MARYLAND HIGHER EDUCATION COMMISSION
ACADEMIC PROGRAM PROPOSAL

PROPOSAL FOR:

__X__ **NEW INSTRUCTIONAL PROGRAM**

_____ **SUBSTANTIAL EXPANSION/MAJOR MODIFICATION**

_____ **COOPERATIVE DEGREE PROGRAM**

_____ **WITHIN EXISTING RESOURCES or** _____ **REQUIRING NEW RESOURCES**

(For each proposed program, attach a separate cover page. For example, two cover pages would accompany a proposal for a degree program and a certificate program.)

Community College of Baltimore County

Institution Submitting Proposal

Fall, 2017

Projected Implementation Date

Associate of Applied Science Degree

Award to be Offered

Digital Forensics

Title of Proposed Program

43.0016

Suggested CIP Code

Suggested HEGIS Code

School of Technology, Arts & Design

Department of Proposed Program

Noell Damron

Name of Department Head

Noell Damron	ndamron@ccbcmd.edu	443-840-2811
Contact Name	Contact E-mail	Contact Phone Number

Sandra Kurtinitis

Signature and Date

President/Chief Executive Approval

2/22/2017

Date

Date Endorsed/Approved by Governing Board

Community College of Baltimore County
Digital Forensics Program – AAS
Proposal to Maryland Higher Education Commission

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

Mission Statement: The Community College of Baltimore County provides an accessible, affordable, and high-quality education that prepares students for transfer and career success, strengthens the regional workforce, and enriches our community.

A Digital Forensics Program supports the Community College of Baltimore County (CCBC) mission statement by preparing students with the technical skills in digital forensics, for entry-level employment and the education needed to transfer to a four-year institution.

While, CCBC also has robust program offerings in Information System Security and Network Technology, the cybersecurity industry has a growing need for professionals trained in digital forensics. Many cybersecurity companies have identified the area of digital forensics as a "high growth market segment" providing growing job opportunities for our students. This program will prepare our students with the technical skills required for entry level positions in the digital forensic field. It will also provide them with the education necessary to transfer to a four-year institution.

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

- Digital Forensics courses were introduced in fall 2016 to enhance CCBC's academic offerings in the field of Cybersecurity. This new degree program will enhance our students' ability to obtain jobs in the digital forensics and incident response fields. These are growing fields in both the government and private sectors.
- The primary goal of the CCBC Digital Forensics program would be to enable students aspiring to work as cybersecurity professionals to hone their skills and enhance their marketability. A degree allows them to effectively compete for jobs in cybersecurity, intrusion detection, data recovery, cyber incident response, E-discovery, computer crimes and other computer misuse.
- Digital Forensics students learn how to conduct actual physical crime scene investigations in hands-on practical situations, gather electronic evidence at the scene, examine seized electronic evidence using forensically sound methodologies, and submit findings to a digital forensics examiner's report. These experiences in developing real life familiarity with the actual digital forensic

process and using cutting edge digital forensic tools, and the ability to clearly articulate the digital forensic examination results in a concise written report will prepare students for a career in digital forensics.

The demand for cybersecurity jobs, including digital forensics, is soaring, with growth projected to be 12 times faster than the overall job market.

If approved, the Digital Forensics program will directly support CCBC's mission and its strategic goal of Teaching and Learning Excellence to encourage students to value lifelong learning, personal development, active citizenship, and educational and professional advancement. The proposed program aligns with the College's Comprehensive Academic Plan by supporting development of academic programs that will attract better-prepared students.

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

Maryland is recognized as a cybersecurity leader both nationally and internationally. The state has developed cybersecurity experts, education and training programs, technology, products, systems and infrastructure. With over 10 million cyber hacks a day, resulting in an annual worldwide cost of over $100 billion, the United States is at risk.

(https://www.fbcinc.com/e/cybermdconference/)

The CCBC Strategic Plan outlines four strategic directions: (i) student success; (ii) teaching and learning excellence; (iii) organizational excellence; and (iv) community engagement.

The CCBC Strategic Plan also describes the core values of the institution. The core values cover areas such as commitment, learning, innovation, responsibility, integrity, inclusiveness, excellence, stewardship and collaboration.

The Cybersecurity Institute at CCBC promotes innovation and supports a climate of discovery. Students, faculty and staff consistently explore new ideas, methods and processes that nurture learning and professional development at the Cybersecurity Institute.

CCBC pursues academic and organizational excellence by ensuring quality as a standard for all we do and consistently looking for ways to improve organizational efficiency and effectiveness.

Enrollment in CCBC's Network Technology and Information Systems Security certificate and degree programs has grown from 30 to 60 students in the year 2008 to over 900 students in the Fall 2016 semester. CCBC has various AAS degree programs and certificate programs related to Cybersecurity. Those programs are in the areas of

Information System Security, Network Technology, Cisco, Microsoft and Red Hat. Adding a Digital Forensics program to our existing high demand programs will help fulfill the growing needs in cybersecurity and cybercrime areas.

A Digital Forensics degree program would provide an excellent pathway for our students to gain the knowledge, skills and expertise needed for careers related to computer and digital forensics. A Digital Forensic degree would also help them transfer to universities and colleges that offer undergraduate and graduate education in computer and digital forensics and related disciplines. The digital forensics curriculum and courses at CCBC will provide a solid foundation to our students in forensics investigation techniques, hands-on experiences with state-of-the art computers and digital forensics software, and hardware products that are used in private industry and government sectors. This program will also assist students in successfully obtaining industry recognized certifications such as AccessData Certified Examiner (ACE) and Certified Computer Examiner (CCE), which are valuable for careers in digital forensics and related areas.

The Cybersecurity Institute at CCBC is actively involved in various outreach activities to bring awareness of the educational opportunities at CCBC and to recruit students. CCBC's Data Communications (DCOM) Department Chair, Cybersecurity Outreach and Recruiting Coordinator, and faculty visit various private and public high schools to promote our academic programs. The Cybersecurity Institute at CCBC conducts workshops for high school students at the Essex and Catonsville campuses. These workshops introduce students to digital forensic and cybersecurity activities through various hands-on exercises. The outreach activities also include visits by faculty and administrators to private and government agencies and bring experts from these agencies to our college to make presentations and interact with our students and faculty on issues at the forefront of these fields.

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

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

CCBC Digital Forensics AAS Program Requirements

General Education Courses			
Course Name	**Course ID**	**Credits**	**Completed**
College Composition I	ENGL 101	3	
Choose courses in each category from the list of approved General Education Courses. One course must be a Diversity course.			
Arts and Humanities	CMNS 101 recommended	3	
Biological and Physical Sciences		3-4	
Information Technology	CSIT 111 recommended	3	
Mathematics		3-4	

Social and Behavioral Sciences		3	
	Total	18/20	
Digital Forensic Core Courses			
Course Name	**Course ID**	**Credits**	
Introduction to Data Communications	DCOM 101	3	
Introduction to Linux/UNIX	DCOM 142	3	
Operating System Security	DCOM 214	4	
Introduction to Information Security	DCOM 258	3	
Introduction to PC Repair and Operation	DCOM 141	4	
Local Area Network	DCOM 251	4	
Ethical Hacking and Systems Defense	DCOM 215	4	
Computer Related Crime	CRJU 118	3	
Digital Forensics I	DCOM 150	3	
Digital Forensics II	DCOM 250	4	
Mobile Forensics	DCOM 265	4	
Any DCOM or CSIT course not already in the program.		3	
	Total	**42**	
	Total	**60/62**	

DCOM 101 – Introduction to Data Communications **3 credits**

Introduction to Data Communications provides students with an overview of the concepts, theory, principles, and practices of data communications and computer networks. Students survey networking hardware, including servers, switches, and routers; networking software, including operating systems, protocols, and services; and network management, including design, implementation, and administration. The course is designed for a student pursuing a career in networking.

DCOM 142 – Introduction to Linux/UNIX **3 credits**

Introduction to Linux/UNIX provides students with the fundamental concepts of Linux and other UNIX and UNIX-like operating systems. Students use command line utilities; learn basics of shell scripting, pipes, redirection, Linux file system, and the GNOME GUI.

DCOM 214 – Operating Systems Security **3 credits**

Operating Systems Security provides students with the hands-on skills needed to protect networks from the inside-out by focusing on Linux and Windows system hardening. The class is designed to help students prepare for professional careers in the information and communication technology (ICT) field and the Security Certified Network Professional (SCNP) certification exam.

DOM 258 - Introduction to Information Security **3 credits**

Introduction to Information Security serves the needs of students interested in understanding the field of Information Security and how it relates to other areas of Information Technology (IT). The material covered in this class provides the broad-based knowledge and skills necessary to prepare students for further study in specialized security fields, or may be used by those interested in a general introduction to the field. This course is also intended to serve the needs of those seeking to pass the Computing Technology Industry Association's (CompTIA) Security+ certification.

CRJU 118 Computer –Related Crime **3 credits**

Computer-Related Crime explores the types and extent of current computer crime, criminal typology and the motivation of offenders. The criminal justice system response to computer related crime is also explored through the issues of computer forensics for evidence collection, constitutional protections afforded computer users and the procedural law that governs cyber-crime detection and prosecution.

DCOM 141 - Introduction to PC Operation and Repair **4 credits**

Introduction to PC Operation and Repair provides an introduction to the expansive microcomputer field. The course focuses on microcomputer operating systems, broad concepts, and diagnostic tools that allow the student to rapidly determine the condition of a PC system and how best to rectify a fault. This is a first of a two course sequence designed to help prepare the student for the CompTIA A+ certification examinations.

DCOM 251 - Local Area Networks **4 credits**

Local Area Networks explores planning, installing, configuring, administering, and troubleshooting a computer network. This is accomplished through hands-on exercises and lecture material covering the fundamental building blocks that form a modern network, such as protocols, topologies, hardware, and network operating systems. This class is intended to serve the needs of students who are interested in mastering foundational, vendor-independent networking concepts, as well as those interested in taking the CompTIA Network+ certification exams.

DCOM 215 - Ethical Hacking and System Defense **4 credits**

Ethical Hacking and System Defense is the capstone course that combines an ethical hacking methodology with the hands-on application of security tools to better help students secure their systems. Students are introduced to common countermeasures that effectively reduce and/or mitigate attacks. The class is designed to help students prepare for professional careers in the information and communication technology (ICT) field and the EC-Council Certified Hacker (CEH) certification exam.

DCOM 150 - Digital Forensics I **3 credits**

Digital Forensics I provides the student with an overview of the field of digital forensics. Students perform forensic procedures for seizure, preservation, and documentation of electronic

evidence. Students use forensic hardware and software tools to authenticate and analyze digital information for possible use as evidence in civil, criminal or administrative cases. Students perform hands on laboratory exercises using digital forensics tools and evidence preservation techniques.

DCOM 250 - Digital Forensics II **4 credits**

Digital Forensics II enables the student to implement a methodological digital forensics analysis. This course covers major forensic investigation techniques such as password cracking, encryption technology, in-depth imaging analysis, and investigating browser history. Students perform hands-on digital forensic exercises using various forensics tools.

DCOM 265 - Mobile Devices **4 credits**

Mobile Forensics presents advanced topics in mobile forensics. Students examine mobile devices including cell phones and tablets. Students perform forensic acquisition and analysis of various mobile computing devices including Android, Blackberry and Windows phone devices. Students apply industry best practices when performing evidence collection and analysis; and perform hands-on exercises using forensically sound and industry standard tools.

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

Student Learning Outcomes of Digital Forensics Program:
Students will be able to:

a). Define digital forensics and describe how to take a systematic approach when preparing a digital investigation
b). Apply computer forensic procedures for seizure, preservation and documentation of electronic evidence
c). Describe processing crime and incident scene and chain of custody.
d). Discuss various File Systems and File System Management of storage medium.
e). Compare and contrast the methods of data storage on a mobile device
f). Apply the best practices for the isolation of mobile devices from cellular networks
g). Analyze digital media using forensic tools.
h). Identify some of the current techniques and tools for forensic examinations

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

See General Education Courses outlined in #1.

Students have to complete 18 to 20 credits of general education courses.

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

There are no specialized accreditation or graduation certification requirements.

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

There are no current institutional or non-collegiate contracts. If approved, we will seek articulation agreements with a number of four-year institutions.

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:**

The need for the advancement and evolution of knowledge;

The Office of the United States Attorney General states that "Cybercrime is one of the greatest threats facing our country, and has enormous implications for our national security, economic prosperity, and public safety. The range of threats and the challenges they present for law enforcement expand just as rapidly as technology evolves".

One of the fastest growing areas of Cybersecurity is the field of Digital Forensics. This field involves areas such as incident response, digital forensics, e-discovery, and network forensics. There is hardly a day that goes by that an incident isn't reported that requires the expertise in digital forensics of computer workstations, laptops, mobile devices, network servers and network perimeter devices. Along with this type of forensics, the growing use of email and social media by all businesses and government agencies requires an expertise in the recovery of not only deleted files and emails but also e-discovery of documents and emails housed in large data sets maintained by corporate server farms. This has led to many cybersecurity firms and government contractors to identify digital forensics as a "high growth market segment."

To respond to this growing demand, CCBC offers education and training to students who want to become cybersecurity professionals. These students are not only educated and trained in standard cybersecurity methods but also in the areas such as incident response and digital forensics.

Societal needs, including expanding educational opportunities and choices for minority and educationally disadvantaged students at institutions of higher education;

Nearly 33% of students at CCBC are African-American and 5% of students are of Hispanic or Latino ethnicity. About 58% of students are females. CCBC's yearly tuition

cost is less than half the national average for four year public universities. CCBC provides various means for students to earn an AAS degree in Digital Forensics Program at an affordable cost. Moreover, veterans who take courses receive benefits from CCBC. In addition to traditional financial aid (scholarships, grants and loans), other forms of tuition assistance programs are available for certain members of the CCBC community, including initiatives that expands access for minority and educationally disadvantaged students.

The need to strengthen and expand the capacity of historically black institutions to provide high quality and unique educational programs.

Currently none of Maryland's historically black institutions offer a Digital Forensics program, but CCBC will explore articulation agreements for related Computer Science programs.

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

This program will promote Goal #1: ***Quality and Effectiveness*** of the Maryland State Plan by establishing a Digital Forensics curriculum that is in high demand in fighting cyber threats nationwide. CCBC signed an educational agreement with the Department of Defense Cyber Crime Center (DC3) whereby CCBC can apply to become a Center of Academic Excellence in Digital Forensics. CCBC will be mapping the Digital Forensics curriculum to eight knowledge domains specified by the Defense Cyber Crime Center (DC3). CCBC offers a very successful programs in Information System Security and Network Technology. The Digital Forensics program will bring enhancement to our existing Cybersecurity program and Baltimore County students can take advantage of this very exciting program to make them more marketable in the field of cybercrime.

The program also promotes **Goal #2: *Access, Affordability and Completion***. The program is also affordable as it is provided in the community college tuition structure. Lastly, the program will promote completion. Cybersecurity programs are offered at the Catonsville, Essex and Owings Mill campuses. Offerings will be expanding to Dundalk, Hunt Valley and Randallstown campuses in the near future to help meet the growing job market demand in the field of cybersecurity. Cybersecurity courses are offered in different formats, such as face-to-face, blended learning and online courses, to make it more accessible to our diverse population of students. A Pearson VUE Authorized Certification Center was established at the Cybersecurity Institute – Essex Campus in summer 2016. The certification center allows students to take industry recognized certification exams at CCBC without traveling across the region to another center. Obtaining industry certifications is important for students who are in cybersecurity and Digital Forensics programs. Students who are enrolled in the Digital Forensics program can obtain the following industry certifications:

a) CompTIA → A+ certification.
b) CompTIA → Network+ certification
c) CompTIA → Security+ certification
d) Certified Ethical Hacking (CEH) certification.
e) Linux Essentials

Faculty who teach cybersecurity and digital forensics courses encourage and help students to take industry certifications and complete their degree requirements and prepare them for the job market.

The program promotes **Goal #3: *Diversity***.

CCBC is the second largest college in the State of Maryland, with 65,000 student enrollments over the past year. CCBC is the main job trainer and provider in Baltimore County. CCBC graduates 2,500 students annually. The School of Arts, Technology and Design (STAD) has largest enrollment at CCBC. In addition to that, STAD has a sizable minority and female enrollment.

This program promotes **Goal # 4: Student Centered Learning**

CCBC is committed to student success as stated in CCBC strategic plan, vision and value statements. The Digital Forensics courses employ multi-faceted approaches to student learning, such as

> Hands-on activities for kinesthetic leaners (learn by doing) and simulation. All of our Digital Forensics courses provided hands-on activities. Students are also encouraged to participate in cyber club activities.
>
> The CCBC Cybersecurity program received about four million dollars in grants under the Trade Adjustment Assistance Community College and Career Training Grants Program (TAACCCT) Rounds 3 and 4 used to establish and promote state-of-the-art curriculum and laboratory facilities.
>
> CCBC started in fall 2016 various pathways for students to select and complete their degree requirements. One of the pathways is Technology, Science and Math (TSM) theme. The main goal of the pathway is retention and completion. Various activities are planned during each semester including orientations, resume writing workshops, transfer workshops, internship fairs and others. Faculty, advisors and career coaches are heavily involved in supporting student success.

This program will also promote Goal #5: ***Economic Growth and Vitality*** of the Maryland State Plan by supporting a knowledge-based economy through education and training. An associate degree facilitates entry into the workforce or continuing to a four year degree program in Digital Forensics. This program is bundled with many industry certifications that students can obtain along with their degree to make them more

marketable. The Baltimore-Washington area has many federal and contracting jobs related to our Digital Forensics program. This program will provide a pipeline of skilled graduates who are prepared to enter the workforce in the Baltimore-Washington metropolitan region.

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

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

A leading magazine, Network World states " 'Increasing crime, terrorist attack threats and rising security concerns' are among the drivers behind new demand for digital forensics".

Digital Forensics Market is expected to Reach USD 4.97 Billion by 2021, at a CAGR of 12.5% from 2015 - 2021: Transparency Market Research (http://www.prnewswire.com/news-releases/digital-forensics-market-is-expected-to-reach-usd-497-billion-by-2021-at-a-cagr-of-125-from-2015---2021-transparency-market-research-521253551.html)

Digital Forensics is an important area of study for information security students because, while computer forensic investigations do not prevent the crime from occurring, it serves as a powerful deterrent for the criminals to know that their acts can be discovered and prosecuted.

Amount of monetary damage caused by reported cyber-crimes to the IC3 from 2001 to 2015 (in million U.S. dollars)

The statistic shows the amount of damages caused by cyber-crimes reported to the IC3 from 2001 to 2015. In the last reported period, the annual loss of complaints referred to the IC3 amounted to 1.07 billion U.S. dollars, up from 781.84 million U.S. dollars in 2013.

The need for highly trained professionals to address this growing problem is clearly identified by the number and high dollar amount of losses.

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

Opportunities for gainful employment in cybersecurity, also known as "information security," have consistently grown in numbers alongside the growth of our digital age. A July 2015 annual report by Burning Glass Technologies points out that in addition to

plenty of cyber jobs typically available at government agencies, "hiring has boomed in industries handling consumer data like finance (up 137% in the past five years), health care (up 121 %) and retail (up 89 %)" (http://burning-glass.com/research/cybersecurity/). The Bureau of Labor Statistics projects an 18% growth rate for information security analyst jobs from 2014 to 2024—that's 11% which is higher than the average growth rate for all occupations (http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm). Digital forensics is a necessary field in cybersecurity to address these growing needs.

Since the early 2000s, Corby Hovis, an NSF program director, has led Advanced Technological Education (ATE) efforts to grow cybersecurity education opportunities at community colleges. Horvis states, "A lot of cybersecurity jobs—the front-line, foot-soldier [entry-level] positions that protect information systems, can be filled by people with two-year degrees. So it was important to recognize the role that two-year colleges can play in cybersecurity and help them develop curricula and faculty to address that need."

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

Program Graduates

Fiscal Years 2011-2015

Program Name: **Information System Security (current degree offering)**

	Fiscal Years				
	2011	2012	2013	2014	2015
Degree Certificate		2	5	7	3
Associate		4	8	32	29
Total		6	13	39	32
Gender Male		4	9	31	24
Female		2	4	8	8
Unknown					
Total		6	13	39	32
Ethnicity					
Hispanic or Latino			1	3	1
Caucasian/White		6	8	22	17
African American/Black			3	9	10
Asian			1	4	2
Multi-Racial				1	2

Program Name: **Network Technology (current degree offering)**

	Fiscal Years				
	2011	2012	2013	2014	2015
Degree Certificate					
Associate	35	37	34	47	34
Total	35	37	34	47	34
Gender Male	31	32	30	40	30
Female	4	5	4	7	4
Unknown				47	
Total	35	37	34	47	34
Ethnicity					
Hispanic or Latino	1	1	2	2	2
Caucasian/White	20	25	23	25	16
African American/Black	9	10	7	13	9
Asian	3	1	1	3	5
Multi-Racial	1		1	4	2

Program Name: Digital Forensics (projected degree offering)

	Fiscal Years				
	2017	2018	2019	2020	2021
Degree Certificate					
Associate	1	3	12	20	27
Total					
Gender Male	1	2	8	14	19
Female		1	4	6	8
Unknown					
Total	1	3	12	20	27
Ethnicity					
Hispanic or Latino			1	3	5
Caucasian/White	1	2	5	7	9
African American/Black		1	5	7	9
Asian			1	3	4
Multi-Racial					

The number of available jobs in cybersecurity are soaring, with growth projected to be 12 times faster than the overall job market. The various job reports both nationally and locally demonstrate the growing need for cybersecurity professionals skilled in digital forensics (http://www.networkworld.com/article/3008520/malware-cybercrime/digital-forensics-market-set-to-double-report-says.html). While we are currently addressing that need in the Information System Security and Network Technology areas, the growing area of digital forensics needs to be further addressed to support cybersecurity. By providing a degree program in Digital Forensics we can provide our students with the credentials needed to obtain digital forensic jobs in the Law Enforcement, Military, Banking, Accounting, Corporate Incident Response and other related areas.

"CCBC expanded my network and opportunities, helping me achieve my ultimate goal of working in network security," says Elliott Pfarr, who, after nine short months of coursework, landed a full-time position with Dunbar Cybersecurity in Hunt Valley, MD. Positioning students like Pfarr with the degree and certifications they need to gain entry and build their way up in the industry is the focus of CCBC's Cybersecurity program.

CCBC students gain hands-on experience through the use of real-time cybersecurity attack-and-defend simulations via the new Cybersecurity Institute at CCBC Essex. The Institute is equipped with latest intrusion-protection systems and a virtual desktop infrastructure that are accessible 24/7 from any location.

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.**

A few other Community Colleges offer Digital Forensics programs, but none serve the Baltimore County/Baltimore City area.

Anne Arundel Community College offers Information Assurance and Cybersecurity, Digital Forensics Concentration (AAS) and Advanced Cyber Forensics Certificate programs.

Howard Community College offers Cyber Forensics Technology (A.A Degree Transfer) program and Cyber Forensics Technology Certificate Program.

Other Maryland Community Colleges do not have degree programs related to digital forensics but they offer one or two courses related to digital forensics.

2. **Provide justification for the proposed program.**

As the threat to network and computer systems continues to grow, the need for professionals trained to respond to these threats grows as well. While we are currently addressing that need in the Information System Security and Network Technology areas, the growing area of digital forensics needs to be further addressed to support cybersecurity. By providing a degree program in Digital Forensics we can provide our students with the credential needed to obtain digital forensic jobs in Law Enforcement, the Military, Banking, Accounting, Corporate Incident Response, and other related areas.

While there are currently two previously mentioned community colleges have programs related to digital forensics in Maryland, CCBC proposes to help bridge a gap of growing demand skilled workers for digital forensics jobs.

Continuing to build on CCBC's national reputation in the two-year information security education space, the Cybersecurity Institute is committed to providing solutions to the national cybersecurity workforce shortage problem by helping shape standardized cyber security curriculum; through cyber exercises, like the Mid-Atlantic Collegiate Cyber Defense Competition (MA CCDC) and through partnerships with public and private sector organizations seeking to hire CCBC graduates.

The National Security Agency (NSA) and the Department of Homeland Security (DHS) have designated the Community College of Baltimore County as a National Center of Academic Excellence in Information Assurance/Cybersecurity (CAE2Y).

E. **Relevance to Historically Black Institutions (HBIs)**

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

While HBI's in the Baltimore area do not have specific Digital Forensic Degree programs, they do have Information Assurance and Cybersecurity programs. Some of the courses taught in the Digital Forensics Program will also support Information Assurance and Cybersecurity programs at other institutions, including HBI's.

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

As indicated, HBI's in the Baltimore area have as part of their mission and degree programs Information Assurance and Cybersecurity. Several of the courses in this program are in line with the course material needed to support the HBI's institutional mission.

F. **If proposing a distance education program, please provide evidence of the Principles of Good Practice** (as outlined in COMAR 13B.02.03.22C).

The Digital Forensics program will not be offered exclusively as on online program. Some courses may be offered in an online or blended format. For those courses CCBC will follow the Quality Matters (QM) standards, as well as those standards identified by Middle States.

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

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

CCBC is fortunate to have well-qualified faculty and staff to teach and maintain the integrity of the growing cybersecurity courses. CCBC is committed to faculty training and certifications. Faculty members have various Industry certifications that are required to teach related courses in the curriculum. As part of the NSA/DHS Center of Academic Excellence review process, all of the cybersecurity faculty qualifications were reviewed to ensure that they are qualified to teach cybersecurity related courses. Based on projected load, approximately 75% of the courses will be taught by full-time faculty.

Fulltime Faculty List

Name	Position	Degrees	Courses
Noell Damron	Department Chair	M.S Computer Science	Data Communication Courses
Sabum Anyangwe	Assistant Professor/Coordinator at Essex Campus	M.S. Business Administration	Cisco, Security Courses
Wendy Chin	Assistant Professor	M.S in Cybersecurity	Cisco CCNA, Data Communications, Information Technology Courses
Jeremy Hoffman	Instructor		Network+, Security+, Linux, RedHat courses
Ben Mayock	Associate Professor	M.A. Instructional Systems Development	CCNA, CompTIA A+, Data Communication Courses
Vinitha Nithianandam	Associate Professor	B.E (Bachelor of Engineering) M.S Solid State Electronics	CCNA, CompTIA A+, Linux Essentials, Digital Forensics
Greg Schmidt	Assistant Professor/Coordinator at Catonsville campus	Master of Arts in Teaching; BS of Arts in Biology	Security+, Advanced TCP/IP, Cisco CCNA, Linux courses
Dan Whitaker	Associate Professor	Ed.D. Doctor of Education	Secure+, VMware Academy courses
Eric Ward	Assistant Professor	M.S Degree	Linux, Operating System Security, Ethical Hacking courses

Adjunct Faculty List

Name	Position	Degree	Courses
John Auman	Instructor	M.S in Policy Management	Firewall, IDS courses
Mike Crane	Instructor	MBA	Cisco.

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

Describe the library resources available and/or the measures to be taken to ensure resources are adequate to support the proposed program. If the program is to be implemented within existing institutional resources, include a supportive statement by the President for library resources to meet the program's needs.

New program proposals at CCBC are reviewed and approved according to the process developed through college governance, which includes approval by the Curriculum and

Instruction Committee and the full College Senate. In addition, this new program proposal was carefully reviewed by the President and her Senior Staff prior to submission to the CCBC Board of Trustees for their endorsement. The President has affirmed that the program can be implemented within existing institutional resources. A plan for ongoing equipment and facility upgrades and other routine needs has been developed and is in accord with CCBC's strategic plan.

The CCBC Libraries provide services and resources in both physical and online environments to a diverse community of learners.

Located on the three main campuses, the CCBC Libraries provide services and research resources to promote academic student success, such as:

- Access to materials on reserve and research guides
- Vast selection of eBooks and text books
- Interlibrary loans, allowing students to borrow from other libraries
- Technology resources, such as computers, laptops, printing, copying and scanning services
- Assistance with APA formatting, MLA formatting and citation
- Articles and research databases and more...

Library Services Support for the Digital Forensics Program

"The CCBC Libraries' current, print and digital book and research journal collections more than adequately support the proposed Digital Forensics program. The CCBC print book and ebook collection covers the digital forensics discipline with over 100 titles available to students. The Science Direct database provides above average coverage of digital forensics in the research journal literature for students completing writing projects and research in this new concentration".

From
Cynthia Roberts
Senior Director of Library Services

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

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

The Digital Forensics Program is currently offered in multiple locations. CCBC has state of the art physical infrastructure including hardware, computers and forensics software to teach the students. The following table shows Digital Forensics lab computers, hardware and software lists.

Digital Forensics Workstation and OS Software Library

Hardware/Software Specifications	Quantity
Catonsville Campus – HTEC 115 Essex Campus – HTEC 208 room Compaq HP Elite Desk 800 G1 Small Form Factor Dual Monitors 16B RAM Windows 7 Professional Operating System Autopsy (4.0version) X-way forensics FTK Imager VMware Workstation Kali Linux installed in VMware Workstation	18 (Catonsville Campus) 24 (Essex Campus)

Digital Forensics Hardware and Software

Software and Hardware	License
Access Data - Academic Program -Computer Forensics	FTK Academic Program includes 31 license on a single dongle
Forensics Academic Program Manual and CD	
X-Way Forensics	25 perpetual, dongle-based licenses for X-Ways Forensics with 1 year of update maintenance
BlackLight Analyze from BlackBag Technologies- Comprehensive Windows, Android, iPhone/iPad, and Mac forensics analysis software	one flat, annual fee.- Product includes 1network dongle with 30 licenses
Mobilyze from BlackBag Technologies - mobile device triage tool.	one flat, annual fee- Product includes 1 network dongle with 30 licenses
Forensics UltraDock FUNDv5.5 – Write Blocker	10
Ditto Forensic Field Station - Portable case for quick analysis of loose media	4
Tablets (Android, Ipad, Windows)	10

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

1. **Complete Table 1: Resources (pdf) and Table 2: Expenditure (pdf). Finance data (pdf)for the first five years of program implementation are to be entered. Figures should be presented for five years and then totaled by category for each year.**

Table 1: Resources					
Resources Categories	Year 1	Year 2	Year 3	Year 4	Year 5
1. Reallocated Funds					
2. Tuition/Fee Revenue (c+g below)	**$56,132.00**	**$87,400.00**	**$149,560.00**	**$211,720.00**	**$262,200.00**
a. # Full Time Students	13	20	35	50	60
b. Annual Tuition/ Fee Rate	$3,692.00	$3,692.00	$3,692.00	$3,692.00	$3,692.00
c. Annual Full Time Revenue (axb)	$47,996.00	$73,840.00	$129,220.00	$184,600.00	$221,520.00
d. # Part Time Students	6	10	15	20	30
e. Credit Hour Rate	$113.00	$113.00	$113.00	$113.00	$113.00
f. Annual Credit Hours -Average Credits)	12	12	12	12	12
g. Annual Part Time Revenue (d x e x f)	$8,136.00	$13,560.00	$20,340.00	$27,120.00	$40,680.00
3. Grants, Contracts, & Other External Sources	NA	NA	NA	NA	NA
4. Other Sources					
5. TOTAL REVENUE GRANTS AND OTHER (Add 1-4)	**$56,132.00**	**$87,400.00**	**$149,560.00**	**$211,720.00**	**$262,200.00**

Table 2: Expenditures					
Expenditure Categories	Year 1	Year 2	Year 3	Year 4	Year 5
1. Faculty (b+c below)	**$ 0.00**	**$48,600.00**	**$97,200.00**	**$97,200.00**	**$97,200.00**
a. # FTE	.5	1	2	2	2
b. Total Salary	18,000	$36,000	$72,000	$72,000	$72,000
c. Total Benefits	6,300	$12,600	$25,200	$25,200	$25,200
2. Admin. Staff (b+c below)	$ 0.00	$5,400.00	$5,400.00	$5,400.00	$5,400.00
a. #PTE	0	2	2	2	2
b. Total Salary	0	$4,000	$4,000	$4,000	$4,000
c. Total Benefits	0	$1,400	$1,400	$1,400	$1,400
3. Support Staff (b+c below)	$ 0.00	$9,450.00	$9,450.00	$9,450.00	$9,450.00
a. # PTE	0	2	2	2	2
b. Total Salary	0	$7,000	$7,000	$7,000	$7,000
c. Total Benefits	0	$2,450	$2,450	$2,450	$2,450
4. Equipment Hardware & Software	$30,000	$10,000	$10,000	$25,000	$10,000
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)	$54,300.00	$73,450.00	$122,050.00	$137,050.00	$122,050.00

2. **Provide a narrative rational for each of the resource category. If resources have been or will be reallocated to support the proposed program, briefly discuss the sources of those funds.**

Add information that relates back to the resource and expense tables.

Table 1: Resources

1. **Reallocated Funds**

Data: Enter the amount of funds for the first five years of implementation that will be reallocated from existing campus resources to support the proposed program. This would include funds reallocated from the discontinuance or downsizing of academic programs.

Narrative: There are no funds that will be reallocated from existing campus resources or discontinued academic programs.

2. **Tuition and Fee Revenue**

Data: Enter the estimated tuition and fee revenue that will be directly attributable to students new to the institution enrolled in this program each year. The revenue should be calculated by multiplying the tuition rate by the projected annual FTE enrollment.

Narrative: The table shows in-county tuition rates. Enrollment projections are based on current student enrollment in classes with a modest increase

3. **Grants and Contracts**

Data: Enter the amount of grants, contracts or other external funding which will become available each of the five years as a direct result of this program.

We will be seeking Perkins funding.

4. **Other Resources**: N/A

Table 2: Expenditures

1. **Faculty (# FTE, Salary, and Benefits):** Enter (a) the cumulative number of new full-time equivalent faculty needed to implement the program each year, (2) the related salary expenditures, and (3) the related fringe benefit expenditures. (For example, if two new faculty members are needed, one in the first year and one in the second, the full-time equivalency, salary, and benefits for one member should be reported in Year 1, and the same information for both members should be reported in Year 2 and each successive year.)

Current full-time faculty will meet educational needs. One additional full-time or adjunct faculty member may be needed in a year or two.

2. **Administrative Staff (# FTE, Salary, and Benefits):** Enter the cumulative number of new full-time equivalent administrative staff needed to implement the program each year, (2) the related salary expenditures, and (3) the related fringe benefit expenditures.

   There is no new full-time administrative staff needed to implement this program. Current staff in the program will support the implementation of the new program.

3. **Support Staff (# FTE, Salary, and Benefits):** Enter the cumulative number of new full-time equivalent support staff needed to implement the program each year, (2) the related salary expenditures, and (3) the related fringe benefits expenditures.

   There is no new support staff needed to implement this program. Current two staff will be needed on a one-third time basis for five years.

4. **Equipment:** Enter the anticipated expenditures for equipment necessary for the implementation and continuing operation of the program each year.

   Hardware and software for the program is purchased. Additional funds will be needed for equipment and software maintenance, repair and service contract renewal.

5. **Library:** Enter the anticipated expenditures for library materials directly attributable to the new program each year.

   No additional expenditures for library materials needed.

6. **New and/or Renovated Space:** Enter anticipated expenditures for any special facilities (general classroom, laboratory, office, etc.) that will be required for the new program. As a footnote to the table or in attached narrative, indicate whether the renovation of existing facilities will be sufficient or new facilities will be necessary.

   Current facilities will meet the needs of the program. No new space is required.

7. **Other Expenses:** Enter other expenditures required for the new program. Attach descriptive or provide footnotes on the table. Included in this category should be allowances for faculty development, travel, memberships, office supplies, communications, data processing, equipment maintenance, rentals, etc.

   Other expenses include material and travel costs

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

   Discuss procedures for evaluating courses, faculty and student learning outcomes

   As stated in CCBC's Strategic Plan, the college is committed to "Routinely measure and assess student outcomes using multiple measures of achievement and success, and act upon the results to improve student outcomes"

   1. Students in the Digital Forensics program will be required to demonstrate their competency with regard to the stated learning outcomes for each course in this program. This will be achieved through various deliverables, which include quizzes, written exams, projects and oral presentations.

   2. Faculty are evaluated for each course they teach in fall and spring with Course Instructor Evaluation Questionnaire (CIEQ). CIEQ form provides student rating feedback for each instructor and assesses both course and faculty teaching performance. Faculty are evaluated every year for overall performance. The Annual Professional Summary (APS) further evaluates each instructor's performance in the classroom as well as college and community service.

   3. Each program will be included in the institution's 5-year cycle of rigorous program review, focused specifically on evaluation and documentation of outcomes.

   4. CCBC signed an educational agreement with the Department of Defense Cyber Crime Center (DC3) whereby CCBC can apply to become a Center of Academic

Excellence in Digital Forensics. CCBC will be mapping digital forensics curriculum to eight knowledge domains specified by the Defense Cyber Crime Center (DC3).

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

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

Provide a learning environment that values diversity, multiculturalism, inclusiveness and global awareness.

CCBC is devoted to providing an environment where cultural diversity thrives. CCBC has a dedicated multicultural affairs office and offers a host of programs designed to enhance minority student success including guest speakers, study programs, clubs, and academic counseling. (http://www.ccbcmd.edu/Campus-Life-and-Activities.aspx)

Recruitment strategies include high school visitation and information provided on the CCBC website. CCBC does not discriminate on the basis of race, sex, age, religion, national origin, marital status, sexual orientation, or disabilities.

We value the diversity of people, cultures, ideas and viewpoints and we honor the dignity of all persons. We insist on open and honest communications, fairness, mutual respect, collegiality and civility at all times. We are committed to preparing students to be active citizens, ready to meet the challenges of an increasingly diverse world and a changing global marketplace.

K. **Relationship to low productivity programs identified by the Commission:**

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

N/A

References:

http://catalog.ccbcmd.edu/content.php?catoid=28&navoid=1873

https://www.edsurge.com/news/2016-04-28-community-colleges-are-new-gateways-to-hot-cybersecurity-jobs

http://www.forensicscolleges.com/careers/computer-forensics-examiner

https://www.justice.gov/usao/priority-areas/cyber-crime

https://www.fbi.gov/investigate/cyber

https://www.dhs.gov/topic/cybersecurity-education-career-development

https://www.statista.com/statistics/267132/total-damage-caused-by-by-cyber-crime-in-the-us/

https://www.edsurge.com/news/2016-04-28-community-colleges-are-new-gateways-to-hot-cybersecurity-jobs

http://www.ccbcmd.edu/Campus-Life-and-Activities.aspx

http://www.ccbcmd.edu/Campus-Life-and-Activities/Clubs-and-Organizations.aspx

443-840-CCBC (2222)

CCBC Catonsville
800 South Rolling Road
Baltimore, Maryland
21228

CCBC Dundalk
7200 Sollers Point Road
Baltimore, Maryland
21222

CCBC Essex
7201 Rossville Boulevard
Baltimore, Maryland
21237

CCBC Hunt Valley
11101 McCormick Road
Suite 100
Hunt Valley, Maryland
21031

CCBC Owings Mills
10300 Grand Central Avenue
Owings Mills, Maryland
21117

CCBC Randallstown
at The Liberty Center
3637 Offutt Road
Randallstown, Maryland
21133

The incredible value of education.

www.ccbcmd.edu

March 30, 2017

Ms. Vanessa Bennett
Education Policy Analyst
Maryland Higher Education Commission
6 N. Liberty Street
Baltimore, Maryland 21201

Dear Ms. Bennett,

The Community College of Baltimore County (CCBC) respectfully submits the attached revisions to the proposal for a new Associate of Applied Science in Digital Forensics in response to your request via email on March 24, 2107. In this letter, we seek to clarify several questions that were raised upon initial review of the proposal.

First, you addressed (COMAR) 13B.02.02.16 (A) (1) (b) and the need for an AAS degree to be 60 credits unless it meets the criteria for an exception. In the Associate of Applied Science in Digital Forensics, the minimum graduation requirement for the degree is 60 credits when a student opts to take a three credit Mathematics course and a three credit Biological or Physical Science course. However, if a student choses a four credit Mathematics class and/or a four credit Biological or Physical science course the total credits could be as high as 62 credits. In addition, all general education requirements are met per MHEC and CCBC guidelines.

Second, you requested clarification on the format in which courses in the degree will be offered. All courses outlined in the degree will be offered in a face-to-face format. Some of the courses (DCOM 101, DCOM 141, DCOM 142, DCOM 251, and DCOM 258) will also be offered online and/or in a blended format. Students may choose a course format based on their schedule and preferred learning style. A statement on page 16 of the proposal has been added to address this question.

Furthermore, information in Table 2 was inadvertently omitted (see below) for Faculty in year one. The total for year one should state $24, 300.00. Table 2 on page 21 has been revised to include this figure.

1. Faculty (b+c below)	**$ 24,300.00**
a. # FTE	.5
b. Total Salary	18,000
c. Total Benefits	6,300

If you have any questions or need more information, please contact me.

Sincerely,

Dr. Mark McColloch
Vice President of Instruction

Encl.
cc: Jack McLaughlin
Jennifer Kilbourne

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

   While HBI's in the Baltimore area do not have specific Digital Forensic Degree programs, they do have Information Assurance and Cybersecurity programs. Some of the courses taught in the Digital Forensics Program will also support Information Assurance and Cybersecurity programs at other institutions, including HBI's.

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

   As indicated, HBI's in the Baltimore area have as part of their mission and degree programs Information Assurance and Cybersecurity. Several of the courses in this program are in line with the course material needed to support the HBI's institutional mission.

F. **If proposing a distance education program, please provide evidence of the Principles of Good Practice** (as outlined in COMAR 13B.02.03.22C).

The Digital Forensics program will not be offered exclusively as on online program. All courses outlined in the degree will be offered in a face-to-face format. Some of the courses (DCOM 101, DCOM 141, DCOM 142, DCOM 251, and DCOM 258) will also be offered online and/or in a blended format. For those courses CCBC will follow the Quality Matters (QM) standards, as well as those standards identified by Middle States.

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

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

CCBC is fortunate to have well-qualified faculty and staff to teach and maintain the integrity of the growing cybersecurity courses. CCBC is committed to faculty training and certifications. Faculty members have various Industry certifications that are required to teach related courses in the curriculum. As part of the NSA/DHS Center of Academic Excellence review process, all of the cybersecurity faculty qualifications were reviewed to ensure that they are qualified to teach cybersecurity related courses. Based on projected load, approximately 75% of the courses will be taught by full-time faculty.

Table 2: Expenditures					
Expenditure Categories	Year 1	Year 2	Year 3	Year 4	Year 5
1. Faculty (b+c below)	**$24,300.00**	**$48,600.00**	**$97,200.00**	**$97,200.00**	**$97,200.00**
a. # FTE	.5	1	2	2	2
b. Total Salary	18,000	$36,000	$72,000	$72,000	$72,000
c. Total Benefits	6,300	$12,600	$25,200	$25,200	$25,200
2. Admin. Staff (b+c below)	$ 0.00	$5,400.00	$5,400.00	$5,400.00	$5,400.00
a. #PTE	0	2	2	2	2
b. Total Salary	0	$4,000	$4,000	$4,000	$4,000
c. Total Benefits	0	$1,400	$1,400	$1,400	$1,400
3. Support Staff (b+c below)	$ 0.00	$9,450.00	$9,450.00	$9,450.00	$9,450.00
a. # PTE	0	2	2	2	2
b. Total Salary	0	$7,000	$7,000	$7,000	$7,000
c. Total Benefits	0	$2,450	$2,450	$2,450	$2,450
4. Equipment Hardware & Software	$30,000	$10,000	$10,000	$25,000	$10,000
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)	$54,300.00	$73,450.00	$122,050.00	$137,050.00	$122,050.00

2. **Provide a narrative rational for each of the resource category. If resources have been or will be reallocated to support the proposed program, briefly discuss the sources of those funds.**