to elicit direct, persuasive, and comprehensive testimony relative to evidentiary issues in criminal/civil matters are practiced. Formal reports pertaining to evidence in accordance with the law, explain the scientific methodologies applied, and develop techniques to conduct effective presentations.

FSCS 487 Field Internship in Forensic Science (3)
Provides field experience to students through laboratory assignments with various criminal justice entities. This requirement is completed at the end of the program. Eligible for continuing studies grade.

FSCS 490 Forensic Incident Response – Capstone (3)
Examines the methods, procedures, and policies necessary for a collaborative incident response team. Allows opportunity to review, analyze, and integrate what has been learned in each of the prerequisite courses. Students will learn how Incident response teams organize, identify, and gather evidence using a number of real-world scenario cases related to various aspects of cyber forensics to complete a capstone project that demonstrate mastery of the culmination of the cyber forensics degree program.

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

Students must complete 38 credits of general education in the following areas:[3]

- Arts & Humanities (6 credits)
- Arts & Humanities – Ethics (3 credits, upper-division)
- Social & Behavioral Sciences (6 credits)
- Physical & Biological Sciences (7 credits)
- Mathematics (3 credits)
- English Composition (6 credits to include WRIT 101 and 300)
- General Education Electives (7+ credits)

In addition, students must meet Graduation Requirements in four areas. Courses within the major or in the overall general education curriculum can fulfill these requirements. Apart from the capstone, it may also be possible to transfer in credits that could meet a graduation requirement; students may ask advisors about their specific cases and course equivalencies. UB courses seeking to fulfill graduation requirements are reviewed by UB's General Education Committee to see if they meet the SLOs for these areas[4]:

- Global Awareness and Diversity: students will be directed to courses that have been certified to fulfill this requirement.
- Information Literacy: If one or more courses in this major satisfy these GR SLOs, they will be nominated for certification by the General Education Committee. In addition, freshmen typically take INFO 110.
- Oral Communication: students will be directed to courses that have been certified to fulfill this requirement
- Technological Fluency: If one or more courses in this major satisfy these GR SLOs, they will be nominated for certification by the General Education Committee.
- Capstone Experience: FSCS 490 will be designed to meet the SLOs for this requirement.

Transfer Students: As this program was developed in consultation with community college faculty, it is anticipated that a sizeable proportion of students matriculating in the program will

[3] A list of courses meeting General Education requirements by area can be found at: https://www.ubalt.edu/academics/undergraduate/general-education/gen-ed-2017.cfm
[4] The SLOs for each General Education area and Graduation requirements can be found at: http://www.ubalt.edu/academics/undergraduate/general-education/gen-ed-SLO.cfm

transfer with their AA or AS degree, which would mean all general education at the lower-division level has been completed. Articulation agreements will be developed to assure ease of transfer. In general, transcripts are evaluated by admissions and transfer evaluators for meeting General Education requirements as well as graduation requirements and electives.

- Students missing lower division General Education courses after review will be directed to lower-division courses offered at UB;
- Upper division general education requirements: Ethics Requirement (IDIS 302 or PHIL 301) and English Composition (WRIT 300) are offered regularly during the Fall and Spring semesters at UB in both online and face to face modalities.
- Transfer students must also satisfy Graduation Requirements through general education classes or classes in the major.

Degree Program Summary

Graduation Requirements (GR) may be met through General Education electives or courses approved in the major that meet the GR student learning outcomes.

Requirement	Number of Credits
Arts and Humanities (lower- or upper-division)	6
Arts and Humanities – upper-division ethics	3
Social and Behavioral Sciences	6
Mathematics	3
Composition (WRIT 101)	3
Upper-Division Writing (WRIT 300)	3
Physical & Biological Sciences	7
General Education Electives (may also meet GRs)	7
Oral Communication (GR) – generally met by CMAT 200	3
Information Literacy (GR) – generally met by INFO 110	3
Technological Fluency (GR) – could be in major or electives	3
Global Awareness and Diversity (GR) – could be Gen Ed course or a general elective	3
FSCS 301 Fundamentals of Cyber Forensics	3
FSCS 310 Cyber Crime and the Law	3

FSCS 320 Operating System Forensics	3
FSCS 325 Mobile Forensics	3
FSCS 360 Network Forensics	3
FSCS 375 Scripting for Cyber Forensics	3
FSCS 380 Fundamentals of Cryptography	3
FSCS 400 Ethical Hacking	3
FSCS 430 Forensic Investigations	3
FSCS 445 Forensic Data Analysis	3
FSCS 480 Forensic Documentation	3
FSCS 482 Moot Court	3
FSCS 487 Field Internship in Forensic Science	3
FSCS 490 Forensic Incident Response – Capstone (also GR)	3
General elective credits	27
TOTAL =	**120**

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

   Not applicable

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

   Not applicable

8. Provide assurance and appropriate evidence the proposed program will provide students with clear, complete, and timely information on the curriculum, course and degree requirements, nature of faculty/student interaction, assumptions about technology competence and skills, technical equipment requirements, learning management system, availability of academic support services and financial resources, and costs and payment policies.

   Once approved, a set of program pages will be established on UB's website to provide students with current information on curriculum, course and degree requirements, technology competence and other skills required for the degree, equipment requirements for the degree, and links to financial aid and tuition and fee costs. If a course has a lab fee, that is indicated by the course description when the student registers. Also listed are student support services available to the wider university community.

Students at UB are assigned to a professional advisor and must meet with them when they achieve certain credit-hour milestones. In addition, students are provided with degree requirements sheets by their advisor; these guides to graduation may also be available online through the program pages. These professional advisors are the primary point of contact with the students on curriculum and degree requirements. They may also provide students with referrals to the Achievement and Learning Center, UB's primary tutoring service, which has not only writing and math tutoring but tutoring for other subjects as well. The Center for Excellence in Learning, Teaching and Technology (CELTT) provides a number of video guides for UB's Learning Management System (Sakai).

The students will also be advised by the faculty program director as to the technology competence and skills needed by students in the program. In terms of technical equipment, UB maintains two dedicated digital forensic laboratories for student use. As noted elsewhere in this application, the program will also establish a "virtual" lab for students to complete homework assignments. The University offers computer labs for students to use for free in the Bogomolny Library, the Student Center, and the Academic Center, as well as in specialized labs operated by the programs.
Faculty members all have a web page as well, where contact information is listed. Faculty office hours are identified on syllabi.

All such requirements are also part of UB responsibilities through its Middle States regional accreditation.

9. **Provide assurance and any appropriate evidence that advertising, recruiting, and admissions materials will clearly and accurately represent the proposed program and the services available.**

Recruitment, advertising, and admissions materials will clearly and accurately represent the proposed program and the services available, as is consistent with standards for Middle States accreditation. UB's marketing professionals have extensive higher education experience. The UB website readily provides information on programs, costs, and services, as well as admission requirements. The Consumer Information web page and UB Fact Book, posted on the Institutional Research page, provide plenty of information to support advertising materials. The University's undergraduate catalog is updated annually and posted online.

H. Adequacy of Articulation

If applicable, discuss how the program supports articulation with programs at partner institutions. Provide all relevant articulation agreements.

At this time no articulation agreements exist; however, the institution has been in discussions with faculty at community colleges throughout the state to ensure the proposed program curriculum is consistent post-AA and AS undergraduate requirements within the field of cyber forensics. UB prides itself on being transfer-friendly with respect to Maryland community colleges and is open to developing articulation agreements to facilitate transfer into the BS.

I. Adequacy of Faculty Resources

Quality of Program Faculty:

A combination of full-time faculty from the University of Baltimore and selected adjuncts from the commercial and government arenas with appropriate expertise and field experience will teach the courses. ***Faculty teaching assignments for the program are noted in the course list on p. 2.***

The UB forensics faculty are expert professionals who, in addition to their academic expertise, have acquired decades of practical experience in the investigation and prosecution of crime, cybersecurity and digital forensics. A complement of theoretical and practical expertise, forensic faculty work in metropolitan, state and national agencies and in corporate and private industry; they research with professionals from other countries and consult nationally and internationally. All full-time faculty have terminal Ph.D. in the field, all adjuncts are working in the field and have the appropriate graduate level education to teach in the program. Qualified faculty include:

Weifeng Xu, Associate Professor and MSFS Program Director.
Ph.D. in Software Engineering, North Dakota State University.

His areas of expertise include software security, mining software engineering data, and applied formal methods. He has published more than 50 peer-reviewed papers in international journals and conference proceedings, including prestigious venues such as IEEE Transactions on Dependable and Secure Computing and IEEE Transactions on Reliability. He was successfully awarded over $1.5M in research grants from NSF, DoE, and General Electric.

Nima Zahadat, Assistant Professor and USG MSFS Program Director
Ph.D. in Computer Science, The George Washington University

Dr. Zahadat has spent most of his career in high education or professional training. He has more than 20 years as a trainer/educator. He has written curriculum for numerous programs and courses. He currently teaches in the MSFS Cyber Investigations program and serves as the Program Director of that program at the USG campus.

Melvin de la Cruz, Assistant Professor, MSFS Program
Ph.D. in Linguistics, Forensic Speech Science, University of Huddlesfield (U.K.)

Most of Dr. de la Cruz's professional experience has been in federal law enforcement. He has 14 years of experience working with the US Department of Labor, US Department of Homeland Security, and the US Department of Justice as a federal agent. While working full-time for the federal government, he taught Criminal Law, Statutory Law, Ethics and Advanced Firearms, and he also taught algebra and analytical geometry, calculus, and administration of justice courses.

Patricia Hall, Esq., Lecturer, MSFS and BSFS Programs
J.D., University of Baltimore

Attorney Hall has more than 28 years of professional experience in the field of law processing high-technology crime cases. Prior to her appointment as lecturer this year, she had six years' experience as a part-time faculty member in higher education. She has an outstanding background in the legal field and brings enormous professional experience and real-world application of the law and business regulations to the classroom. She currently teaches in UB's MSFS Cyber Investigations and BS in Forensic Science programs.

Donte Leggette, Cyber Investigations Lab Director and Adjunct Professor
MSFS in Cyber Investigations, University of Baltimore

Mr. Leggette has served as the Lab Director for he MSFS Cyber Investigations Program since 2016. His full-time position is with MECU as a network administrator managing the networks security and infrastructure protections. He has 18 years of experience working in IT and cyber security at MECU.

Joshua Rosenblatt, Esq., Adjunct Professor, MSFS Program
J.D., University of Baltimore

Mr. Rosenblatt is a former police officer who has more than 12 years' experience as a practicing attorney. He was the first appointed Chief of Criminal Strategies Unit, Baltimore State's Attorney's Office, before he moved to the Baltimore Police Department's Training Academy faculty as the head of Legal training. He currently teaches in UB's MSFS Cyber Investigations and BS Forensic Science programs.

UB's Center for Excellence in Learning, Teaching and Technology (CELTT) includes among its staff a Director of Online Learning who holds a doctorate in instructional technology and has extensive experience with faculty professional development in the area of online pedagogy. CELTT provides online and in-person opportunities for faculty to learn more about using technology effectively and how to enhance students' learning. There are regular opportunities for faculty fellowships in CELTT, and the new associate director has extensive experience in assessment.

Program faculty are also active in professional organizations, both academic and technical, and maintain currency in their fields through research, grant projects, consulting and collaboration.

J. Adequacy of Library Resources

Library Requirements:

UB has a law library as well as the Bogomolny Library, and as a University System of Maryland member, UB has electronic and interlibrary loan access to the entirety of the System libraries.

The materials students need are largely available through open source databases, governmental archives, or are available online through organizations like the Department of Justice, Police Research Foundation, Westlaw, or a variety of professional organizations and businesses. Peer reviewed material in journals is easily accessible through existing library subscriptions.

K. Adequacy of Physical Facilities, Infrastructure and Instructional Equipment (as outlined in COMAR 13B.02.03.13)

1. 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.

The program will utilize the current Forensic Computer Laboratories in the Academic Center built for the Master of Science in Forensic Science – Cyber Investigations degree program. Courses with a lab component will need a classroom space that will allow students to break down computer hardware and hard-wire computer workstations and special software tools.

2. Provide assurance and any appropriate evidence that the institution will ensure students enrolled in and faculty teaching in distance education will have adequate access to: a) An institutional electronic mailing system, and b) A learning management system that provides the necessary technological support for distance education

The program will not be taught online. However, all students enrolled in the program will have access to a virtual learning environment to complete their external classroom assignments. All students enrolled in the institution have access to the UB email system and technology, and all courses, whether online or face-to-face, have dedicated space on the learning management system (Sakai), where the syllabus and various resources are available. The Center for Excellence in Learning, Teaching, and Technology provides resources and training for faculty and students so they are able to use Sakai resources effectively.

L. Adequacy of Financial Resources:

1. Complete **Table 1: Resources and Narrative Rationale**. Provide finance data for the first five years of program implementation. Enter figures into each cell and provide a total for each year. Also provide a narrative rationale for each resource category. If resources have been or will be reallocated to support the proposed program, briefly discuss the sources of those funds.

TABLE 1: PROGRAM RESOURCES					
Resource Categories	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**
1. Reallocated Funds	0	0	0	0	0
2. Tuition/Fee Revenue (c + g below)	$177,044	$213,013	$285,060	$328,364	$344,207

a. Number of F/T Students[2a]	17	20	26	30	30
b. Annual Tuition/Fee Rate[2b]	$9,236	$9,379	$9,567	$9,716	$9,868
c. Total F/T Revenue (a x b)	$157,012	$187,582	$248,743	$291,476	$296,032
d. Number of P/T Students	4	5	7	7	9
e. Credit Hour Rate[2e]	$5,008	$5,086	$5,188	$5,270	$5,353
f. Annual Credit Hour Rate[2f]	12	12	12	12	12
g. Total P/T Revenue (d x e x f)	$20,032	$25,432	$36,318	$36,888	$48,175
3. Grants, Contracts & Other External Sources	0	0	0	0	0
4. Other Sources[5]	$27,500	0	0	0	0
TOTAL (Add 1 – 4)	$204,544	$213,013	$285,060	$328,364	$344,207

2. Complete **Table 2: Program Expenditures and Narrative Rationale**
   Provide finance data for the first five years of program implementation. Enter figures into each cell and provide a total for each year. Also provide a narrative rationale for each expenditure category.

TABLE 2: PROGRAM EXPENDITURES:					
Expenditure Categories	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**
1. Faculty (b + c below)	$71,118	$98,881	$114,833	$129,817	$131,345

[2a] Proportion of students in each category (FT, PT) were calculated using current forensic program students: 78% of students in program are full-time and 22% are part-time. Students may vary from term-to-term as to whether they are full-time or part-time.
[2b] FT students in Forensic studies generally take 15 credit hours per semester. However, tuition rates do not increase once a student enrolls for more than 12 credits. Projections indicate that the program may attract up to 2 out-of-state students per year and using current Forensic Studies enrollments, all of these students are full-time. However, in-state rates will be used in the revenue calculations. Rates assume a 2% tuition increase per year and a 2% fee increase in year 3 (placing the AY2021 tuition at $7154 and fees at $2082).
[2e] The PT in-state rate for a 6-credit hour semester is used here. With the proposed 2% increase for AY 21, tuition would be $1958 and fees would be $546. Part-time tuition and fee increases are estimated in the same manner as full-time.
[2f] Part-time forensic studies students take (on the average) 12 credit hours per year.
[5] Line 4 Resources – USM Enhancement Funds grant, part of which is assigned to this program for initial technology needs.

a. Number of FTE[6]	.70	1.1	1.3	1.4	1.4
b. Total Salary[7]	$54,121	$77,251	$89,714	$101,420	$103,145
c. Total Benefits[8]	$16,997	$21,630	$25,119	$28,397	$28,200
2. Admin. Staff (b + c below)	$5107	$5208	$5310	$5413	$5515
a. Number of FTE	.1	.1	.1	.1	.1
b. Total Salary	$3,990	$4,069	$4,149	$4,229	$4,309
c. Total Benefits	$1,117	$1,139	$1,161	$1,184	$1,206
3. Support Staff (b + c below)	$37,425	$38,071	$38,817	$39,563	$40,309
a. Number of FTE[9]	.5	.5	.5	.5	.5
b. Total Salary	$29,260	$29,743	$30,326	$30,909	$31,492
c. Total Benefits	$8,165	$8,328	$8,491	$8,654	$8,817
4. Technical Support and Equipment[10]	$10,000	0	0	0	0
5. Library	0	0	0	0	0
6. New or Renovated Space	0	0	0	0	0
7. Other Expenses[11]	$17,500	0	0	0	0
TOTAL (Add 1 – 7)	$141,150	$142,160	$158,960	$174,793	$177,169

[6] Faculty teaching in this program also teach in the undergraduate Forensic Studies program and the graduate program in Cyber Investigations. Therefore, the FTE is calculated based on a standard formula that each class constitutes 10% of a faculty members annual workload.
[7] Total salary is calculated as the proportion of faculty salary devoted to this program. A 2% COLA is added for Years 2-5.
[8] Benefits are calculated as 28% of salary.
[9] This position is a Digital Forensics Laboratory Director. Half the cost of this position will be charged to the graduate Cyber-Investigations Program
[10] The University was awarded $20,000 in Workforce Development Funds for Technology Upgrades in the Digital Forensic Labs. Half the cost of these upgrades have been allocated to the graduate program. In the future, technical upgrades are supported through student fees.
[11] The University was awarded funding for a Virtual Lab Environment ($35,000) through Workforce Development Funds. Half the cost was allocated to the graduate program. This effort will also be supported by course fees.

Data in Table 2 shows anticipated expenditures for the new program. We anticipate that as the program grows, additional faculty lines will be made available. In addition, we are providing for a one-course release for the program director. As noted in the program proposal, we do not anticipate that new resources will be needed from the library as many of the topical areas relevant to this area are available through ResearchPort. Staff assistance to faculty will be provided through the Academic Program Specialist assigned to the School of Criminal Justice. Student advising will be undertaken through the College of Public Affairs Advising staff.

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

Procedures for conducting program and individual course evaluations will be outlined in a program assessment plan, which is required of every program at the University. An Assessment Plan will be developed for the BS Cyber Forensics degree prior to the implementation of the program, and the plan is documented in TaskStream, the University's assessment management system. The plan will identify overall program learning objectives and measurable course-level objectives for each of the required courses for the program; the program SLOs are mapped to courses as part of the assessment planning. The plan will also outline a process for setting student learning goals and objectives; shared governance processes at UB have new courses with the SLOs reviewed up to the provost. Assessment of all program SLOs will be conducted at least once very two years, and the data will be used to identify the strengths and weaknesses of the program to guide faculty in making improvements to the program and to modify as appropriate student learning outcomes. In addition to the internal program and course review process, an external program review will be conducted every seven years. As noted above, that process involves a self-study and external peer review.

Student course evaluations, course syllabi, course materials, exams, assignment criteria, and classroom peer observation will be used to evaluate faculty annually and as part of the evaluation of teaching that is included in promotion and tenure review processes.

N. Consistency with the State's minority student achievement goals and in the State Plan for Postsecondary Education.

The B.S. Cyber Forensics Program is committed to minority student achievement and overall student success. The program is in conformance with the University's recruitment and retention of a diverse student body. UB has a long-standing commitment to the recruitment of a diverse student body and has proactively sought to identify multiple recruitment channels and communication strategies to ensure that there is outreach to a diverse population. The University also has a number of programs in place that will help the program's diverse student body persist until graduation. The University continuously assesses the success of these programs and has developed an achievement gap plan to further increase minority graduation rates of students. In 2019, the undergraduate graduation rate for African-American students was the same as for white students, and the freshmen-to-sophomore retention rate was well over 80%.

In addition, the University has just launched the Parsons Scholarship program, which is a last-dollar scholarship program that would enable Pell-eligible, full-time students with a Maryland associate degree who transfer to UB to complete their bachelor's degree for free. The University anticipates that this program could assist many minority students in furthering their education in Maryland.

O. Relationship to Low Productivity Programs Identified by the Commission:

Not Applicable.

P. Adequacy of Distance Education Programs (as outlined in COMAR 13B.02.03.22)

While UB is approved to offer distance education—and has been offering online degrees for 20 years--the proposed program will be taught in traditional classrooms and laboratories. Students will, however, have full access to an interactive virtual learning environment for use outside the classroom to complete course assignments, and courses will, like all UB courses, have dedicated space on the learning management system.

Off-Campus Delivery of Program

The program will only be offered at the University of Baltimore campus.