BALTIMORE CITY COMMUNITY COLLEGE

2901 Liberty Heights Ave.
Baltimore, Maryland 21215

410-462-8300
www.bccc.edu

November 14, 2022

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

Dear Dr. Fielder:

On behalf of the Baltimore City Community College, this letter is the official requesting your approval for a new Cybersecurity Digital Forensics Program (HEGIS: 5505, CIP: 43.0403). This new AAS degree program is being implemented as a result of being awarded a capacity building grant from the National Security Agency's Cybersecurity Education Diversity Initiative (CEDI). This is a nationwide initiative that supports Minority Serving Institutions (MSI)'s and Historically Black Colleges and Universities (HBCU)'s to obtain funding and educational resources and access for students.

Upon approval from MHEC and commensurate with COMAR 13B.02.03.03, students will be welcomed to enroll in courses for the new program beginning in spring 2023. In addition, appropriate advertising and recruitment for new students will take place. The awarded grant includes a budget allocation of $2,000 per student for 20 students in the first semester and for 22 students in the second semester. The program course offerings and student scholarships will greatly enhance the enrollment numbers for this program.

Payment has already been submitted to MHEC via R*STARS interagency fund transfer, transaction number JA220040 and JA220048, in accordance with the MHEC fee schedule. The new program proposal outlines all the relevant details for this much needed program to educate our students to support the immediate Baltimore City community and country. We look forward to hearing back from you soon regarding the approval of the BCCC Cybersecurity Digital Forensics Program.

Sincerely,

Laura J. Cripps, PhD
Vice President of Academic Affairs

Office Use Only: PP#

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

Institution Submitting Proposal	Baltimore City Community College

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

Payment Submitted: (●) Yes ( ) No

Payment Type: (●) R*STARS # ( ) Check #

Payment Amount: 850.00

Date Submitted: 4/29/22

Department Proposing Program	Business and Technology	
Degree Level and Degree Type	AAS	
Title of Proposed Program	Cybersecurity Digital Forensics	
Total Number of Credits	60	
Suggested Codes	HEGIS: 5505	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: 2023
Provide Link to Most Recent Academic Catalog	URL: http://bccc.catalog.acalog.com/	
Preferred Contact for this Proposal	Name: Laura J. Cripps	
	Title: Vice President Academic Affairs	
	Phone:	
	Email: lcripps@bccc.edu	
President/Chief Executive	Type Name: Debra L McCurdy	
	Signature: Debra L. McCurdy	Date: 04/29/2022
	Date of Approval/Endorsement by Governing Board:	03/16/2022

Revised 1/2021

MHEC

ACADEMIC PROGRAM PROPOSAL MATERIALS

Academic Program Proposals

FOR DEGREE-GRANTING INSTITUTIONS AUTHORIZED TO OPERATE IN MARYLAND
GUIDELINES FOR PROPOSING
NEW ACADEMIC DEGREE PROGRAMS, NEW STAND-ALONE CERTIFICATE PROGRAMS, AND SUBSTANTIAL MODIFICATIONS

An institution submits a proposal using guidelines in accordance with State regulations found in **COMAR 13B.02.03**. Proposals shall be submitted electronically to **acadprop.mhec@maryland.gov**.

A. Centrality to Institutional Mission and Planning Priorities:

1. **Provide a description of the program, including each area of concentration (if applicable), and how it relates to the institution's approved mission.**

   Mission: Baltimore City Community College provides quality, affordable, and accessible education meeting the professional and personal goals of a diverse population, changing lives, and building communities.

   Vision: Baltimore City Community College is an innovator in providing quality career pathways and educational opportunities for a diverse population of learners to exceed the challenges of an ever-changing competitive workforce and environment.

   Baltimore City Community College provides quality, affordable, and accessible educational opportunities with comprehensive programs that meet the professional and personal goals of students while improving communities in the greater Baltimore area. The primary goal of the Cybersecurity Digital Forensics program is to provide a career pathway to a knowledge-economy job and to provide a curriculum that is more accessible for community college students. Students will have the option to enrich their academic, experience, and marketing credentials by doing real-work projects using the same software they will use in the industry**.** Organizations such as the Department of Homeland Security (DHS), DoD, NSA, FBI, NASA, Government Contractors, and more have estimated shortages in cybersecurity professionals needed to monitor and defend State and Federal Government, and Private and Public Corporate systems in the US. Graduates from this program will provide resources to help fulfil this requirement. This program will provide significant opportunity to Baltimore City Community College students; a Minority Serving Institution dedicated to serving the local City community. With close connections to City four-year Universities such as Coppin State University and the University of Baltimore, Baltimore City Community College provides unique and dedicated transfer pathways for its students.

2. **Explain how the proposed program supports the institution's strategic goals and provide evidence that affirms it is an institutional priority**.

   The primary strategic Goals for Baltimore City Community College focus on Student Success, Community Engagement, and Institutional Framework. Focusing on these strategic goals and objectives will not only equip our students with the necessary competitive skills but will also significantly contribute to the college's financial sustainability.

Student Success – The new Cybersecurity Digital Forensics program was developed under the leadership team with both extensive industry-based cybersecurity experience and approximately 30 years of combined teaching experience. Also, the Cybersecurity Advisory CTE Board was consulted in outlining the proposed curriculum for our students. The course selection, pedagogy methods with hands on labs, and planned training for participation in Cyber Competitions will offer equitable access to BCCC's diverse population.

Community Engagement – BCCC has been a staple in the Baltimore area for over 75 years. This new program will enhance community engagement by providing its community with a new program in Cybersecurity Digital Forensics. This is a growing field with greater needs and jobs than current trained students to fulfill the needs. Ongoing partnerships with local businesses provide students with technology skills to strengthen their employability. The new program will enhance their cyber skills and offer hands-on experiences with business partners and internship opportunities. Students will learn new cyber skills in a state-of-the-art setting.

Institutional Framework – BCCC ensures Cyber resources are highly skilled in teaching and supporting our students in one of the fastest growing fields. The staff not only have the educational requirements, but they are required to have ongoing professional development to stay abreast of academic trends, best practices, and applicable future emerging initiatives.

3. **Provide a brief narrative of how the proposed program will be funded for at least the first five years of program implementation (Additional related information is required in section L).**

   During the initial program implementation (first semester), existing BCCC Faculty resources will maintain the program. Students will benefit from scholarship opportunities of $2,000 each for their initial semester into the new program. Current resources including full-time and adjunct faculty will be used to support the program's resource requirements. The program will be evaluated in harmony with BCCC's Program Review and Evaluation strategies to ensure ongoing successful program continuation and resource allocation.

4. **Provide a description of the institution's a commitment to:**

   a. **ongoing administrative, financial, and technical support of the proposed program**

      Baltimore City Community College has the full support of the academic leadership including the associate dean of business and technology, dean of BSTEM, associate vice president of academic affairs, vice president for academic affairs, Baltimore City Community College's president, and the Board of Trustees. This support encompasses ensuring the new Cybersecurity Digital Forensics is staffed with exceptional faculty and the classroom and lab are equipped with the state-of-the-art facilities, equipment, software, networking, and other college-wide resources for this innovative program. The program currently has one full-time faculty member, and the college is actively recruiting for a second full-time position. The program also benefits from experienced and consistent adjunct faculty who work in the field.

This commitment also includes collaborative support from admissions, registration, and program advising. A full-time program chair is dedicated to ensuring students have a complete educational plan of their courses throughout their scholastic journey at the college, providing academic advising as needed. In addition, outstanding faculty are in place to support students; enhancing their skills in cyber range activities, clubs, competitions, and related certifications.

b. continuation of the program for a period of time sufficient to allow enrolled students to complete the program.

The students who enroll in this program are provided with an educational plan clearly delineating course sequencing and the academic scheduling is built with this in mind. Currently, faculty advising ensures that all students enrolled in the program of study are able to complete their program. Further, the following committees ensure any changes to curriculum are made with full consideration of student catalog year and completion. An academic teach-out policy is currently being drafted.

Program Review and Evaluation Committee (PREC)
Baltimore City Community College is committed to ensuring all students are provided an opportunity to complete their program of study. This includes students desiring to complete the degree and certificate programs. All Baltimore City Community College programs go through an internal program review and evaluation every five years led by the Faculty Senate's college-wide Program Review and Evaluation Committee to ensure adherence to established state guidelines by the Maryland Higher Education Commission (MHEC), Code of Maryland (COMAR), and Middle States Commission on Higher Education (MSCHE). This review is a proactive approach to confirm programs meet the standards and are contributing to the college's overall program goals for student learning, retention, and graduation.

Curriculum Instruction Committee (CIC)
The college-wide supported Curriculum Instruction Committee is dedicated to ensuring standards and approvals of course syllabi, and curricula for Baltimore City Community College. Every two years the committee reviews syllabi for course deletions and obsolescent curricula. New courses, major changes to existing courses or curricula must go through the CIC and applicable college administration for approval. This ongoing process ensures continual process improvement in the college's courses and program offerings.

Student Learning Outcomes and Assessments (SLOA) Committee
Baltimore City Community College also supports the Student Learning Outcomes and Assessments Committee consisting of faculty and non-faculty members. This committee completes periodic reviews of student learning outcomes, assesses student learning, and provides ongoing training and support student learning and assessments. In collaboration with faculty and administrators, the SLOA Committee's completes a Learning Improvement Plan annually based on student learning course outcomes.

B. Critical and Compelling Regional or Statewide Need as Identified in the State Plan:

1. **Demonstrate demand and need for the program in terms of meeting present and future needs of the region and the State in general based on one or more of the following:**
   a. **The need for the advancement and evolution of knowledge**
   b. **Societal needs, including expanding educational opportunities and choices for minority and educationally disadvantaged students at institutions of higher education**
   c. **The need to strengthen and expand the capacity of historically Black institutions to provide high quality and unique educational programs**

   Reply for Sections 1a, 1b, and 1c Above:
   Baltimore City Community College is a Predominantly Black Institution (PBI). The new Cybersecurity Digital Forensics will enhance course offerings and training for students by providing them with educational opportunities in high demand such as computer systems analyst, computer forensic investigators, and more. By offering high technical programs in demand, BCCC will strengthen students' skills and career opportunities. According to the U.S. Bureau of Labor Statics *Occupational Outlook Handbook* (June 2022), these job opportunities are projected to increase by 9% over a 2021-2031 period.

   In addition to the organizations such as DHS, DoD, and NSA, the Baltimore Cyber Range has a wide range of partners through which graduates can do internships with for hands-on training and workforce development opportunities (Baltimore Cyber Range, 2021). Currently there are more opportunities than resources available to fulfill the need. According to a recent Gartner Report, organizations are changing their focus on greater cybersecurity protection, governance, and cybersecurity business priorities (Proctor, 2020).

   The new Cybersecurity Digital Forensics Program was developed as a result of receiving a capacity building grant awarded by the Department of Defense (DoD) Cybersecurity Education Diversity Initiative (CEDI). DoD's initiative is to provide quality cybersecurity education, access, and mentoring to students attending Minority Serving Institutions (MSIs) and Historically Black Colleges and Universities (HBCUs) throughout the United States. Other opportunities include internships and hands-on experience in the Maryland Innovation and Security Institute's cyber range. Baltimore City Community College was one of two schools to receive the capacity building grant in Baltimore City, Maryland and one of eight Minority Serving Institutions to receive the grant in the country.

2. **Provide evidence that the perceived need is consistent with the Maryland State Plan for Postsecondary Education.**

   The *2017–2021 Maryland State Plan for Postsecondary Education* outlines 11 strategies to ensure students are provided fair access to reasonably priced postsecondary education exemplifying excellence. These strategies are grouped by "Access," "Success." and "Innovation."

ACCESS

Strategy 1: Continue to improve college readiness among K-12 students, particularly high school students. Baltimore City Community College (BCCC) partners with Baltimore City's Mayor Scholar's Program (MSP), Upward Bound, and P-Tech (Pathways in Technology) to provide quality support, information, college prep, college education, and career opportunities for students from underserved communities. BCCC's faculty and staff work collectively to track students' progress from enrollment, graduation, and career planning. The highly skilled cybersecurity faculty stay abreast of ongoing technologies and trends and participate in student orientation sessions for incoming students in these programs.

SUCCESS

Strategy 4: Continue to ensure equal educational opportunities for all Marylanders by supporting all postsecondary institutions. Baltimore City Community College's new Cybersecurity Digital Forensics Program was planned with scholarship opportunities for students to ensure students have equal educational opportunities for all Marylanders. The first and second semester will offer students $2,000 scholarships in support of this strategy. Additionally, BCCC will offer tutoring and educational opportunities that are in high demand for students.

Strategy 6: Improve the student experience by providing better options and services that are designed to facilitate prompt completion of degree requirements. The new Cybersecurity Digital development program offers a well-planned pathway for students entering the program to obtain the degree and/or stackable certificate. The Program Coordinator will meet with students periodically to plan their courses, advise them on the course content and related skills obtained, mapped to career opportunities.

INNOVATION

Strategy 8: Develop new partnerships between colleges and businesses to support workforce development and improve workforce readiness. The Cybersecurity Program Coordinator collaborates with community organizations, four-year colleges, the Cybersecurity Advisory Board, and businesses offering cybersecurity opportunities. BCCC continues to develop new partnerships between colleges and businesses to ensure students are workforce ready.

BCCC has ongoing collaborations and communications with the following universities:

University of Maryland Baltimore County (UMBC) – A Memorandum of Understanding (MOU) is underway between UMBC and BCCC to establish access to and enrollment in, the Cyber Range for certain BCCC faculty for the purposes of administering credit-bearing courses or for cyber clubs. BCCC students will benefit by:

- Having an opportunity to experience analyzing and monitoring real-world threats in a safe and controlled environment
- Learn how to recognize and handle threats, working on teams
- Study how to use industry software and skills they can use in a cyber career
- Participate in cyber competitions such as "Capture the Flag"

Coppin State University – An ongoing collaboration exists between Coppin State University and BCCC. Prior collaborations have included engaging BCCC's students to participate in the Google ExploreCSR Award. BCCC had the opportunity to recommend students to participate in a program to strengthen women computer science majors' selected technical skill(s). Coppin State representatives have also communicated with the Program Coordinator at BCCC regarding CISCO's Networking Academy. In turn, the BCCC Program Coordinator has has begun a series of courses offered by the CISCO Network Academy. Program Coordinator successfully completed the IT Essentials for Instructors in October. 2022 in preparation for teaching future network essential courses.

Howard University and Morgan State University – Communications is ongoing between Howard and Morgan Universities to introduce the National Cyber League's (NCL) Course Curriculum and Student Scholarships to HBCUs and MSIs. The NCL offers students cyber training, participation in cyber competitions, certification training and more. The BCCC Program Coordinator was also introduce to the NCL Coach's Manual in preparation to teach Cyber Courses using the NCL Course Curriculum Guide.

Bowie State University (BSU) – Bowie State University, a designated a National Center of Academic Excellence in Cyber Defense (NCAE-CD), and BCCC have established an Articulation Agreement to accept all required courses from the current Cyber Security and Assurance Program into their Cyber Engineering Operations Program. BSU continues to collaborate with the BCCC Cyber Security Program Coordinator and most recently invited the BCC students to attend "A Cyber Day" at Bowie State University.

In addition, BCCC has numerous Articulation Agreements with College and Universities enhancing student support, educational and career opportunities, and cyber skills training leading to potential certifications.

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**.

   The proposed Cybersecurity Digital Security program is expected to provide BCCC's graduates for entry into a variety of cybersecurity positions in a wide range of industries. Graduates will also obtain credited course skills transferable to numerous four-year colleges and universities. Additional skills will prepare students for competencies to take various certification test to become certified as a: Certified Secure Computer User (CSCU), Computer Hacking Forensics Investigator (CHFI), and Certified Network Defender (CND), Other preparation skills include training for the CompTIA A+, Net+, and Security + certifications. Obtaining such certifications will enhance students' employability options.

The following are examples of employment opportunities for students according to the Bureau of Labor Statistics (BLS), May 2021, with technical skills focused on Computer Systems Analysts(151211), Information Security Analysts (15-1212), Computer Network Support Specialists 15-1231, Computer User Support Specialists(151232), Network and Computer Systems Administrators(151244), and Computer Occupations, All Other(151299):

Multiple occupations for one geographical area

Area:Maryland
Period:May 2021

Occupation (SOC code)	Employment[1]	Employment percent relative standard error[3]	Hourly mean wage	Wage percent relative standard error[3]	Hourly median wage	Hourly 75th percentile wage	Hourly 90th percentile wage	Employment per 1,000 jobs
Computer Systems Analysts(151211)	13150	4.3	49.23	1.6	47.43	61.11	78.26	5.165
Information Security Analysts(151212)	7330	12.5	60.63	4.0	60.03	78.33	93.61	2.879
Computer Network Support Specialists(151231)	7210	6.0	36.60	2.9	36.96	41.76	49.19	2.831
Computer User Support Specialists(151232)	9770	6.9	27.68	2.3	25.80	30.73	38.07	3.839
Network and Computer Systems Administrators(151244)	9470	6.8	51.19	1.9	48.53	61.51	76.24	3.719
Computer Occupations, All Other(151299)	23640	3.9	57.97	2.1	59.44	67.17	78.33	9.283

(1)Estimates for detailed occupations do not sum to the totals because the totals include occupations not shown separately. Estimates do
(3)The relative standard error (RSE) is a measure of the reliability of a survey statistic. The smaller the relative standard error, the more

SOC code: Standard Occupational Classification code -- see http://www.bls.gov/soc/home.htm
Date extracted on :Sep 30, 2022

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

Cyberattacks continue to increase locally, nationwide, and internationally. This growth has impacted the rise in the job demand for resources in the cybersecurity field to help provide countermeasures to detect and prevent hackers from gaining access to networks, data, and unauthorized systems. The Bureau of Labor Statistics has projected that security analyst is one of the fastest growing occupational fields with anticipated growth of 35% from 2021 to 2031.

Employment projections data for information security analysts, 2021-31

Occupational Title	SOC Code	Employment, 2021	Projected Employment, 2031	Change, 2021-31		Employment by Industry
				Percent	Numeric	
Information security analysts	15-1212	163,000	219,500	35	56,500	Get data

SOURCE: U.S. Bureau of Labor Statistics, Employment Projections 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.**

According to Gartner, Inc. more organizations are recognizing the need to take cybersecurity needs into consideration when making key business decisions including hiring third party cyber professionals, cyber risks in marketing, finance, management and leadership (Mandy, Lee, Addiscott, Scholtz, & Gopal, 2022). As organizations become more client focused, by 2025 over 50% of strategic planning will include cybersecurity is at the forefront to ensure safe customer experiences and quantifying cyber risks in decision-making (Mandy, et al., 2022).

As cybersecurity risks rise daily, organizations move to increase their measure of Key Risk Indicators (KRIs) (Holmes, 2022). Thus, organizations move to employ experts to help identify and protect their digital footprints. The continuous cyber risks, demonstrates a need for more skilled security analysts and related occupations to provide counter measures to offset cyber risks.

The U.S. Bureau of Labor Statistics (2022) projected an increase in growth by 35% from 2021 to 2031. This increase demonstrates a growing need for resources to fill anticipated openings. According to Meeks, 2022, taking the educational route to obtain an Associate's Degree, is beneficial since completion of hands-on skills and training for entry-level jobs can be obtained in just two years. Furthermore, the projections indicate approximately 19,000 opportunities for employment in this high demand field.

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

Baltimore City's Community College's Strategic Goals 2018-2022, outline BCCC's commitment to attract and retain an ongoing supply of students and graduates.

Goal 2: Community engagement – Implement a comprehensive approach to engage current and future students, alumni, and the community

2.2 – Grow partnerships with business and industry, government agencies, community members, educational institutions, and all potential partners in serving our students and community

2.3 – Strengthen partnerships to promote and increase access to student learning and transfer opportunities, collaborative planning, and resource sharing

BCCC recruits from Baltimore City High Schools, Baltimore County, and through the Mayor's Scholars Program (MSP). An additional source of students is recruited through the dual-enrollment programs such as P-Tech and Upward Bound. BCCC students benefits from the U.S. Department of Education's Federal TRIO Program offering a host of student support including grants, academic development, tutoring, and more to successfully complete their secondary education. BCCC also attracts seniors, veterans, transfers, international students and has support offices and dedicated support services for the traditional and non-traditional students.

The capacity building grant received includes a budget allocating 42 student scholarships at $2,000 per student. These scholarships will be used to recruit students into the proposed program. Retention strategies include working with business associates at the Baltimore Cyber Range, our current Cybersecurity Advisory Board, and Cybersecurity organizations.

Students will be offered hands-on enhancement experience, internships, and no cost to low-cost supplemental training to increase career potential opportunities.

According to the Maryland State Plan for Higher Education "it is the goal of the State that at least 55% of Maryland's adults age 25 to 64 will hold at least an associate's degree by the year 2025" (Md. Code, Educ. § 10-205, *Current with changes from the 2022 Legislative Session* 2022).

The projected student enrollment in the new Cybersecurity Digital Forensics Program and Certificate over a five- year period is outlined below. With enrollment in this program, students will develop a deep sense of pride knowing they are in a field contributing the national cyber defense. The projections below are based on past performance of the current Cyber Security and Assurance Program. The new proposed cyber program will provide scholarships to attract and encourage new students into the program.

Program: Cybersecurity Digital Forensics Program & Certificate					
Projected # of Majors Over Five Years					
Estimates	**Spring 2023**	**Spring 2023**	**Spring 2024**	**Spring 2025**	**Spring 2026**
# of Students	22	44	66	88	110
Projected Graduates*			22	30	44
*** Not all Full-Time Students**	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**

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.**

   Several community colleges were researched in the Maryland area. There were similarities and differences in the programs.

   Anne Arundel Community College (AACC) – There are similar titles such as Digital Forensics 1-3; however, the course content covered has different focus areas. Also, the Capstone for the BCCC focus course is different, and covers a combination of the content that will be covered in the BCCC program and proposes to include internship opportunities.

Community College Baltimore County CCBC – The only similarity appeared to be both three and four credit courses. The program appeared to focus more on the Network/ Defense/CCNA certification training.

Garret Community College – The similarity was the combination of three and four credit hour courses. However, this program was more similar to the CCBC program focusing on CISCO/Networking with one course on Computer Forensics.

Howard Community College (HCC) – HCC offered an entry, mid-level, and advanced level Computer Forensic Courses vs. the proposed Digital Forensics courses for BCCC. There was also a Python course offered. All the Cyber courses are three credit offerings vs four credit courses at BCCC for the proposed program.

Montgomery Community College – The similarities were the inclusion of network courses, some three and four credit hour courses, and a Capstone course. The major difference was the concentration of the program to CISCO/Networking.

2. Provide justification for the proposed program.

Cybercrime continues to be on the rise worldwide. Recently, the Federal Government issued an Executive Order on Improving the Nation's Cybersecurity. Organizations (Biden, Jr., 2021). This Executive Order states the President's commitment to address the rise in cyberattacks and crime. The government's bold attempt to address this problem head-on involves the Federal Government taking actions to prevent, protect against, and detect cyber incidents. In addition, the oversight includes ensuring the agencies such as the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and Intelligence Community (IC) work together to share and combat cybercrime (Biden, Jr., 2021).

Another important area addressed in this Order included modernizing Government approaches for best practices to protect against attacks, identifying classifications of data, using multifactor authentication and encryption, and establishing effective training programs (Biden, Jr., 2021). CISA's responsibilities include strengthening the workforce for today and the future. Federal training includes free virtual online training on cybersecurity. Certification preparation courses. Moreover, CISA has developed a Cyber Career Pathways Tool to enhance cybersecurity skills (The White House, 2022). The Federal Government is leading the way to ensure cybersecurity training and educational programs are developed to support national security. BCCC's new Cybersecurity Digital Forensics program will help prepare students to support the effort to defend against growing cybercrimes.

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 Cybersecurity Digital Forensics Program is being developed as a result of a capacity building $300,000 grant awarded to BCCC in 2020. The grant awarded is part of the Cybersecurity Education Diversity Initiative (CEDI) to aid HBCUs or Minority Serving Institutions (MSIs) across the US. To increase access to cybersecurity education, the National Security Agency's National Centers of Academic Excellence in Cybersecurity (NCAE-E) Program Management Office and the DoD's Office of

Industrial Policy, Small Business Program's (OSBP) Mentor Protégé Program (MPP) collaborated to ensure its program's success.

A sizable portion of the grant's funds will be used for building the program, including equipment, hardware, software, furniture, and more. A significant percentage of the grant is allocated to award 42 student scholarships to encourage students to enroll in the new program. Approximately $40,000 will be awarded to students in this program during the first year. There will be $42,000 awarded to students in the second year.

Additionally, BCCC has started the process to be a CAE candidate and in turn to be designated as a Center of Academic Excellence (CAE). This is a very esteemed designation which will be an excellent promotional tool to attract future cybersecurity and maintain current cybersecurity majors. The CAE designation will also ensure students are equipped with the necessary skills to be competitive in the cybersecurity workforce.

Baltimore City Community College is a Predominately Black Institution that sits in the heart of Baltimore City. The careers that students can enter upon completion are in a high demand across the state. Two of the four schools that students can transfer to if they want to continue their education, Bowie State University, Morgan State University, and Coppin State University are HBCUs and have a high demand for enrollment in their programs. Thus, the proposed program is relevant to PBI's and HBI's.

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

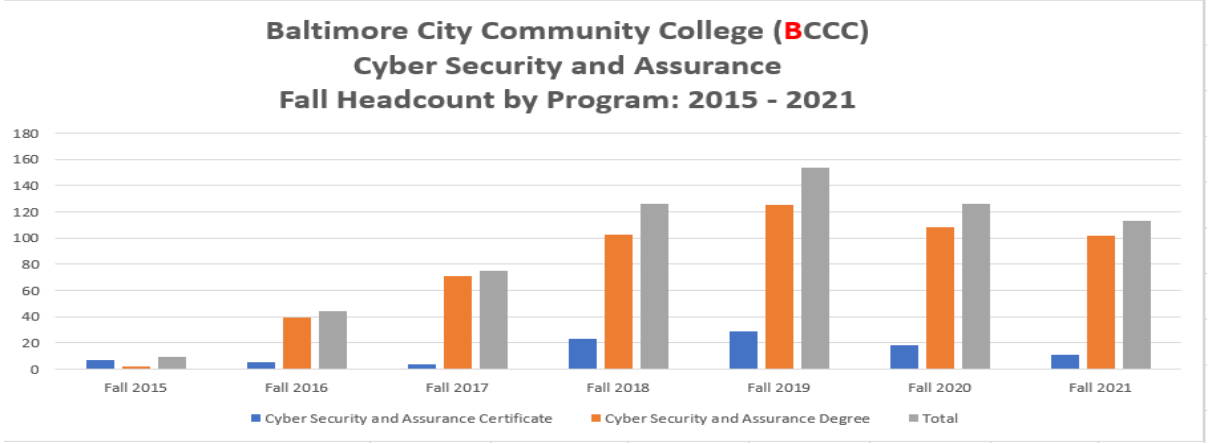
1. Discuss the program's potential impact on the uniqueness and institutional identities and missions of HBIs.

BCCC
Baltimore City Community College

Cyber Security and Assurance Credit Programs
Fall Headcount by Program: 2015 - 2021

Program	Fall 2015	Fall 2016	Fall 2017	Fall 2018	Fall 2019	Fall 2020	Fall 2021
Cyber Security and Assurance Certificate	7	5	4	23	29	18	11
Cyber Security and Assurance Degree	2	39	71	103	125	108	102
Total	*9*	*44*	*75*	*126*	*154*	*126*	*113*

Source: BCCC fall Enrollment Information System (EIS) files submitted to the Maryland Higher Education Commission.
Office of Institutional Reearch - September 2022



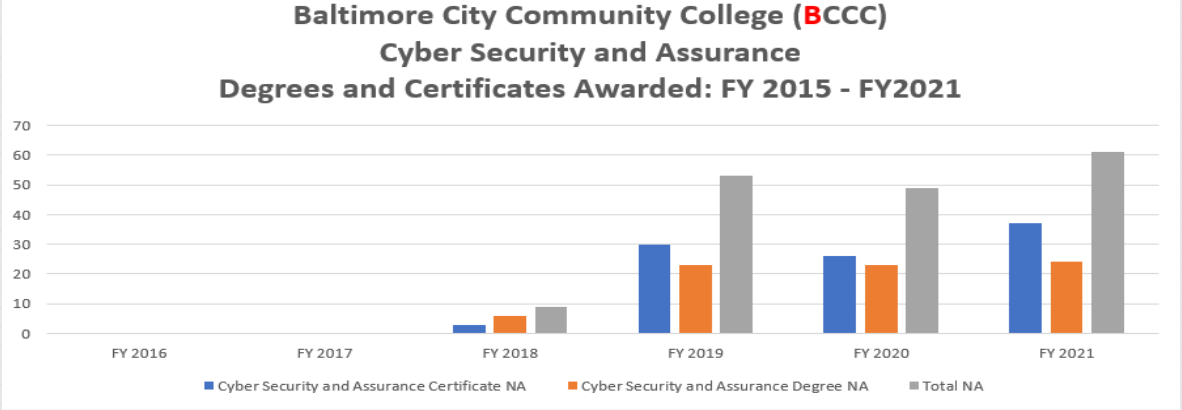
The proposed program meets the mission of HBI's. Students will gain access to a career-oriented degree for a high demand career. The following table displays an example of the successful increase in enrollment of the current cyber program and number of graduates receiving an AAS Degree and or certificate from 2015 to 2021.

BCCC
Baltimore City Community College

Cyber Security and Assurance
Degrees and Certificates Awarded: FY 2015 - FY 2021

Program	FY 2015	FY 2016	FY 2017	FY 2018	FY 2019	FY 2020	FY 2021
Cyber Security and Assurance Certificate	NA	0	0	3	30	26	37
Cyber Security and Assurance Degree	NA	0	0	6	23	23	24
Total	NA	*0*	*0*	*9*	*53*	*49*	*61*

Source: BCCC annual Degree Information System (DIS) files submitted to the Maryland Higher Education Commission annaully in August.
Office of Institutional Research - September 2022



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

1. Describe how the proposed program was established, and also describe the faculty who will oversee the program.

The Cybersecurity and Forensics program was established as a result of a Capacity Building Grant Awarded for a new Cybersecurity Program to be developed at an HBCU or Minority Serving Institution (MSI). Baltimore City Community College is recognized as an MSI. BCCC currently has a Cyber program that focusses on Cyber Security and Assurance. The new program will focus on Cybersecurity Digital Forensics. The program was developed with input and recommendations from the Cyber Faculty and the Cybersecurity Advisory Board.

The Program Coordinator, Dr. Denise Holland was responsible for writing the Proposal and being Awarded the Capacity Building Grant. Dr. Holland is a Professor over the Cyber Program and has over 20 years in Higher Education. She has served as a CEO of an Educational Consulting and Training Organization overseeing a wide range of technology services including ERP systems. Dr. Holland also has overseen multiple technical teams supporting ERP new implementation and maintenance systems including functional development for human resources, payroll, and time management; programming; systems networking; systems security; change management; and helpdesk support. Additionally, Dr. Holland has directed corporate security audit controls and reporting; chaired the organizational ERP change management system and served on the Corporate PMO Board for capital projects.

Dr. Holland has also served as the President Elect and President of a Non-Profit National Technology Organization overseeing a 60-member Board of Directors and a 13-member Executive Board. Dr. Holland also Chairs BCCC's Cyber Advisory Board and is a Board Member of BCCC's Health Information Technology (HIT) Advisory Board. Dr. Holland's leadership also extends to BCCC's Faculty Senate where she currently serves as the Instructional Technology Committee Chair. Also, she is the current Faculty Senate Vice President and has served as the Past Faculty Senate Secretary.

2. Describe educational objectives and learning outcomes appropriate to the rigor, breadth, and (modality) of the program.

The educational objectives of the program fulfill a need for expanded numbers of cybersecurity majors in the Maryland, DC, and Virginia (DMV) and all across the US. Governmental and private sector organizations have estimated shortages in cybersecurity professionals. Cyber majors are needed to monitor and defend State and Federal Government, and Private and Public Corporate systems in the US. Graduates from this program will provide resources to help satisfy this requirement.

Outcomes in addition to meeting BCCC's Core Competency outcomes over the course of the program sequence are provided. The following are the Cybersecurity Digital Forensics Learning Outcomes:

1. Identify and analyze the risks, threats, and vulnerabilities associated with digital tools, using various tools in virtual labs.

2. Define and Identify the UNIX, Window, Linux, and Android operating systems, challenges, related security Examine LAN, MAN, WAN, WLAN, circuit and packet switching, and transport protocol models, complexities of operating systems and related file management, operating system security system performance.

3. Investigate and analyze Forensic Images of Windows RAM. Examine Web Browser Artifacts. Identify and Investigate Various Network Attacks using Wireshark, Splunk, or related tools.

4. Install hardware, software, and networks; manage and support end-user computers; solve installation problem regarding operating systems, application software, hardware, mobile devices, or networks; and be able to deskside support management responsibilities.

5. Implement Role-Based Access Controls in Windows Admin Center (WAC) and Implement Password Policies using Windows Group Policy. Implement IDS/IPS functionality. Employ Host-based and Network-based IDS functionality, Remote Patch Management and Perform related functions such as database backups, file recovery, and more.

6. Classify and collect data and digital evidence; maintain audit trails for chain of custody and evidence integrity; and prepare related documentation for cases. Utilize e-mail, database, and malware forensic tools to investigate e-mail and digital crimes.

3. Explain how the institution will:

a) provide for assessment of student achievement of learning outcomes in the program
b) document student achievement of learning outcomes in the program

Courses are evaluated each semester they are taught. Faculty working in conjunction with the Director of Assessment design the tools used to measure the learning outcomes for the courses and for the programs. The two College-wide committees, the **Program Review and Evaluation Committee and the Student Learning Outcome and Assessment Committee** focus on evaluating courses, faculty, and student learning outcomes. The Program Review and Evaluation Committee (PREC) is designed to work in collaboration with the Office of the Vice President of Academic Affairs and the various academic departments to systematically assess the quality and viability of academic programs. The committee follows a set of procedures developed by the faculty and administration to ensure programs meet standards for relevance, viability, cost effectiveness, and adherence to Code of Maryland (COMAR) and Middle States Commission on Higher Education (MSCHE) requirements, program specific secondary accrediting institutions and support the College and program goals in terms of retention, graduation, and student learning outcomes. The program review is a cyclical process for evaluating and continuously enhancing the quality of BCCC programs.

The Program Review Evaluation Committee reviews programs on a 5-year cycle. New programs are added to the five-year cycle to ensure maximum data gathering. The process captures data on learning outcomes, financial data on expenditures in the program, enrollment and number of majors, graduation and retention data are collected as well. Surveys are sent to the faculty and students to gather information on satisfaction of the program. The document produced is reviewed in the Division and at the Cabinet level to discuss changes needed to the program.

The Student Learning Outcomes and Assessment (SLOA) Committee periodically assesses, supports, and maintains the SLOA process at Baltimore City Community College. The Director of Assessment and the Curriculum committee review Program Learning Outcomes to ensure they meet the COMAR guidelines. The curriculum committee reviews course learning outcomes to confirm they properly evaluate the course.

4. **Provide a list of courses with title, semester credit hours and course descriptions, along with a description of program requirements (Where is the sixth 3-credit Gen Ed in the outline below?)**

The following are the proposed courses, course IDs, Category Requirements/Course Pre-requisites for the Cybersecurity Digital Forensics Program.

Baltimore City Community College

New Program Proposal

Cybersecurity Digital Forensics

Proposed Course Sequence:

Course ID	Credits	Course Name	Category Requirement Fills:	Course Pre-Requisites
1st Semester				
PRE 100	**1**	Preparation for Academic		**None**
ENG 101 (Gen Ed Core)	**3**	English Writing		RENG 92 or appropriate course waivers or Accuplacer score
CDF 100	**3**	Cybersecurity Fundamentals	**Major**	**None**
CDF 110	**4**	An Introduction to Operating Systems (Windows, NOS & DO/S, Unix, Linux)	**Major**	**None**
CDF 115	**4**	Digital Forensics I	**Major**	**None**
	15			
2nd Semester				
MAT 107 (Gen Ed Core)	**3**	Modern Elementary Statistics		MAT 86 or MAT 92 and RENG 92 or appropriate course waivers or Accuplacer score
CDF 120	**4**	Introduction to IT Technical/ Help Desk Support	**Major**	CDF 100 and CDF 110
CDF 125	**4**	Introduction to Python	**Major**	**None**
CDF 130	**4**	Digital Forensics II	**Major**	CDF 100, CDF 110, and CDF 115
	15			
3rd Semester				
SP 101 (Gen Ed Core)	**3**	Fundamentals of Speech Communication		RENG 92 or appropriate course w waivers or Accuplacer score
HLF-Elective	**2**	Health and Life Fitness		**None**
CRJ 210 (Interdisciplinary and Emerging Issues Core)	**3**	Investigative Principles and Concepts		**None**
CDF 230	**4**	Fundamentals With Networking	**Major**	CDF 100, CDF 110, and CDF 120
CDF 240	**4**	Digital Forensics III	**Major**	CDF 115 and CDF 130
	16			
4TH Semester				
Gen Ed Core	**3**	Social and Behavioral Sciences		ENG 82 or RENG 92
BPS-Elective (Gen Ed Core)	**3**	Biological and Physical Sciences		MAT 86 or MAT 92 and RENG 92 or appropriate course w waivers or Accuplacer score
CDF 250	**4**	Network Intrusion and Penetration Testing	**Major**	CDF 230
CDF 260	**4**	Digital Forensics Capstone	**Major**	CDF 130 and CDF 240
	14			
Total Credits	**60**			

Baltimore City Community College				
New Program Proposal				
Cybersecurity Digital Forensics Certificate				
Proposed Course Sequence:				
Course ID	**Credits**	**Course Name**	**Category Requirement Fills**	**Course Pre-Requisites**
1st Semester				
PRE 100	**1**	Preparation for Academic Achievement		**None**
CDF 100	**3**	Cybersecurity Fundamentals	**Major**	**None**
CDF 110	**4**	An Introduction to Operating Systems (Windows, NOS & DO/S, Unix, Linux)	**Major**	**None**
CDF 115	**4**	Digital Forensics I	**Major**	**None**
	12			
2nd Semester				
CDF 120	**4**	Introduction to IT Technical/Help Desk Support	**Major**	CDF 100 and CDF 110
CDF 130	**4**	Digital Forensics II	**Major**	CDF 100, CDF 110, and CDF 115
	8			
3rd Semester				
CDF 230	**4**	Fundamentals With Networking	**Major**	CDF 100. CDF 110. and CDF 120
CDF 240	**4**	Digital Forensics III	**Major**	CDF 115 and CDF 130
	8			
Total Credits	**28**			

The following are the course catalog descriptions for the proposed/new courses for the Cybersecurity Digital Forensics Program.

PRE 100 – Preparation for Academic Achievement--1 credit - 15 lecture hours
Prerequisites: None
All new, degree- or certificate-seeking students and students entering with fewer than 15 credits are required to complete the College's Orientation course. The purpose of this course is to provide information necessary for academic success in college and to give students knowledge of what to expect in their classes. Students learn strategies that empower them to achieve success.

ENG 101: ENGLISH WRITING--3 credits--45 lecture hours
Meets Category V General Education Requirements; D and F Grades are not awarded. A minimum of a C grade is required to pass the class.
Prerequisites: ENG 82 or RENG 92 or appropriate course waivers or ACCUPLACER scores. Non-native English speakers pursuing an academic certificate or degree take a mandatory sequence of courses in core skill areas (ELI 80W; ELI 80R; ELI 81G; ELI 81W; ELI 82G; and ELI 82W). Successful completion of ELI 82G and ELI 82W courses is required before taking ENG 101. (Details under English Language Instruction).

This course offers classroom instruction and practice in the skills necessary to write effective informative and persuasive essays, to understand the primary principles of scholarly inquiry and research, and to use the conventions of documentation. Students learn to use the conventions of standard written American English to establish a clear purpose in their writing, to develop their purpose with adequate and pertinent evidence, and to adapt their presentations to a range of audiences. The preparation of regularly scheduled essays is required, as is revision and editing of instructor-evaluated work.

(X) CDF 100: CYBERSECURITY FUNDAMENTALS--3 credits--45 lecture hours
Prerequisites: None
Cybersecurity Fundamentals provides an overview of major topics and trend in the cybersecurity field. Students will learn the core components involving cybersecurity. The main topics covered include Securing the Operating Systems, Malware and Antivirus software, and Internet Security. Other central topics include Security on Social Networking Sites, Securing Email Communications, Securing Mobile Devices, Securing the Cloud, and Securing Network Connections. Finally, students will be introduced to leading and overall understanding of Data Backup and Disaster Recovery processes, requirements, and best practices.

(X) CDF 110: AN INTRODUCTION TO OPERATING SYSTEMS (WINDOWS, NOS & DO/S, UNIX, LINUX)-4 credits--(60 hours, combined lecture and lab)
Prerequisites: None
An Introduction to Operating Systems provides an overview to the operating systems, how operating systems work with hardware, software, and peripheral devices, the history of operating systems and more. Students learn the management of main memory resources, single processor and multiprocessor management, and managing available devices without conflicts. In addition, student learn about file management, and files with system instructions, security of the operating systems, and system's management. Students also learn about specific operating systems including UNIX, Windows, Linux, Android operating systems, and network operating systems.

(X) CDF 115: DIGITAL FORENSICS I--4 credits--(60 hours, combined lecture and lab)
Prerequisites: None
Digital Forensics I provides an overview of computer forensics fundamentals topics. Students will learn about the investigative process involving digital forensics including understanding hard drives and file systems, data acquisition and duplication, defeating anti-forensics techniques. Also, students will learn the fundamentals of defeating anti-forensics techniques; Windows Linux, Mac, Network, Dark Web, Malware Forensics. Students will also learn techniques to investigate Web attacks and e-mail crimes.

SP 101: FUNDAMENTALS OF SPEECH COMMUNICATION--3 credits—45 lecture hours
Meets Category I General Education Requirements.
Prerequisites: ENG 82 or RENG 92 or appropriate course waivers or ACCUPLACER scores
Human communication in both a theoretical and an experiential framework is investigated. Areas of study include communication theory, interviewing, and informative and persuasive speaking. Students prepare, and present informative and persuasive speeches based on classic models. Theory, preparation, appropriate form, and delivery are studied and evaluated. Each student is responsible for at least one formal interview and three speeches. Several impromptu speeches may be included.

(X) CDF 120: INTRODUCTION TO IT TECHNICAL/HELP DESK SUPPORT—4 credits--(60 hours, combined lecture and lab)
Prerequisites: CDF 100 and CDF 110
Introduction to IT Technical/Help Desk Support provides an overview to the popular and evolving field of help desk support. Students learn the technical core components needed for Information Technology (IT) help desk functions. The Core Topics covered include CompTIA A+ Core 1 and A+ Core 2 Exam Objectives Mapped to Chapters. Additionally, students learn about mother- boards, memory, power supplies, hard drives and storage devices, setting up networks, troubleshooting, and how to disassemble and reassemble computers. Other concepts discussed include end user computing, installation of end user computer systems, documentation for end users, computer facilities management, and common support problems and information resources for user support. Students are also introduced to leading help desk support software.

(X) CDF 125: INTRODUCTION TO PYTHON--4 credits--(60 hours, combined lecture and lab)
Prerequisites: None
Introduction to Python provides an introduction to the Python fundamentals. Students will learn about control statements, explore controlling program flow, and work with structured programs via functions. Python Fundamentals problem-solving skills for building efficient applications. Students learn about data structures and study ways to correctly store and represent information; object-oriented programming (OOP) concepts of abstraction, encapsulation of data, inheritance, and polymorphism. The course also includes an overview of how imports, modules, and packages work in Python, error handling, preventing apps from crashing, and file manipulation.

(X) CDF 130: DIGITAL FORENSICS II--4 credits--(60 hours, combined lecture and lab)
Prerequisites: CDF 100, CDF 110, and CDF 115
Digital Forensics II provides an expanded concepts of computer forensics in today's world. Topics will include the digital forensics investigative process, understanding hard drives and file systems, data acquisition and duplication, defeating anti-forensics techniques. Also, students will learn the fundamentals of defeating anti-forensics techniques; Windows Linux, Mac, Network, Dark Web, Malware Forensics. Students will also learn techniques to investigate Web attacks and e-mail crimes.

HLF Elective – Health and Life Fitness--2 credit - 30 lecture hours
Prerequisites: None
Students can choose any two credit or two one credit HLF electives to fulfill this requirement.

CRJ 210: INVESTIGATIVE PRINCIPLES AND CONCEPTS-3 credits--45 lecture hours
Prerequisites: None
Students are introduced to criminal investigation: basic investigative techniques, preliminary investigation, crime scene protection and search, collection of physical evidence, documentary evidence, interviews and interrogations, and operations such as raids and undercover work.

MAT 107: MODERN ELEMENTARY STATISTICS--3 credits--45 lecture hours Meets Category IV General Education Requirements.
Prerequisites: MAT 82 or MAT 92; RENG 92 or appropriate course waivers or ACCUPLACER scores
Topics useful to students in business and social sciences are covered with an emphasis on applications rather than theory. Topics include sets, the Cartesian coordinate system, functions and graphs, exponents and logarithmic functions, systems of linear equations and matrices, linear inequalities and linear programming, including the simplex method, probability, including conditional probability and Bayes' formula, and probability distribution.

(X) CDF 230: FUNDAMENTALS WITH NETWORKING--4 credits--(60 hours, combined lecture and lab)
Prerequisites: CDF 100, CDF 110, and CDF 120
Fundamentals With Networking provides an overview of network security fundamentals topics. Students will learn about current and future techniques to detect and secure the network and digital devices connected to the network. Also, students will learn how to identify, authenticate, authorize users for network access. Additional content includes Network Security Controls for Administrators and Technical resources. Students will also learn how to monitor, security on various digital devices such as mobile phones, PCs, and Laptops. Finally, Network Security Physical Controls will be discussed.

(X) CDF 240: DIGITAL FORENSICS III--4 credits--(60 hours, combined lecture and lab)
Prerequisites: CDF 115 and CDF 130
Digital Forensics III provides an advanced concepts of computer forensics in today's world. Topics will include the digital forensics investigative process, understanding hard drives and file systems, data acquisition and duplication, defeating anti-forensics techniques. Also, students will learn about database forensics and how to defeat anti-forensics techniques; Windows Linux, Mac, Network, Dark Web, and Malware Forensics. Students will also learn techniques to investigate Web attacks and e-mail crimes. Investigating Cloud Forensic is also discussed.

GEN ED CORE - Social and Behavioral Sciences Elective--3 credit - 45 lecture hours
Prerequisites: ENG 82 or RENG 92
Students can choose any 100 level three credit Social and Behavioral Sciences Elective to fulfill this requirement.

BPS-ELECTIVE - Biological and Physical Sciences Elective--3 credit - 45 lecture hours
Prerequisites: MAT 86 or MAT 92 and RENG 92 or appropriate course waivers or Accuplacer score
Students can choose any 100 level three credit Biological and Physical Sciences Elective to fulfill this requirement.

(X) CDF 250: NETWORKING INTRUSION AND PENETRATION TESTING--4 credits--(60 hours, combined lecture and lab)
Prerequisites: CDF 230
Networking Intrusion and Penetration Testing provides an overview of network security strategies and defense topics. Students will learn about current and future techniques to detect and secure the networks and digital devices connected to the network. Also, students will learn about Network Perimeter Security, Endpoint Security-Linux Systems, Mobile-Devices, Windows Systems, and IoT devices. Students will also learn about Administrative Application, Data, Enterprise Virtual Network/Cloud, and Wireless Security. Finally, students will gain knowledge regarding Network Monitoring and Analysis.

(X) CDF 260: DIGITAL FORENSICS CAPSTONE--4 credits--(60 hours, combined lecture and lab)
Prerequisites: CDF 130 and CDF 240
Digital Forensics Capstone is the final and inclusive course for the Cybersecurity Digital Forensics Degree program. The course content provides a building block of skills obtained in prior semesters such as cybersecurity networking and defense strategies; digital forensics investigative techniques; network authentication, intrusion, monitoring, and controls; and performing effective digital analysis and forensics investigations. Students will develop a Capstone Project as a team, building on monthly deliverables. The course content also exposes students to the key knowledge areas covered in the CHFI-CQ-EXAM-PREP and CHFIv10 Exam Prep.

5. **Discuss how general education requirements will be met, if applicable.**
   The Cybersecurity Digital Forensics Program was created in alliance with the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. The program provides students with practical experience in understanding the threats and dangers, security assessments and analysis to a wide range of different businesses, and the steps that need to be taken to mitigate these vulnerabilities by using state-of-the-art technology. The program prepares students for vendor-specific or commercially available security certifications. The program also emphasizes the need to build a wall between our information and those that want to exploit it. The recurring events such as virus and worm attacks and the success of criminal attackers, illustrate the weaknesses in current information technologies and the need for heightened security of these systems.

   As an AAS degree program, students will be required to complete the minimum of 18 credits in General Education courses. Specific courses have been identified within the curriculum to meet the COMAR requirements of General Education and Learning

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

   The program does not have a selective admissions policy for the cyber program other than a high school diploma, GED Diploma, or high school transcript for dual enrollment students.

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

   BCCC is not partnering with any external resources for this new program proposal.

8. **Provide assurance and any appropriate evidence that 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 aid resources, and costs and payment policies.**

   The program description in the catalog will be as follows: Cybersecurity Digital Forensics Program provides students with practical experience in understanding the threats and dangers, security assessments and analysis to a wide range of different businesses, and the steps that need to be taken to mitigate these vulnerabilities by using state-of-the-art technology. The program prepares students for vendor-specific or commercially available security certifications. The program also emphasizes the need to build a wall between our information and those that want to exploit it. The recurring events such as virus and worm attacks and the success of criminal attackers illustrate the weaknesses in current information technologies and the need to heighten security of these systems.

   The BCCC's Website will include up-to-date list of course descriptions, prerequisites, scheduled courses by semester, degree requirements, related teaching modalities, advising, and more. The contact information for the teaching faculty and program coordinator's information will also be maintained on the website. Other support services listed on the website include financial aid, tutoring, registration, and graduation planning.

   BCCC's academic affairs, student affairs, and student support services will work collaboratively to ensure the best possible student experience for students enrolled in the program. This includes supporting the new cyber lab, a dedicated cyber lab server, hardware and software, lab tools, and instructional materials. Course materials used will be easily accessible through BCCC's Learning Management System. In addition, updated marketing materials will be displayed on the BCCC website and throughout the community to outline the new program, benefits, skills to be obtained, and related internship and career opportunities. Finally, the program coordinator will meet with students to plan their initial and ongoing course registrations to ensure students stay on a path that leads to their targeted graduation completion date.

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.**

   BCCC's marketing staff works together with academic affairs and college-wide student support services to ensure descriptive, concrete, and well designed, and well-planned materials are displayed on the website for each academic program. Highlights of materials available for students include the overall program description, the program education plan for the degree and certificate programs, benefits of program and potential career opportunities, and program coordinator contact information. In addition, the college catalog outlining the program details will also be accessible from the website.

H. Adequacy of Articulation

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

   This is a new proposal for the Cybersecurity Digital Forensics program. Thus, there are no current Articulation Agreements in place for this program. However, there are articulation agreements with other four-year colleges and universities for the current Cyber Security and Assurance Program. Future Articulation Agreements can be planned.

I. Adequacy of Faculty Resources (as outlined in COMAR 13B.02.03.11).

1. **Provide a list of current faculty (and areas of expertise) who will teach in the program. List faculty by rank required for full implementation of the program. Indicate which additional faculty members are to be hired and describe their qualifications.**

   Dr. Denise P. Holland – Is a fulltime faculty member and Program Coordinator for the Cybersecurity and Assurances program at BCCC with over 20 years of experience in teaching information technology/cyber courses. Dr. Holland is an Assistant Professor and holds a Masters in Cybersecurity, a Master's in Information Technology, and a PhD in Organization and Management with a concentration in Leadership. Dr. Holland is also certified in Approva's Enterprise Security Controls Management software for ERP systems. In addition, Dr. Holland has a wide range of technology industry experience in directing ERP systems functional, technical, security, networking and programming resources; project management; information systems audit controls; and change/problem management. Dr. Holland will be able to teach all of the CDF courses.

   BCCC is currently in the process of hiring a second full-time cybersecurity faculty member, with credentials in the following area:

   - A Master's degree in Cybersecurity or Information Technology with a concentration on cybersecurity-related courses
   - Four years of teaching experience, preferably in a Community College using various modalities
   - Demonstrated experience in teaching advising

- Work experience in a related cybersecurity field
- Experience in effectively using an LMS in a Community College
- Cybersecurity-related certifications such as CompTIA's A+, Net+, Sec+, CEH, CISSP, CCNA or other relevant Cybersecurity certifications.

Adjuncts Faculty currently teaching cyber courses and future adjuncts hired to teach in the program and will need to hold a Masters in Cybersecurity or Information Systems/ Technology. They must also have previous experience teaching in either Cybersecurity or Digital Forensics courses. The following list reflects current Adjunct Faculty teaching Cyber courses. These faculty members have credentials to teach courses in the new Cyber Program. In addition to the educational credentials, the full-time and adjunct faculty have extensive information technology/cybersecurity related experience in private, public, and state/federal government organizations.

The following table highlights the Full-time and Adjunct Faculty qualified and available to teach the courses in the new Cybersecurity Digital Forensics Program.

Faculty Name	Status	Degree(s)	Institution	Courses to be Taught
Dr. Denise Holland	Full-time	PhD in Organization and Management with a concentration in Leadership	Capella University	CDF100, CDF110, CDF115, CDF120, CDF125, CDF130, CDF230, CDF240, CDF250, CDF260
		MS Cyber Security Technology	UMGC	
		MS IT/Project Management	AIU	
		BA Business/Computer Science	Notre Dame University of Maryland	
		Approva Risk and Compliance	Certification	
Jackie Stanton	Adjunct	MS Information Assurance	Capitol College	CDF100, CDF110, CDF130, CDF240
		B.S. Applied Information Technology	University of Baltimore	
		AAS Computer Information Systems	BCCC	
Neal Helton, Jr.	Adjunct	Doctoral Candidate	Capella University	CDF100, CDF110, CDF115, CDF120, CDF125, CDF100, CDF130, CDF230, CDF240, CDF250, CDF260
		M.S. Information Systems	University of Phoenix	
		A+, Net+, Sec+, CCENT	Certifications	
Dr. Lamonte Tyler	Adjunct	D.IT	Walden University	CDF100, CDF110, CDF115
		M.S. IT	Walden University	
		DoD TS/SCI, PMP, AWA, CISM, CASP	Certifications	
Dr. Geselle Archie	Adjunct	D. International Business	Argosy University	CDF100, CDF110, CDF115
		M.S. Information Systems	Strayer University	

		B.S. Information Systems	Morgan State University	
Dwayne Spriggs	Adjunct	M.S. Public Administration	Syracuse University	CDF100, CDF110, CDF115, CDF120, CDF125, CDF130, CDF230, CDF240, CDF250, CDF260
		B.S. Information Systems Management		
		ITIL V4, CISSP	Certification	
		Public Trust	Clearance	
Samuel Bowden	Adjunct	M.S. Cybersecurity/Digital Forensics Investigations	UMGC	CDF100, CDF115, CDF130, CDF240
		M.S. Management	John's Hopkins University	
		B.S. Criminal Justice	Coppin State University	
		CASP, CCNA, ECH	Certifications	
Tolorunju Eko	Adjunct	M.S. Cybersecurity	UMBC	CDF100, CDF115, CDF130, CDF240
		M.A. Education Administration	Obafemi Awolowo University	
		B.S. ED Mathematics	Obafemi Awolowo University	
		Secret	Clearance	
Curtis Roberts	Adjunct	M.S. Information Systems	Strayer University	CDF100, CDF115, CDF130, CDF230, CDF240
		M.A. Educational Technology	North Carolina Central University	
		B.S. Computer Information Systems	Strayer University	
Kimberly Holloway	Adjunct	M.S. Information Systems	UMGC	CDF100, CDF115, CDF130, CDF230, CDF240
		B.S. Cybersecurity	John's Hopkins University	
Azubuike Enwere	Adjunct	M.S. Cybersecurity	Bowie State University	CDF100, CDF110, CDF115, CDF120, CDF125, CDF130, CDF230, CDF240, CDF250, CDF260
		B.S. Computer Technology and Security	Bowie State University	
		A.A. Cybersecurity	Howard Community College	

2. **Demonstrate how the institution will provide ongoing pedagogy training for faculty in evidence-based practices, including training in:**

   a) **Pedagogy that meets the needs of the students**

   The College holds institutional development days at the beginning and end of the academic semesters in the Fall – August and December; and Spring - January and May. During these workshops, faculty receive ongoing training regarding assessments,

curriculum development, and the learning management system. Faculty also discuss best practices in teaching and learning tools. Additional professional development occurs during the semesters on similar topics. Finally, the college has sponsored faculty to attend ACUE courses and conferences to receive training, professional development, and plans to continue this practice to support faculty.

b) The learning management system

BCCC's e-Learning team schedules and conducts training regarding Canvas tools, loading courses into the Canvas shell, Canvas tips and best practices, grading strategies, integration tools, and more. The training schedules are advertised on the Canvas home page for faculty and students. Canvas quick reference guides and course navigation tools and videos are available and are incorporated into Canvas courses for students.

c) **Evidence-based best practices for distance education if offered.**

BCCC offers multiple teaching modalities to support its student demographics. While the majority of courses are taught synchronously, the college offers some asynchronous courses online. The college requires full-time and part-time faculty to successfully complete an online training course to ensure student success. In addition, BCCC has a College-wide Instructional Technology Committee that offers training throughout the semesters for professional development.

J. Adequacy of Library Resources (as outlined in COMAR 13B.02.03.12)

1. **Describe the library resources available and/or the measures to be taken to ensure resources are adequate to support the proposed program.**

The Librarian and the cyber faculty met to discuss library needs for the new program. It was determined that because the materials are all available online to all students, no print materials are required to be maintained in the Library. However, the Library is available for students to use computers for homework, access the online database to conduct research for journal articles, and more. The Bard Library subscribes to a 24/7 cooperative virtual reference service, BCCC LibChat, which connects students to librarian assistance outside of library operational hours.

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 new Cybersecurity Digital Forensics program is being developed as a result of an NSA capacity building grant award. An existing classroom will be used as a dedicated classroom and lab for cyber students. The classroom will be equipped with all new desks, chairs, dual monitors, PCs and related peripherals. A dedicated server will be installed in the lab as well. The grant funds have been budgeted to cover all equipment costs. The faculty have dedicated office space equipped with a PC, monitor, camera, speakers, and related computer peripheral devices to conduct training, attend virtual training, and conduct student advising in person or virtually.

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**

BCCC faculty, staff and students are able to use the college's internal email server and network for their incoming and outgoing email. The BCCC faculty and staff use the @bccc.edu and students use the @student.bccc.edu email domains. Students are encouraged to use their school email address in all their communication with the Faculty and for creating accounts with approved third party vendors for their classes. Faculty use their BCCC e-mail for all college related communications. In addition, the e-mail server, BCCC students and Faculty have access to the Learning Management

Systems (LMS) – Canvas Inbox to communicate with students. Canvas is the college's office LMS used to house all course material, integrate with third party software, take quizzes and tests, access interactive course links, and more. Students have access to the LMS via the Web browser and via their cell phone App.

L. Adequacy of Financial Resources with Documentation (as outlined in COMAR 13B.02.03.14)

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 l: Resources Narrative

1. Reallocated Funds

   No funds are anticipated to be reallocated for the new program.

2. Tuition and Fee Revenue

   It is assumed that tuition and fees will be constant in the next five years. The in-state tuition rate is currently $110 per credit hour and a total fee of $62 (consisting of consolidated fees of $15 per credit hour, technology fee $10 per credit hour, one time per semester registration fee of $26 and one time per semester of facilities capital fee of $11) for a total of $172 of which $25 are fees per credit hour and $37 are fees per semester. These were used in calculating the revenue: with 24 credits per year for full-time students and 12 credits per year for part-time students. In addition, credits taken between 12 and 18 per semester are at the same tuition and fee rate of 12 credits. The enrollment projections are based on the current performance of the Cybersecurity Assurances program.

3. Grants and Contracts

   Baltimore City Community College received a grant from the NSA (National Security Association) to fund the development of the Cybersecurity Digital Forensics program. The grant has funds to pay for scholarships for students in the first two years the program will be offered.

4. Other Sources

Baltimore City Community College is the only state funded community college in the state of Maryland. The college will receive approximately $7,573 per student FTE.

5. Total Year

Based on a conservative estimate of resources, the Cybersecurity Digital Forensics Program at Baltimore City Community College is expected to have adequate resources from its inception to maintain a successful and expanding academic program.

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)	$54,604	$109,208	$163,812	$218,416	$273,020
a. Number of F/T Students	11	22	33	44	55
b. Annual Tuition/Fee Rate	$3,314	$3,314	$3,314	$3,314	$3,314
c. Total F/T Revenue (a x b)	$36,454	$72,908	$109,362	$145,816	$182,270
d. Number of P/T Students	11	22	33	44	55
e. Credit Hr. Rate	110	110	110	110	110
f. Annual Credit Hrs.	15	15	15	15	15
g. Total P/T Revenue (d x e x f)	$18,150	$36,300	$54,450	$72,600	$90,750
3. Grants, Contracts, & Other External Sources	$44,000	$44,000	0	0	0
4. Other Sources	0	0	0	0	0
TOTAL (Add 1 – 4)	$98,604	$153,208	$163,812	$218,416	$273,020

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 : Expenditures Narrative

1. Administrative Staff (# FTE, Salary, and Benefits): No additional staff will be needed.
2. Support Staff (# FTE, Salary, and Benefits): No additional staff will be needed.
3. Equipment: Grant funds that were received to develop and implement the program will be used to purchase any needed equipment.
4. Library: No expenditures are anticipated.
5. New and/or Renovated Space: No expenditures are expected.
6. Other Expenses: Funding will be available for professional development for faculty members who teach in the Cybersecurity Digital Forensic program pathway.
7. Total Year: Based on a conservative estimate of expenditures, the Cybersecurity Digital

Forensic program at Baltimore City Community College is expected to have adequate resources to cover the costs of this academic program.

TABLE 2: EXPENDITURES					
1. Faculty (b + c below)	88,000	163,800	163,800	163,800	163,800
a. # FTE	0.5	1.5	1.5	1.5	2.0
b. Total Salary	70,000	130,000	130,000	130,000	130,000
c. Total Benefits	18,200	33,800	33,800	33,800	33,800
1. Faculty (b + c below)	88,000	163,800	163,800	163,800	163,800
2. Admin. Staff (b + c below)	0	0	0	0	0
a. # FTE	0	0	0	0	0
b. Total Salary	0	0	0	0	0
c. Total Benefits	0	0	0	0	0
3. Support Staff (b+ c below)	0	0	0	0	0
a. # FTE	0	0	0	0	0
b. Total Salary	0	0	0	0	
c. Total Benefits	0	0	0	0	0
4. Technical Support and Equipment*	125,508	0	0	0	0
5. Library	0	0	0	0	0
6. New or Renovated Space	0	0	0	0	0
7. Other Expenses	0	0	0	0	0
TOTAL (Add 1 – 7)	213,508	163,800	163,800	163,800	163,800

*****The equipment cost are funded by the NSA Grant Award.

M. Adequacy of Provisions for Evaluation of Program (as outlined in COMAR 13B.02.03.15).

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

As previously discussed in Section A 4b, BCCC has a three-pronged approach to ensure courses and students learning outcomes. BCCC takes full advantage of the internal Program Review and Evaluation (PREC) requirements. This periodic review ensures appropriate guidelines for courses and programs adhere to MHEC and COMAR standards. The process also reviews faculty credentials teaching the credited courses to ensure they have met the educational requirements to effectively deliver instructional materials in multiple modalities in higher educational. Additionally, faculty are evaluated annually to assess the quality, proficiency, and effectiveness of the faculty teaching in their discipline.

2. **Explain how the institution will evaluate the proposed program's educational effectiveness, including assessments of student learning outcomes, student retention, student and faculty satisfaction, and cost-effectiveness.**

   Part of the internal Program Review and Evaluation (PREC) requirements includes distributing surveys to students, faculty, and program advisory board members regarding the program, courses appropriate experience and knowledge of the faculty, delivery effectiveness, quality of material covered, teaching facilities and tools, working environment, and more. The surveys are completely anonymous and provide feedback to the faculty, program chair, associate dean, dean, and vice president of academic affairs to determine if there are any required changed to be made. Also, faculty complete student learning outcomes and assessments for each course at the end of each semester. Data is aggregated and uploaded into the internal Assessment Tool – TracDat. As applicable, changes may be required regarding student learning outcomes, teaching modalities, faculty course schedules, equipment, and more based on consistency in the feedback from the surveys. The Curriculum and Instruction Committee also communicates with faculty, program coordinators, associate deans, and deans to review and update the college-wide syllabi as needed.

N. Consistency with the State's Minority Student Achievement Goals (as outlined in COMAR 13B.02.03.05).

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

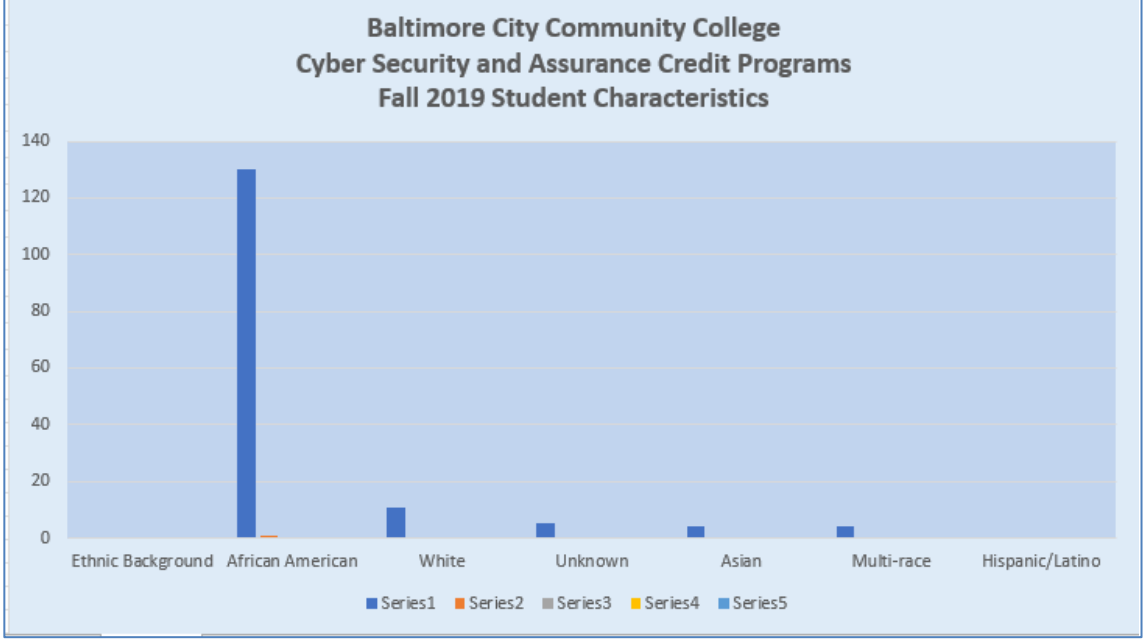
   BCCC is a Minority Serving Institution (MSI). The Cybersecurity Digital Forensics Program is being developed as a result of a capacity building grant awarded as part of the Cybersecurity Education Diversity Initiative (CEDI) to aid HBCUs or Minority Serving Institutions (MSIs) across the US to increase access to cybersecurity education. , the National Security Agency's National Centers of Academic Excellence in Cybersecurity (NCAE-E) Program Management Office and the DoD's Office of Industrial Policy, Small Business Program's (OSBP) Mentor Protégé Program (MPP) collaborated to ensure its program's success.

   The BCCC Cyber Program Coordinator meets with cyber students to plan out their academic course schedules throughout their educational journey. Follow-up meetings are scheduled to update the plan if changes in schedules, student availability impact the planned course schedule. Students are apprised of BCCC resources readily available to them including financial aid, tutoring, communication support, and more.

   The current Cyber Security and Assurance program has been successful and has contributed greatly to the increasing graduation rate. The majority of BCCC's students are African American at 84% of the total Cyber population. This demonstrates a need to ensure this community is well-served through BCCC support systems.

Baltimore City Community College
Cyber Security and Assurance Credit Programs

Ethnic Background		
African American	130	84.4%
White	11	7.1%
Unknown	5	3.2%
Asian	4	2.6%
Multi-race	4	2.6%
Hispanic/Latino	0	0.0%
Total	154	100.0%



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

2. 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.

This program is not identified as a low-enrolled program. Also, it is not related to a low enrolled program. Currently there are no plans to reallocate funds from low enrolled programs to the new program,

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

1. Provide affirmation and any appropriate evidence that the institution is eligible to provide Distance Education.

BCCC anticipates the majority of the courses in the new program to be offered in a face-to-face environment. However, since the courses in this program utilize online virtual environment tools, the program courses are able to be taught in an online modality. The current Cyber Security and Assurance Program was successfully taught in an online synchronous setting for two years during the 2020 to 2022 academic years. All reading materials (e-Books), lab assignments, quizzes, tests, and more are all accessible in an online setting. This includes the tools used in the virtual labs.

2. **Provide assurance and any appropriate evidence that the institution complies with the C-RAC guidelines, particularly as it relates to the proposed program.**

BCCC has the approved mission to deliver quality affordable education that assists students in meeting their personal and professional goals using contemporary educational practices. The pandemic has allowed the College to expand its footprint in the online education sphere and through doing so has been able to better sustain enrollment options for students in an era of declining traditional enrollments. Being that the institution serves a diverse population, many of whom work or have family obligations that restrict their ability to attend more traditional classes, online education offered at BCCC provides the opportunity for students to meet its core mission to serve the community.

The E-Learning department advocates and supports online learning efforts through participation in Academic leadership processes and works closely with Institutional Assessment. The department works closely with faculty leadership through the Instructional Technology Committee, and Program Review Committee. BCCC is a member institution of Quality Matters and the E-Learning department provides support and training to faculty in the areas of course design and delivery that are consistent with the Quality Matters rubric and online learning best practices. Courses offered online must meet the same learning outcomes and course objectives as their traditional counterparts and are evaluated using the same process as face-to-face courses. Program review is an internal peer-reviewed process to assess the effectiveness of all programs, including those with online offerings. Additionally, the College subscribes to an assessment and outcome evaluation software, currently Nuventive Improve, that assists program coordinators and academic leadership in evaluating the effectiveness of meeting course and program outcomes to better assist in analyzing areas for improvement to meet the College's mission of delivering quality education.

BCCC provides regular faculty development in the area of teaching online and maintains a self-paced training course to ensure adequate preparation to teach online. The E-Learning department owns and manages the course, refreshing periodically as technologies and pedagogies change at the College. The list of faculty who meet these training requirements, or their equivalent, is provided to the academic deans in each area for scheduling to teach online courses.

BCCC provides support to online students through the use of the College's virtual help desk. Tutoring and academic support is provided to online students through virtual tutoring provided by BCCC's tutors and through a tutoring consortium for the east coast. BCCC provides tutoring services in key courses across majors and the College is constantly reviewing what additional course areas can be supported.

BCCC has an E-Learning department dedicated to supporting faculty and student success in online education. The department is led by the Director who holds a Master's Degree in Distance Education and has twelve years of higher education experience in delivering quality education both online and in the classroom. The department includes a Coordinator who is an instructional technology expert with five years of experience supporting faculty to leverage technology in their teaching, creating and curating digital artifacts, and producing quality professional development for faculty in the area of online education. The Student Success Specialist at BCCC focuses on supporting student use of technology to meet educational goals. This cohesive team interacts with all areas of academics and student support to ensure the College meets its obligations to support, sustain, and expand online education delivery.

BCCC utilizes a variety of methods to ensure that the student who enrolls in a course is the student who completes the work in an online course. BCCC accomplishes this using individual usernames and passwords, Respondus, LLC's Lockdown Browser, Monitor services, Turnitin anti-plagiarism service embedded within the College's learning management system. In synchronous online courses, web conferencing software provides the ability to video verify student attendance.

References

Biden, Jr., J. R. (2021). *Executive Order on Improving the Nation's Cybersecurity*. The White House. Retrieved from https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Bureau of Labor Statistics, U.S. Department of Labor, *Occupational Outlook Handbook*, Computer Systems Analysts, at https://www.bls.gov/ooh/computer-and-information-technology/computer-systems-analysts.htm (visited *September 08, 2022*).

Holmes, R. (2022). *5 Key Risk Indicators Your Organization Should Monitor*. Bitsight Technologies, Inc. Retrieved from https://www.bitsight.com/blog/key-risk-indicators

Mandy, O, Lee, C, Addiscott, R, Scholtz, T, & Gopal, D. (2022). *Cybersecurity Leaders Are Losing Control in a Distributed Ecosystem*. Gartner, Inc. Retrieved from https://www.gartner.com/doc/reprints?id=1-29FBE5ZT&ct=220317&st=sb

Md. Code, Educ. § 10-205 (2022). *Current with changes from the 2022 Legislative Session*. Md. Code, Educ. § 10-205 - Section 10-205 - Goals . Retrieved from https://casetext.com/statute/code-of-maryland/article-education/division-iii-higher-education/title-10-definitions-and-maryland-charter-for-higher-education/subtitle-2-maryland-charter-for-higher-education/section-10-205-goals

Meeks, J. (2022). *Is a Cyber Security Associate Degree Worth It? [2022 Guide]*. Degree Planet. Retrieved from https://www.degreeplanet.com/is-a-cyber-security-associate-degree-worth-it/

The White House (2022). *CYBERSECURITY TRAINING & EXERCISES*. Cybersecurity & Infrastructure Security Agency. Retrieved from https://www.cisa.gov/cybersecurity-training-exercises

U.S. Bureau of Labor Statistics. (2022). *Information Security Analysts*. Occupational Outlook Handbook. Retrieved from https://www.bitsight.com/blog/key-risk-indicators