MARYLAND HIGHER EDUCATION COMMISSION
ACADEMIC PROGRAM PROPOSAL

PROPOSAL FOR:

__X__ NEW INSTRUCTIONAL PROGRAM
____ SUBSTANTIAL EXPANSION/MAJOR MODIFICATION
____ COOPERATIVE DEGREE PROGRAM
____ WITHIN EXISTING RESOURCES or __X_ 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.)

Carroll Community College
Institution Submitting Proposal

August 2016
Projected Implementation Date

AAS	Cybersecurity
Award to be Offered	Title of Proposed Program
0702.10	111003
Suggested HEGIS Code	Suggested CIP Code
Cybersecurity	Matt Day
Department of Proposed Program	Name of Department Head
Dr. Jan Ohlemacher	johlemacher@carrollcc.edu	410-386-8195
Contact Name	Contact E-Mail Address	Contact Phone Number

4/25/2016
Signature and Date — President/Chief Executive Approval

Date Endorsed/Approved by Governing Board Date

A. Centrality to institutional mission statement and planning priorities:

As part of its mission, Carroll Community College is a learner-centered community that serves its constituents by offering career education programs, with an intention of preparing students for an increasingly diverse and changing world. In support of this mission, and recognizing the need for training programs that prepare students for in-demand careers in high growth industries within the State, Carroll has developed an Associate of Applied Science Degree in Cybersecurity. This degree is designed to prepare students for a career in cybersecurity, computer network security, or a related field. The program is intended to provide a well-rounded base of knowledge and skills including computer networking and network security, network analysis, systems hardening, penetration testing, forensics, scripting, and technical writing and documentation. The program incorporates a combination of classroom instruction, industry certification preparation and internship opportunities (through the assistance of the Cyber Technology Navigator position and the Career Development office) to provide an effective career preparation experience. Upon successful completion of the degree, students will also be prepared to sit for the CompTIA A+, CompTIA Network+, CompTIA Security+, CompTIA Linux+, EC-Council Certified Ethical Hacker (CEH), Cisco Certified Entry Networking Technician (CCENT) and Microsoft Certified Professional (MCP) industry certification exams.

Carroll Community College's Strategic Initiatives for 2016 include expanding offerings in credit and non-credit programs and implementing a credit Cybersecurity program that includes multiple on-ramps for students who possess earned industry certifications. This Associate of Applied Science Degree in Cybersecurity will support these initiatives by:

1. Providing a new credit pathway in the areas of cybersecurity, network security, and information technology-related topics.
2. Providing individuals that have not completed formal college coursework with credit for earned industry-recognized certifications.

Carroll Community College has identified this program as in institutional priority, as the college has applied for and been awarded a Trade Adjustment Assistance Community College and Career Training (TAACCCT) grant from the U. S. Department of Labor, in collaboration with 13 other community colleges in the State. This grant award provides the college with funding to develop credit programs that serve as on-ramps and career pathways related to Cybersecurity. The grant award commenced on October 1, 2014 and will conclude on September 30, 2017.

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

Program Length: Four semesters (full-time status)

Program Requirements:

In Major Requirements:

Course No.	Course Name	Credits
CYBR-106	Computer Repair and Support 1	3
CYBR-107	Computer Repair and Support 2	3
CYBR-121	Networking Essentials	3
CYBR-122	Network Security	3

CYBR-151	Networking 1	3
CYBR-152	Networking 2	3
CYBR-181	Installing and Configuring Windows Server	3
CYBR-201	Digital Forensics	3
CYBR-241	Network Intrusion Detection and Penetration Testing	3
CIS-105	Introduction to Object-Oriented Programming	3
ENGL-209	Written Communications for Business	3
Elective	Any CYBR course	3
Elective	Any CYBR course	3
CYBR-291	Cybersecurity Capstone	1

General Education Requirements:

SPCH-101	Introduction to Speech Communication ARTS AND HUMANITIES	3
PHIL-105	Ethics ARTS AND HUMANITIES	3
	BIOLOGICAL AND PHYSICAL SCIENCES	4
	ENGLISH COMPOSITION	3
	MATHEMATICS	4
	SOCIAL AND BEHAVIORAL SCIENCES	3

Program Requirements by Semester:

Semester 1

- CYBR-106 Computer Repair and Support 1 — 3 credits
- CYBR-107 Computer Repair and Support 2 — 3 credits
- CIS-105 Introduction to Object-Oriented Programming — 3 credits
- *English Composition General Education Requirement* — *3 credits*
- *Mathematics General Education Requirement* — *4 credits*

Winter/Summer Semester

- CYBR-121 Networking Essentials — 3 credits

Semester 2

- CYBR-122 Network Security — 3 credits
- CYBR-151 Networking 1 — 3 credits
- CYBR-152 Networking 2 — 3 credits
- CYBR-181 Installing and configuring Windows Server — 3 credits
- *Arts and Humanities General Education Requirement – Required as PHIL-105 (Ethics)* — *3 credits*

Semester 3

- CYBR-201 Digital Forensics — 3 credits
- ENGL-209 Written Communications for Business — 3 credits
- Any elective in the CYBR area — 3 credits
- *Biological and Physical Sciences General Education Requirement* — *4 credits*

Semester 4

- CYBR-241 Network Intrusion Detection and Penetration Testing — 3 credits
- Any elective in the CYBR area — 3 credits
- CYBR 291 Cybersecurity Capstone — 1 credit
- *Social and Behavioral Sciences General Education Requirement* — *3 credits*
- *Arts and Humanities General Education Requirement*
  - Required as SPCH-101
  (Introduction to Speech Communication) — *3 credits*

TOTAL CREDITS **60 CREDITS**

Course Descriptions and Objectives:

CYBR-106

Computer Repair and Support 1, provides the student with hands-on experience installing, configuring and maintaining computers, software and other devices. Students will have the opportunity to develop hardware and software troubleshooting and diagnostic skills, and will learn basic concepts of computer networking and security, as well as appropriate customer service techniques. This course, in combination with CYBR-107, Computer Repair and Support 2, is designed to provide students with the necessary skills required of entry-level IT professionals as well as prepare students for the CompTIA A+ certification exams. Prerequisite: Exemption/completion of READ A-F and MAT-097. Two hours lecture, two hours laboratory each week. Three credits. Three billable hours.

OBJECTIVES: Upon completion of the course, students should be able to:

1. Install and configure standard computer components, such as expansion cards, storage devices and RAM.
2. Install and configure various peripheral devices, such as printers and external drives.
3. Identify common types of network cabling and connectors, and describe the characteristics and limitations of each.
4. Explain common TCP and UDP ports, TCP/IP protocols, and their purposes.
5. Install, configure, and deploy a wireless/wired router using appropriate security settings.
6. Identify various types of computer networks, network devices, and their functions.
7. Install and configure laptop hardware and components.
8. Install and configure printers, and perform printer maintenance.
9. Explain environmental impacts and the purpose of environmental controls in computer technology.

CYBR-107

Computer Repair and Support 2, provides the student with hands-on experience in the areas of desktop operating systems, basic computer and network security, mobile device support, and systems troubleshooting. Students will have the opportunity to properly and safely diagnose, resolve and document common software and hardware issues, and will learn basic concepts of software virtualization, imaging and network deployment of software. This course, in combination with CYBR-106, Computer Repair and Support, is designed to provide students with the necessary skills required of entry-level IT professionals as well as prepare students for the CompTIA A+ certification exams. Prerequisite: Completion of CYBR-106, Computer Repair and Support 1. Two hours lecture, two hours laboratory each week. Three credits. Three billable hours.

OBJECTIVES: Upon completion of the course, students should be able to:

1. Install and configure desktop operating systems using the most efficient and appropriate method.
2. Define appropriate command line tools.
3. Set up and configure Windows networking on a client system.
4. Describe and perform common preventive maintenance procedures.
5. Explain the basic concepts of software virtualization.
6. Implement security best practices to secure a computer workstation.
7. Compare and contrast methods for securing mobile devices.
8. Troubleshoot common issues related to computer components, such as motherboards, RAM, power supplies and drives.
9. Describe and implement common repair methods for printers, laptops and other peripherals.

CYBR-121

Networking Essentials, is designed to provide students with the necessary skills and knowledge required to configure, implement, maintain and troubleshoot TCP/IP-based computer networks. This course provides the student with hands-on experience in planning, configuring and supporting computer networks and computer networking devices. Students will learn the concepts of IP addressing, computer networking cabling and components, network security, and subnetting. This course prepares students for the CompTIA Network+ certification exam. Prerequisite: Completion of CYBR-107, Computer Repair and Support 2. Two hours lecture, two hours laboratory each week. Three credits. Three billable hours.

OBJECTIVES: Upon completion of the course, students should be able to:
1. Install and configure network services and applications, such as DHCP and DNS.
2. Explain the characteristics and advantages of various WAN technologies such as fiber, ISDN, DSL and cable.
3. Implement and configure IP addressing in a variety of scenarios, including IPv4, IPv6 and multicast.
4. Explain the basics of network routing concepts and protocols.
5. Implement a basic computer network, including performing appropriate documentation.
6. Describe network monitoring, metrics, reporting and tracking tools.
7. Install and configure various network components, including switches, routers and wireless access points.
8. Describe common network vulnerabilities and threats, and appropriate countermeasures.
9. Troubleshoot network errors, including wireless, firewall, fiber and routing issues.
10. Describe the layers of the OSI model.

CYBR-122

Network Security, is designed to introduce students to common cybersecurity issues related to wired and wireless computer networks and systems. This course builds on the foundational networking knowledge covered in CYBR-121, Networking Essentials, by teaching students how to apply security concepts to functional networks that were implemented during the CYBR-121 course. Topics include common security attacks and prevention, implementing authentication, firewalls and virtual private networks, securing email and web resources, and security policy implementation. This course is also intended to prepare students for the CompTIA Security+ certification. Prerequisite: Completion of CYBR-121, Networking Essentials. Two hours lecture, two hours laboratory each week. Three credits. Three billable hours.

OBJECTIVES: Upon completion of the course, students should be able to:
1. Draft and implement a security policy for technology resources.
2. Explain vulnerabilities in website and email systems, and implement appropriate security measures.

3. Describe security threats and ramifications, including threats related to ineffective policy and human error.
4. Describe vulnerabilities inherent in remote access, VPN, telnet, and other communications systems.
5. Identify common security attacks and countermeasures, such as spoofing, session hijacking, man in the middle, and malicious code.
6. Describe challenge handshake authentication protocol, security tokens, biometrics and other authentication methods.

CYBR-151

Networking 1, is intended to build on the foundational computer networking knowledge introduced in CYBR-121, Networking Essentials, and when combined with CYBR-152 (Networking 2), is intended to prepare students for the Cisco Certified Entry Networking Technician industry certification exam. This course will further examine the OSI and TCP layered models, IP addressing and TCP/IP concepts introduced in CYBR-121, and will additionally provide students with hands-on experience configuring routing and switching devices. Prerequisite: Completion of CYBR-121, Networking Essentials. Two hours lecture, two hours laboratory each week. Three credits. Three billable hours.

OBJECTIVES: Upon completion of the course, students should be able to:
1. Configure a network operating system.
2. Explain the characteristics of various TCP/IP-based networking protocols.
3. Configure and document access to networked resources.
4. Explain the layers of the OSI and TCP networking models.
5. Configure subnetting on a TCP/IP network.
6. Describe network cabling variations and options, while considering benefits and disadvantages.

CYBR-152

Networking 2, is intended to build on the networking concepts covered in CYBR-151, Networking 1, and when combined with CYBR-151, (Networking 1) is intended to prepare students for the Cisco Certified Entry Networking Technician industry certification exam. This course covers the principles of network routing and switching and explores common routing protocols in additional detail. Students will also learn to identify and correct common network routing issues. Prerequisite: Completion of CYBR-151, Networking 1. Two hours lecture, two hours laboratory each week. Three credits. Three billable hours.

OBJECTIVES: Upon completion of the course, students should be able to:
1. Configure a network router.
2. Troubleshoot router and network connectivity issues at all levels of the OSI model.
3. Implement network security by using an access control list.
4. Explain the static and dynamic routing concepts.
5. Configure a virtual local area network (VLAN) or network segment.
6. Explain and describe address translation for IPv4.

CYBR-181

Installing and Configuring Windows Server, is designed to provide students with hands-on experience implementing a Microsoft Windows Server infrastructure into an existing networking environment. Students will learn how to manage Active Directory Domain Services and Objects and automate administration, implement File and Print Services and Group Policy, and set up server virtualization. This course also prepares students for the Microsoft 70-410 Installing and Configuring Windows Server 2012 certification exam, which by passing, students will earn the Microsoft Certified

Professional certification. Prerequisite: Completion of CYBR-122, Network Security. Two hours lecture, two hours laboratory each week. Three credits. Three billable hours.

OBJECTIVES: Upon completion of the course, students should be able to:
1. Manage Active Directory Domain Services Objects.
2. Automate Active Directory Domain Services Administration.
3. Implement Local Storage and File and Print Services.
4. Document and implement Group Policy.
5. Set up Windows Server Virtualization with Hyper-V.
6. Describe, document and configure Windows Firewall and Security Policies.

CYBR-201

Digital Forensics, is designed to provide students with an understanding of the approach to investigating information technology security incidents and systems breaches. Students will learn to identify threats, identify and recover evidence, and perform forensic analysis and documentation. An analysis of prior breaches will also be covered. Prerequisite: Completion of CYBR-122, Network Security. Three hours lecture each week. Three credits. Three billable hours.

OBJECTIVES: Upon completion of the course, students should be able to:
1. Identify digital forensics tools and explain their role in cyber investigations.
2. Investigate common attack types, such as phishing, identity theft, malware, man in the middle attacks, and social engineering.
3. Describe the legal parameters of handling electronic evidence.
4. Effectively maintain evidence in a court-admissible format.
5. Describe the technical process for searching and seizing computer related evidence.

CYBR-241

Network Intrusion Detection and Penetration Testing, is designed to provide students with an understanding of the techniques, tools and processes used by hackers to penetrate and hack wired and wireless networks, and the countermeasures used to protect against these attacks. Students will learn about hacker tools such as malware and scripts, as well as the countermeasures taken by network administrators to stop these attacks. This course also prepares students in part for EC-Council's Certified Ethical hacker certification exam. Prerequisite: Completion of CYBR-122, Network Security. Two hours lecture, two hours laboratory each week. Three credits. Three billable hours.

OBJECTIVES: Upon completion of the course, students should be able to:
1. Describe the steps of the ethical hacking process.
2. Describe various networking threats, such as malware, viruses and worms, and their countermeasures.
3. Demonstrate an understanding of physical security and social engineering attack methods.
4. Identify weaknesses in wireless access points and wireless networks.
5. Understand and evaluate common network security devices, such as honeypots, firewalls, and IDSs.

CIS-105

Introduction to Object-Oriented Programming introduces the student to programming using object-oriented principles, such as objects, methods and inheritance to write programs. Students will learn how to create decision statements, loops, functions, arrays, objects and classes to construct algorithms and solve problems. Prerequisite: READ A-F and MAT-099. Two hours lecture and two hours of lab each week. Three credits. Three billable hours.

OBJECTIVES: Upon completion of the course, students should be able to:
1. Use decision statements in a program.
2. Use loops to manipulate data.
3. Create, call and return data from classes and functions.
4. Read and/or write data to a file.
5. Write code to handle program exceptions.
6. Use arrays to sort and search data.
7. Understand recursive techniques data.
8. Debug code by fixing syntax and logical errors.
9. Explain how a program works by going through the code line by line.

ENGL-209

Written Communications for Business, engages students in the practice of communicating effectively in the business world and in other professional settings. Emphasis is given to analyzing the communication demands of a variety of professional situations and responding in suitable formats, ranging from written documents (email messages, business letters, memoranda, researched reports, and formal proposals) to professional presentations delivered to an audience. Prerequisite: ENGL-101. Three hours lecture each week. Three credits. Three billable hours.

OBJECTIVES: ENG 209 is designed to develop the student's ability to write in the business world. Specifically, students will:
1. Analyze the rhetorical strategies employed in authentic professional communications, both effective and ineffective;
2. Define the most significant purpose of a given professional communication;
3. Communicate effectively in several business formats, including email, written memos and letters, and electronic and written reports and proposals;
4. Practice an accurate, ethical, and thorough method of researching, evaluating, and documenting source information;
5. Use illustrations and graphics to communicate information that supports a report or proposal;
6. Critique written and visual presentations effectively, accurately, and respectfully;
7. Use standard, edited English.

CYBR-291

Cybersecurity Capstone, is an independent, intensive study and research course for students pursuing the Associates of Applied Science (A.A.S.) degree in Cybersecurity. Students will conduct research and create an independent, comprehensive practical project related to the field of cybersecurity and present their results at the conclusion of the course. It is highly recommended that CYBR-291, Cybersecurity Capstone, be taken as one of the last courses in the Associates of Applied Science degree. Prerequisites: Completion of a minimum of 30 credit hours within the major, including ENGL-209. One credit. One billable hour.

OBJECTIVES: Upon completion of the course, students should be able to:
1. Research topics in cybersecurity to create an independent intensive study project.
2. Develop a well-described written research project proposal with a realistic time line for progressive due dates.
3. Write, edit and finalize the conclusions, results or end-product created by the project.
4. Submit a well written final report which clearly describes the proposal, the research and the project results/conclusions/end product.
5. Create and present an effective oral presentation of the final report.

General Education Requirements and Specialized Accreditation:

This degree program includes a minimum of 20 credits of general education, as required by COMAR for the Associate of Applied Sciences degree, and as listed above. There are no specialized accreditation standards for this program.

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

As mentioned above, this degree is being developed with funding in part by a U.S. Department of Labor TAACCCT grant award. In the application for this grant, the consortium cited the following items as evidence of strong need for cybersecurity-related programs like this degree in Maryland:

1. Nationally, cybersecurity-related job opportunities increased 94% from 2007 to 2013.
2. Maryland is one of the national leaders in cybersecurity-related job opportunities (2nd among all states per capita and 6th among all states overall).
3. Maryland is one of the national leaders in existing information technology-related careers (49% above the national average).
4. A substantial number of cybersecurity-related job opportunities require less than a bachelor's degree; many are entry-level.

Goal 5 of the Maryland State Plan for Postsecondary Education describes promoting "economic growth and vitality through the...development of a highly qualified workforce", specifically citing the need for educational programs that address the changing needs of the State economy. This degree addresses one of the most high growth sectors of the Maryland economy, as evidenced by the statistics above. Additionally, the plan's economic development strategy to provide educational access to Maryland's "untapped workforce populations", included those that are unemployed and underemployed, is addressed as these populations are also defined as target populations in the TAACCCT grant to be served within this degree program.

Goal 4 of the Maryland State Plan addresses the need for student-centered learning, and outlines several ways that programs can be designed to enable students to become intentional learners, and therefore be better prepared to transition from college to the workforce. This degree has been designed with several of these methods in mind. On a course level, many courses include a capstone project where students will apply learned skills in a workplace-like scenario. All faculty have prior experience in the field, and use this experience to identify and include industry-based assignments and research projects within the curriculum. The college has also created and filled a Cyber Technology Navigator position that works directly with students to provide internship, service learning and mentoring opportunities for students within this program.

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

This degree is designed to prepare students for an entry level career in a computer network security or cybersecurity-related position. The U. S. Bureau of Labor Statistics defines the occupational classification of Information Security Analyst (15-1122) as one that "plans, implements, upgrades, or monitors security measures for the protection of computer networks and information." This closely-related classification is forecasted to experience growth of 23% during the next decade within Maryland (see table below).

Forecasted Growth for Related Occupational Classifications in Maryland (2015 – 2025)				
Occupation	2015 Jobs	2025 Jobs	Change	% Change
Information Security Analysts (15-1122)	3,055	3,772	717	23%
Network and Computer Systems Administrators (15-1142)	12,327	12,904	577	5%
Computer User Support Specialists (15-1151)	14,975	17,543	2,568	17%

Economic Modeling Specialists, Intl., Retrieved 8/5/2015

In the process of learning cybersecurity concepts within this program, students will naturally also learn the underlying concepts of network and systems administration and computer support that precede it. As such, students in this degree will also be prepared for entry level opportunities in those careers, such as the Network and Computer Systems Administrators (15-1142) and Computer User Support Specialists (15-1151) classifications. Note that opportunities as both computer support specialists and security analysts are expected to grow much faster than the state average of all careers in Maryland (8.6%) during the next decade, and that even the slower growth category of network and systems administration is still a classification that is experiencing growth. No related career field is forecasted to experience a decline in growth during the next decade.

Of the three occupational classifications listed in the table, Economic Modeling Specialists identifies 5,569 unique job postings in Maryland as of June 2015, with the majority in the Network and Computer Systems Administrators (15-1142) classification. This is a cumulative increase from 3807 unique postings just two years ago (June 2013). Of most importance is the growth of information security-related job postings in Maryland during the last 24 months – an increase of 91%. As computer networks continue to evolve in complexity and cybersecurity-related attacks and crimes increase in frequency, it can be expected that related career job postings will increase as well.

Actual Job Postings for Related Occupational Classifications in Maryland (2013 & 2015)			
Occupation	Jun 2013 Unique Postings	Jun 2015 Unique Postings	% Increase
Information Security Analysts	801	1,526	91%
Network and Computer Systems Administrators	1,936	2,540	31%
Computer User Support Specialists	1,070	1,503	40%
TOTAL	3,807	5,569	46%

Economic Modeling Specialists, Intl., Retrieved 8/5/2015

E. Reasonableness of program duplication:

Some colleges in the area have programs similar to this proposed degree, with minor variations. Frederick Community College, for example, offers a Cybersecurity degree that includes similar core courses, however offers a number of electives that Carroll does not. Carroll's proposed degree differs from Frederick's program in that it has fewer elective options, but does require Cisco vendor-specific training, as well as a capstone project or internship as part of the curriculum. Montgomery College also offers a similar Cybersecurity degree, with many of the same core courses, however some of Carroll's proposed courses are designed to closely align with industry certifications. In addition, the grant received by the consortium of the 14 Maryland community colleges recognizes and encourages duplication to build the training capacity needed for cybersecurity in this region.

Justification for this degree is verified as this degree program was designed under the direction of a cybersecurity industry advisory group, whose direction and advisement confirmed that this degree a) covers all necessary core knowledge areas required for entry-level employment, and b) provides a direct pathway to additional coursework at a bachelor's level and beyond.

F: Relevance to Historically Black Institutions (HBIs):

This degree has the potential for transfer to four year institutions in the State, including those that are Historically Black Institutions. This degree can serve as a feeder program to Maryland's Historically Black Institutions, dependent upon the curriculum offered at those institutions and the specific goals of the individual student. In the past two years, programs such as Bowie State

University and Morgan State University have been recipients of federal grant money to expand their own Cybersecurity programs. As this degree is implemented, Carroll Community College will seek out possible articulation agreements with all transfer institutions with Cybersecurity programs and would value the opportunities that can be provided by Maryland's Historically Black Institutions.

G. If proposing a distance education program, please provide evidence of the Principles of Good Practice:

N/A.

H. Adequacy of faculty resources:

This degree will require new faculty resources to support the program. Faculty members are responsible for classroom preparation, learning management system course creation and maintenance, instruction, coursework grading, and outcomes assessment. Full and part time faculty teaching in this area will include:

1. Matt Day, Director of Cyber Technology, BS in Computer Information Systems, MBA Business Administration. He has over five years of information technology experience as a network administrator. He has instructed computer technology courses at Harrisburg Area Community College and Carroll Community College, is CompTIA A+ certified and has received Cisco Academy training. He will teach CYBR-151, CYBR-152 and CYBR291 courses.

2. Robert Keller, Cyber Technology Coordinator/Faculty Member in Cybersecurity. He has nearly ten years of teaching experience at the college level and over ten years of experience in the information technology field. He is also CompTIA A+ and CompTIA Network+ certified. Robert will teach CYBR-106, CYBR-107, CYBR-181 and CYBR-201 courses.

3. J. Grant Jewell, Adjunct Instructor. He has over 15 years of information security experience, and a bachelor's degree in Business Information Systems. Additionally, he is CISSP certified. He will teach CYBR-121, CYBR-122 and CYBR-241 courses.

4. John Fenner, Adjunct Instructor. He has over 15 years of information security and security engineering experience, and a master's degree in Information Systems. Additionally, he is CISSP, ISSEP, and CCNA certified. He will teach CYBR-121 and CYBR-122 courses.

5. Additional adjunct instructors will be hired as needed to teach sections of courses required in the program as well as specific elective courses that may be applied to the degree, as offered. Carroll seeks out the highest qualified adjunct faculty to teach its courses when hiring. Cybersecurity adjunct faculty will be no different and will include experts currently in the field with all relevant educational and industry experience and certifications.

6. Marlene Titus, Cyber Technology Navigator. She has a J.D. in law and over 10 years of experience in higher education, with focuses on non-credit program development and student advising. She will provide student support services and career and internship navigation for students in this program.

I. Adequacy of Library Resources:

Carroll is in the process of securing agreements with several vendors and industry groups that can provide curriculum, software, and student support materials to partner colleges and their students. Carroll has already formed partnerships with the CompTIA Education to Careers (E2C) program and is a Cisco Networking Academy. Also, the college has agreements with Microsoft and Adobe to provide educational software licenses to students.

In addition to these resources, existing library resources are comprehensive enough to serve the needs of this degree program, as Carroll already has acquired resources to support related programs in Computer Information Science, including full text periodical databases such as Ebsco Academic Search Premier, Business Source Premier, and the Military and Government Collection. In addition, the Library provides access to the Proquest Ebrary Master Academic Collection of eBooks which includes hundreds of eBook titles dealing with cybersecurity, Cisco systems, and computer science. Any print resources that are needed can be purchased for the collection. A professional librarian serves as a liaison to the Cyber Technology faculty and is the central point of contact for any research needs for the program.

J. Adequacy of physical facilities, infrastructure and instructional equipment:

Carroll has renovated an existing 1,032 sq. ft. classroom space to accommodate this program. Renovations include expenditures to repaint and upgrade electric and wiring as well as purchases of new student tables and computer equipment. Computer equipment purchased to support this program includes nine computer networking racks that each house multiple routers, switches, and firewalls and associated equipment, and new computers for each student. Renovations and equipment are being funded by grant resources. This space will support up to 18 students per class session, and is specifically designed to serve as both lecture and laboratory space. Faculty and staff supporting this program will reside in existing office space on campus.

K. Adequacy of financial resources with documentation:

TABLE 1: RESOURCES:					
Resource Categories	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**
1. Reallocated Funds	$0	$0	$0	$0	$0
2. Tuition/Fee Revenue (c + g below)	$98,623	$129,680	$167,588	$175,967	$184,765
a. Number of F/T Students	21	26	32	32	32
b. Annual Tuition/Fee Rate	$3,619	$3,800	$3,990	$4,189	$4,399
c. Total F/T Revenue (a x b)	$76,003	$98,804	$127,685	$134,069	$140,773
d. Number of P/T Students	10	13	16	16	16
e. Credit Hour Rate	$150	$158	$166	$174.57	$183
f. Annual Credit Hour Rate	15	15	15	15	15
g. Total P/T Revenue (d x e x f)	$22,620	$30,876	$39,902	$41,896	$43,992
3. Grants, Contracts & Other External Sources	$279,709	$260,239	$0	$0	$0
4. Other Sources	$25,893		$65,861	$62,151	$67,715
TOTAL (Add 1 – 4)	$404,225	$389,919	$233,449	$238,118	$252,480

Narrative for Table 1: Resources:

1. Reallocated Funds: Carroll Community College does not anticipate a need to reallocate funds from any other area to support this degree program.
2. Tuition and Fee Revenue: Carroll intends to launch two full time cohorts each year (fall and spring semesters), and based on current enrollment, prospective student interest and marketing outreach efforts, expects each cohort in year 1 to comprise of 8 14 students. We are assuming an attrition rate of 25% for all cohorts, and therefore are estimating a conservative 12 21 full time students in year 1 (8 14 in fall cohort + 8 14 in spring cohort = 16 28 full time students x

.75 student retained = 12 21 full time students). We are also estimating an increase of 5% per year in tuition. We also are anticipating that growth in years two and three will increase by 50 25% in each year, again with an expected 25% attrition. Enrollment in years four and five are expected to level out as the program solidifies and gains sustainability. Part-time student enrollment is expected to match be half that of full time enrollment, as students completing similar programs in the continuing education area are expected to enroll on a part time basis, however at a minimal rate. Part-time students will complete the program in approximately 3 years, while completing 20 credits per year.

3. Grants and Contracts: Grant funding in years one and two, providing by the Department of Labor TAACCCT grant award is $279,709 and $260,239, respectively.
4. Other Sources: Carroll will apply state and local funding to the program.

TABLE 2: EXPENDITURES:					
Expenditure Categories	Year 1	Year 2	Year 3	Year 4	Year 5
1. Faculty (b + c below)	$98,132	$100,095	$111,706	$113,940	$116,219
a. # FTE	2	2	2.5	2.5	2.5
b. Total Salary	$68,660	$70,033	$80,360	$81,968	$83,607
c. Total Benefits	$29,472	$30,061	$31,345	$31,972	$32,612
2. Admin. Staff (b + c below)	$187,616	$191,368	$97,598	$99,550	$101,541
a. # FTE	2	2	1	1	1
b. Total Salary	$130,000	$132,600	$67,626	$68,979	$70,358
c. Total Benefits	$57,616	$58,768	$29,972	$30,571	$31,183
3. Support Staff (b + c below)	$16,577	$16,909	$24,145	$24,628	$25,121
a. # FTE	0.25	0.25	0.35	0.35	0.35
b. Total Salary	$9,375	$9,563	$13,655	$13,928	$14,207
c. Total Benefits	$7,202	$7,346	$10,490	$10,700	$10,914
4. Equipment	$89,300	$20,400	$0	$0	$9,600
5. Library	$0	$0	$0	$0	$0
6. New or Renovated Space	$12,600	$0	$0	$0	$0
7. Other Expenses	$0	$0	$0	$0	$0
TOTAL (Add 1 – 7)	$404,225	$328,772	$233,449	$238,118	$252,480

Narrative for Table 2: Expenditures:

1. Faculty: Carroll estimates that years 1 and 2 of the program will require one full time faculty member and several part time faculty members that combine for a load equivalent to a second full time faculty member. Additionally, this load is expected to increase in years 3 and beyond as additional electives are added to the curriculum and enrollment increases. Salary and benefits in this area are calculated based on existing salary and benefits costs, with a built in increase of 2% per year. TAACCCT grant funding will cover all expenses in this area in years 1 and 2.
2. Administrative Staff: Carroll will be assigning two administrative positions to this program – a program director and a Cyber Technology Navigator. The Navigator salary and benefits portion are covered by grant funds in years 1 and 2. As the program moves beyond its initial startup phase in years 1 and 2, the college expects to reassign these two positions to additional programs and prorate their time to this program at 50%, hence the decreased costs in years 3 – 5. Yearly salary and benefits increases are estimated at 2% per year.

3. Support Staff: Carroll will assign a support staff member to this program, with an estimate of 25% of their time used to support this program and related faculty. Prorated support staff time is increased to 35% in years 3 – 5 to support the additional faculty in section 1.
4. Equipment: Equipment requirements are substantial in years 1 and 2, but are covered fully by grant funds. This equipment includes the necessary hardware, computers, servers and routers to deliver cybersecurity curriculum. This equipment has a minimal useful life of 5 years. We anticipate a cost for additional computers in year 5 as the program expands.
5. Library: Note section I above. No additional library resources are required.
6. New or Renovated Space: Year 1 costs for classroom renovation include new desks and electrical upgrades. All costs are grant funded. No additional expenses are anticipated.
7. Other: No other expenses are anticipated.

L. Adequacy of provisions for evaluation of program:

Student learning outcomes at a course level will be assessed by evaluation methods outlined in each course syllabus. These methods include assignments, lab exercises, examinations and projects. Additionally, many courses in this degree are intended to prepare students for a third party industry certification exam. Carroll will be monitoring and tracking student success on these exams, and will adjust and update curriculum as necessary, based in part on the competency results of these exams as well as post-test student feedback

All new courses and new faculty are assessed via a SIR-II evaluation each semester. Additionally, Carroll also administers an open response survey, which allows students to provide added feedback. Faculty supervisors regularly observe and critique faculty to observe lesson plans, syllabi, and teaching style. The College also requires programs to submit an annual report each year that details enrollment from the past year, data from learning outcomes assessment, and action plans for the coming year. In addition, all programs complete a thorough program review every five years that encapsulates the annual reports and provides a more extensive review of the curriculum, job outlook for the field and visioning for the next five years.

M. Consistency with the State's minority student achievement goals:

Carroll Community College serves a racially and ethnically homogeneous population. The latest official estimates, from July 2006, report 160,339 of the 170,260 residents of Carroll County—94.2 percent—were non-Hispanic white. Carroll County is thus atypical of Maryland, which has a population that is 58.1 percent non-Hispanic white. The demographic reality of Carroll County presents a challenge to the college, which is dedicated to promoting diversity in its student body and programming. Detailed below are activities undertaken by the college to promote recruitment and retention of African American and Hispanic students. The College maintains a commitment to hire minority faculty to help attract minority students and to serve as role models for these students.

Student Recruitment

The recruitment approach at Carroll is to market the college overall as well as specific program options. We host three major Open House programs and four Financial Aid Workshops each year, inviting the total population in a targeted age range within Carroll County. In addition we conduct ongoing visits at area high schools. Frequently, high school counseling staff arrange for individual meetings with minority students and their families. Our recruitment activities are designed to be inclusive and our marketing materials reflect broad representation on campus in terms of race, gender, age and populations with disabilities. We also are intentional in our inclusion of minority students in the Campus Ambassador program. Ambassadors provide campus tours and answer questions of prospective students and their families.

First Advising Sessions

The college does not target one specific population of prospective students, but reaches all students to add a personal touch in an effort to ensure they enroll. The office follows up with all students that have attended a First Advising Session. These sessions are attended by all first-time students. Follow-up phone calls are used to check in with these prospective students and answer any questions they may have. In addition, advising staff are trained to use special sensitivity when explaining test results and meeting with students to ensure that they feel supported and understand their placement and course options.

When working with non-citizens, individual attention is given to ensure they are given the resources they need to both enroll and be successful in their classes.

In addition, the Admissions and Advising Office employs two mixed-race Native Americans and an African American in an effort to be inclusive and sensitive to minority student needs.

Targeting English for Speakers of Other Languages Students

Carroll Community College has assumed responsibility for Adult Education Programs in Carroll County. Degree-credit student recruiters work with the college's Continuing Education and Training area to encourage students in English for Speakers of Other Languages (ESOL) courses to complete the GED and then pursue college degree programs. In recent years, 85 percent of the college's ESOL students have been Hispanic.

Future plans include working with the ESOL students to help them feel more connected to the college community by offering special invitations to campus events. All ESOL students will receive student handbooks, be encouraged to attend the free film series on campus with their families, and participate in major events such as the health fair, job fair, and global issues fair. Further we are developing enrollment management goals to provide an ESOL Bridget program for completers of the ABE program to attend credit classes toward the degree.

N. Relationship to low productivity programs identified by the Commission:

N/A.