BOARD OF REGENTS

UNIVERSITY SYSTEM of MARYLAND

SUMMARY OF ITEM FOR ACTION, INFORMATION, OR DISCUSSION

TOPIC: University of Maryland University College: Restructuring of Existing Area of Concentration in Information Assurance to Master of Science in Cyber Operations

COMMITTEE: Education Policy and Student Life

DATE OF COMMITTEE MEETING: Tuesday, September 19, 2017

SUMMARY: The proposed restructuring and revision of the existing Area of Concentration in Information Assurance to a freestanding M.S. in Cyber Operations will strengthen the curriculum and better align it with the needs of employers. This action will also clarify the content of the degree and simplify the pathway to completion, allowing for a better communication of the program outcomes to students and employers.

The proposed program is targeted towards those with academic and/or professional backgrounds in hands-on computer science. "These include early or mid-career individuals with experience in the military, public, or private sectors who desire to expand their knowledge and skill set in cybersecurity technologies in order to enhance their opportunities for special operations in cyber space. The revised program is a highly technical program grounded in computer sciences."

Cyber Operations related occupational categories are projected to grow by 9.2% nationally and 6.1% in Maryland between 2017 and 2022.

ALTERNATIVE(S): The Regents may not approve the program or may request further information.

FISCAL IMPACT: No additional funds are required. The program can be supported by the projected tuition and fees revenue.

CHANCELLOR'S RECOMMENDATION: That the Education Policy and Student Life Committee recommend that the Board of Regents approve the proposal from UMUC to offer the Master of Science in Cyber Operations.

COMMITTEE RECOMMENDATION: Approval		DATE: September 19, 2017
BOARD ACTION:		DATE:
SUBMITTED BY: Joann A. Boughman	301-445-1992	jboughman@usmd.edu

UNIVERSITY SYSTEM OF MARYLAND INSTITUTION PROPOSAL FOR

__X__ New Instructional Program
_____ Substantial Expansion/Major Modification
_____ Cooperative Degree Program
__X__ Within Existing Resources or _____ Requiring New Resources

University of Maryland University College

Institution Submitting Proposal

Restructuring of Existing Area of Concentration (AOC) in Information Assurance within the M.S. in Information Technology
to
Master of Science in Cyber Operations

Title of Proposed Program

Master of Science	**Fall 2018**
Degree to be Awarded	Projected Implementation Date
079901	**11.1003**
Proposed HEGIS Code	Proposed CIP Code
The Graduate School	**K. Klose, PhD, Vice Provost and Dean**
Department in which program will be located	Department Contact
(240) 684-2400	**Kathryn.Klose@umuc.edu**
Contact Phone Number	Contact E-Mail Address
	**9/8/17**
Signature of President or Designee	Date

University of Maryland University College
Master of Science in Cyber Operations

University of Maryland University College (UMUC) proposes to restructure and revise the existing Area of Concentration (A.O.C.) in Information Assurance (HEGIS 070200; CIP 11.0401) within the Master of Science (M.S.) in Information Technology. The change consists of removing and discontinuing the Information Assurance curriculum from the M.S. in Information Technology and restructuring the curriculum as a freestanding M.S. in Cyber Operations (proposed new HEGIS 079901; proposed new CIP 11.1003). The restructured M.S. program requires the successful completion of six six-credit courses for a total of 36 semester hours of graduate-level coursework.

A. Centrality to Institutional Mission Statement and Planning Priorities

1. Program description and alignment with mission

Consistent with the institutional purpose as stipulated by State statute (Md. Education Code Ann. § 13-101(2012)), the mission of UMUC is improving the lives of adult learners. UMUC will accomplish this by:

(1) Operating as Maryland's open university, serving working adults, military servicemen and servicewomen and their families, and veterans who reside in Maryland, across the United States, and around the world;
(2) Providing our students with affordable, open access to valued, quality higher education; and
(3) Serving as a recognized leader in career-relevant education, embracing innovation and change aligned with our purpose and sharing our perspectives and expertise.

The purpose of restructuring the curriculum to create a freestanding M.S. in Cyber Operations is to 1) strengthen the curriculum and better align it with the needs of employers via competency- based teaching and learning approaches and 2) clarify the content of the degree and simplify the pathway to completion so that it can be more readily communicated to prospective and current students and employers.

The current structure of having the A.O.C. in Information Assurance nested within the M.S. in Information Technology places an emphasis on the core coursework in general Information Technology rather than on the specific content of the concentration in Information Assurance. The revised program structure benefits students and employers by more clearly focusing the content on Information Assurance and Cyber Operations. As a result, UMUC will be better able to differentiate the degree from others within its portfolio of offerings and ensure the currency and relevancy of the curriculum relative to current workforce and employer demands.

The proposed M.S. in Cyber Operations program is aimed at those with academic and/or professional backgrounds in hands-on computer sciences. The targeted audience includes

early or mid-career individuals with experience in the military, public, or private sectors who desire to expand their knowledge and skill set in cybersecurity technologies in order to enhance their opportunities for special operations in cyber space. The revised M.S. in Cyber Operations is a highly technical program grounded in computer sciences. The M.S. program is being designed to meet the requirements of NSA Centers of Excellence in Cyber Operations,[1] and is in support of the President's National Initiative for Cybersecurity Education (NICE). The emphasis of the program is on technologies and techniques related to operations in cyber space to enhance the security of our nation.

The new program builds on the existing A.O.C. by recombining content of the existing three-credit courses to create a new series of six-credit courses, refining and adding content consistent with current industry practices and requisite knowledge and skills, and incorporating new delivery and assessment methods based on the principles of project- and competency-based pedagogy. The 6-credit hour structure reflects the increased workload required per course. The new series of six six-credit course will present a streamlined path to degree completion.

2. Alignment with institutional strategic goals

As the public state and national leader in distance and distributed education, UMUC awards associate's, bachelor's, master's and doctoral degrees, as well as undergraduate and post-baccalaureate certificates. The university's academic inventory offers programs that are core to any public university, but UMUC's mission to the adult student results in an emphasis on workforce-relevant programs. Consequently, the university awards degrees and certificates in the arts and humanities, behavioral and social sciences, business and management, health-related fields, computing, education and technology, including degrees in fields facing critical shortages, such as cybersecurity, information security, and graduate-level teacher-training in STEM areas. As part of its emphasis on workforce needs, UMUC offers non-credit professional development programs such as those in executive leadership and hosts professional conferences and meetings that support the economic and societal needs of the State.

This proposal aligns with UMUC's mission by providing a learner-focused program based on leading-edge adult learning theory and curriculum design that addresses the needs of students and the community. The revised program is consistent with UMUC's commitment to offering current and relevant degrees that prepare students for the workforce. Students are given time to practice skills as they progress through formative instruction and engage in authentic assessment of learning. The program will support students' professional development with project-based opportunities to learn from employers and peers. The program model offers flexibility and continuing education opportunities to adults interested in refreshing and reshaping their career opportunities.

[1] NSA Centers of Excellence in Cyber Operations Requirements:
https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-operations/

B. Adequacy of Curriculum Design and Delivery to Related Learning Outcomes

1. Program requirements

The M.S. in Cyber Operations is an interdisciplinary technical program that provides a solid foundation in competencies and skills related to security principles and architecture, networks security, risk analysis, applied cryptography, and information assurance, cyber law, forensics, software reverse engineering and cyber offense. The program requires students to demonstrate competencies in hands-on computer sciences, specifically in the following areas: (1) C, assembler and system programming, (2) operating systems, (3) computer architecture, (4) mobile and cellular communications and networking, (5) virtualization & cloud computing, and (6) discrete mathematics.

This program revision restructures and enhances the existing curriculum by incorporating teaching, learning, and assessment strategies that focus on students developing concrete, job-related knowledge and skills. The revised curriculum is based on principles of competency- and performance-based learning. The required competencies comprising the program learning outcomes have been developed and verified with the help of academic experts and employers and drive the program curriculum and assessments. The approach is learner-focused, and authentic assessments are embedded in every step of the learning process. Through embedded assessments, students perform real-world authentic project-based tasks, demonstrating their knowledge and skills as they work toward mastery. Students "learn by doing" and graduate better prepared for workplace opportunities.

As shown below, the revised M.S. in Cyber Operations (COP) requires the completion of six 6-credit courses for a total of 36 credits. Core to the revised program is a 6-credit foundational course that is required for all graduate students and that covers essential intra- and interpersonal competencies required for successful graduate work and identified by employers as highly desirable in graduates. This course includes the core competencies of written and oral communications, critical thinking, quantitative reasoning and leadership. The remaining five 6-credit courses build on the foundation to complete the degree, keeping the total number of credits the same as in the original A.O.C. offering. This revised program represents UMUC's commitment to offering current and relevant degrees to its students. Course descriptions are presented in Appendix A.

Required Courses for the M.S. in Cyber Operations:

- CBR 600 Communicating, Problem Solving, and Leading in Cybersecurity (6)
- COP 610 Foundations of Cyber Operations (6)
- COP 620 Cybersecurity Defense (6)
- COP 630 Cyber Law & Digital Forensics (6)

- COP 640 Secure Software (6)
- COP 670 Cyber Offense & Capstone (6)

2. Educational objectives and student learning outcomes

Through completion of the foundational course (CBR 600), students who complete the M.S. in Cyber Operations will be able to:

- Communicate clearly both orally and in writing.
- Apply logical processes to formulate clear, defensible ideas and to draw conclusions based on the consideration of ethical implications.
- Use mathematical information, operations and quantitative analyses to solve problems and inform decision-making.
- Lead, facilitate, and collaborate with a variety of individuals and diverse teams to achieve organizational objectives.

Through completion of the sequential COP courses, students who complete the M.S. in Cyber Operations will be able to:

- Apply the security foundational knowledge and skills including security first principles, access control and layered defense in protecting information assets.
- Perform risk analysis of information systems.
- Leverage cryptographic techniques for protecting information systems.
- Employ tools and techniques for protecting enterprise assets including networks, hosts and devices from cyber threats.
- Carry out network, media and RAM forensics tasks for common operating systems and devices.
- Utilize static and dynamic analysis tools to find security vulnerabilities in software.
- Use tools and techniques for secure design and coding of software.
- Apply reverse engineering techniques for malware analysis and generation.
- Formulate a cyber-offense campaign in compliance with applicable U.S. laws.
- Carry out steps in a cyber-offense exercise including exploit development, and network and web hacking.

3. General education requirements

Not applicable.

4. Specialized accreditation or graduate certification requirements

Not applicable.

5. Contractual agreement with other institutions

Not applicable.

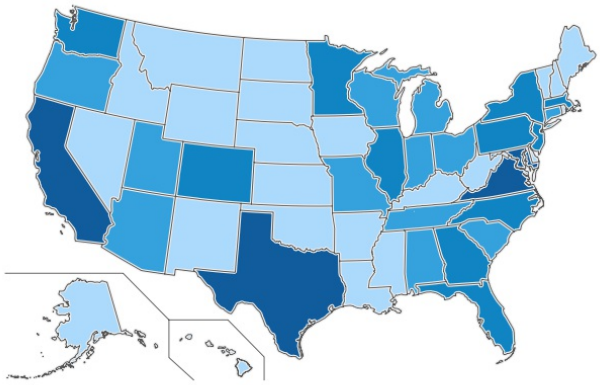
C. Critical and Compelling Regional or Statewide Need as Identified in the State Plan

1. Demand and need for the program

We used data and models of Economic Modeling Specialists International (EMSI)[2] to provide evidence of program demand.

A key word search on skills or topics that these programs emphasize (e.g., software security, software vulnerability, vulnerability exploitation, penetration testing, ethical hacking) identified 133,367 and 109,13 unique job postings in the nation and Maryland, respectively, from Feb. 2016 to Feb. 2017. Maryland ranks third nationally in the number of jobs advertised in these searches, next only to Virginia and California, as shown below in Figure 1 (the darker the color, the more the demand there is):

Figure 1. Demand for Skills Emphasized by the Cyber Operations Program



State	Unique Postings (Feb 2016 - Feb 2017)
Virginia	17,149
California	16,208
Maryland	10,913
Texas	10,444
New York	5,560

The five occupations that are most relevant to the topics and skills emphasized in the program

[2] Economic Modeling Specialists International (EMSI): http://www.economicmodeling.com/

are:

1. Information Security Analysts
2. Computer and Information Systems Managers
3. Software Developers, Applications
4. Network and Computer Systems Administrators
5. Computer Occupations, All Other.

The projected growth over the next five years for Cyber Operations related occupations is 9.2% for the nation and 6.1% for Maryland as shown in Table 1 below:

Table 1: Growth of Cyber Operations Related Occupational Categories

	2017 Jobs	2022 Jobs	%Change
Nation	1,900,832	2,074,985	9.2%
Maryland	54,264	57,555	6.1%

The projected growth for the occupation category of Information Security Analysts, the most relevant occupation category to this proposed Cyber Operations program, is 10% and 7% over this five-year time period for the nation and Maryland, respectively.

The jobs in these occupations certainly pay above average. For example, the median and 75% earning per hour for Information Security Analysts in Maryland are $47.43 and $61.46, respectively. The corresponding figures for Information Systems Managers are $67.76 and $79.95.

There is a substantial gap between job postings in and hires for these five occupation categories. In an average (recent) month, there were 313,662 unique job postings for these five occupation categories, and 82,108 actually hired nationwide. This means there was approximately 1 hire for every 4 unique job postings for the five occupations. In the occupation category of Information Security Analysts alone, the number of posted jobs is 30,153, and the number of hires is 4,072 in an average month, i.e., 1 hire for every 5 posted positions. It is likely that postings for unfilled positions keep reappearing until they are filled or no longer needed.

A 2014 report by Rand Corporation entitled, "H4cker5 Wanted: An Examination of the Cybersecurity Labor Market," explores the current status of the labor market for cybersecurity professionals —with an emphasis on their being employed to defend the United States.[3] It concludes that the labor shortage exists, it is worst for the federal government, and it potentially undermines the nation's cybersecurity. The report observes that upper-tier cybersecurity professionals—those who are qualified to do forensics, code-writing, or red-teaming, the skills emphasized in the proposed Cyber Operations program—are the hardest to hire in today's labor market.

[3] Rand Corporation Report:
http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR430/RAND_RR430.pdf

2. Consistency with the Maryland State Plan for Post-Secondary Education

The program revision is designed to meet present and future needs of the state, as identified in *Maryland Ready: The 2013-2017 Maryland State Plan for Post-Secondary Education (State Plan)*, by continuing to expand and enhance UMUC's offerings in STEM disciplines, a prominent goal for public institutions included in the *State Plan.* This program supports major goals in the *State Plan* in a number of specific ways:

- The program serves Goals 1 and 2 (Quality and Effectiveness and Access, Affordability and Completion) in the *State Plan* in that it is designed to support UMUC's overall mission to set a global standard for excellence and to be respected as a leader for affordable and accessible adult education programs. In addition, UMUC administers its programs to meet the goals of the Effectiveness and Efficiency Initiative of the University System of Maryland Board of Regents, by employing data-driven decision-making that ensures that academic programs offer high quality education at an affordable cost to broaden access.

- The program supports Goal 3 (Diversity) in the *State Plan* by offering access to education to diverse populations of students. As shown in Table 2 below, in 2014-2015, the current A.O.C. in Information Assurance awarded 38% of its master's degrees to African-American students and 8% of its master's degrees to Hispanic students, compared, respectively, to 18% and 4% for Maryland institutions as a whole. UMUC is committed to maintaining its position in serving the educational needs of minority students.

Table 2. Percentage of Master's Degrees Awarded to Selected Student Subpopulations, 2014- 2015[4]

% of Master's Degrees Awarded	Maryland Institutions in Total	UMUC, All Programs	UMUC, Current A.O.C. in Information Assurance
Black/African American Students	18%	35%	38%
Hispanic/Latino Students	4%	6%	8%

- The program serves Goal 4 (Innovation) in the *State Plan*, as it is based on principles of competency- and performance-based learning that are at the forefront of developments in higher education. Competency-based learning is an outcomes-based approach to education that emphasizes what students should know and be able to do to be successful in their disciplines. The approach is learner-focused and

[4] Source: 2016 MHEC Data Book and UMUC's FY15 DIS.

authentic assessment (the measurement of what students have learned and the competencies students master) is embedded in every step of the learning process to assist students in building real-world, job-relevant competencies in real time. The revised program employs authentic assessments that are relevant to tasks that graduates will actually perform on the job; such projects serve as both the means of instruction and assessment of learning in the program. Enhanced learning resources and multiple means for supporting students as they progress through their learning experiences are developed to improve retention and student success. The methodology and the on-demand nature of the support are innovative in the field of higher education and online learning, and reflect current best practices in adult learning. There is also innovation in the subject matter. Teaching and learning emphasizes the moral, ethical and legal aspects of cyberwarfare and techniques for exploitation in the training of cyber warriors and planners for cyber campaigns. All these topics are evolving not just at UMUC, but in the entire cyber community and the nation.

- The program serves Goal 5 (Economic Growth and Vitality) in the *State Plan*, in that it is designed to better align the competencies and skills of graduates to the needs of industry and employers. In developing the program revisions, program administrators met with employers and other experts to determine the competencies and skills desired in the workplace. This work resulted in a specific set of competencies for the degree program upon which learning outcomes and learning demonstrations (authentic assessments) were developed. Students will be evaluated based on their mastery of the competencies exhibited through learning demonstrations. The Graduate School also conducted focus groups with employers to identify the intra- and interpersonal professional skills most desired in today's graduates and incorporated development of these skills into the curricula. These efforts ensure closer alignment of graduate skills and dispositions (attitudes) to employer needs than under prior learning models.
- The program serves Goal 6 (Data Use and Distribution) in the *State Plan*. The revision of the program toward a competency-based learning methodology places more emphasis on the monitoring of student and program progress across skills. Student performance will be monitored via well-vetted competency rubrics capable of reporting on areas of excellence and needs for improvement. Aggregated data can be used to inform short- and long-term improvement plans for students, programs, and policies. Robust data systems will offer insights that may assist in identifying populations that need additional support and in closing achievement gaps for underrepresented populations.

D. Quantifiable and Reliable Evidence and Documentation of Market Supply & Demand in the Region and State

1. Market Demand

Table 3 below shows the employment outlook in Maryland and the DC Metro area for graduates

of programs in occupations aligned with the proposed program. The projected 10-year demand shown in Table 3 is drawn from the EMSI employment projections for 2016-2026. Table 3 lists the Cyber Operations program's top five occupations.

Table 3: Employment Projections, Years 2017 and 2026, for Five Cyber Operations Related Occupations

SOC Code	Occupational Category	Maryland			The DC Metro Area		
		2017	2026	10-Yr Change	2017	2026	10 Year Change
15-1122	Information Security Analysts	3,508	3,887	10.80%	15,849	17,194	8.48%
11-3021	Computer and Information Systems Managers	9,428	10,509	11.47%	28,281	31,380	10.96%
15-1132	Software Developers, Applications	13,470	15,942	18.35%	54,279	61,856	13.96%
15-1142	Network and Computer Systems Administrators	13,106	13,840	5.6%	37,515	39,503	5.31%
15-1199	Computer Occupations, All Other	14,752	15,400	4.39%	39,632	40,378	1.88%
Total		**54,264**	**59,579**	**9.79%**	**175,556**	**190,310**	**8.41%**

The data in the table demonstrate the potential for 5,315 (59,579 – 54,264) and 14,754 (190,310 – 175,556) new positions in Maryland and the DC Metro area, respectively, in the five most relevant occupations for which the proposed program will prepare graduates.

Career roles or titles for students graduating from the M.S. in Cyber Operations program include, among others:

- Information Security Analyst/Cybersecurity Analyst (Incident Analyst, Threat Analyst, Vulnerability Analyst, Intelligence Analyst, Malware Analyst, Forensic Analyst, Focused Operations Analyst)
- Cybersecurity Engineer
- Information Security Manager
- Security Architect

2. Educational and training needs

Information Security Analyst jobs are classified by the U.S. Department of Labor as requiring extensive preparation and work-related skill and knowledge, most of which require at least a four-year bachelor's degree in Computer Science. Information Security Analysts need to be proficient in multiple computer-and-electronics areas, networks, administration and management, critical thinking, complex problem solving, and

problem sensitivity. These positions also demand strong written and oral comprehension, deductive reasoning, inductive reasoning, communication, and analytic skills. (Bureau of Labor Statistics, U.S. Department of Labor. *Occupational Outlook Handbook, 2016-17 Edition*).

3. Prospective graduates

The following enrollment projections are based upon expected completion of the program in two years, with students enrolling in an average of 18 semester hours per year. There are 448 students (as of Spring 2017) enrolled in the various courses of the program. Those existing students will be given an opportunity to complete their degrees under the current curriculum and are not included in the table below.

Table 4: Projected Enrollment in Program Years One through Five

Projected Enrollment	Year One	Year Two	Year Three	Year Four	Year Five
First Year Students	50	55	60	65	70
Second Year Students	0	48	53	58	63
Total Students	**50**	**103**	**113**	**123**	**133**

It is anticipated that approximately 60-70 degrees will be awarded each year after the program is established and reaches steady state.

E. Reasonableness of Program Duplication

1. Similar programs in the state

A search of the MHEC program inventory[5] revealed no master's degree programs in Maryland focused on Cyber Operations. However, there are three programs that have components that overlap with the proposed UMUC Cyber Operations program, as shown in Table 5 below:

[5] MHEC program inventory: http://data.mhec.state.md.us/macAux.asp#api

Table 5: Number of Degrees Awarded, By Year, in Similar Master's Degree Programs in Maryland[6]									
					Year				
CIP Code	HEGIS	Institution	Credential	Program Title	2012	2013	2014	2015	2016
119999	070116	Capitol Technology University (CTU)	Master of Science	Cyber and Information Security	89	81	83	88	63
111003	070117	Johns Hopkins University (JHU)	Master of Science	Security Informatics	29	23	25	31	31
Not Available *	Not Available *	University of Maryland, College Park (UMCP)	Master of Engineering	Cybersecurity	Not Available*				
Total					**118**	**104**	**108**	**119**	**94**
Cumulative Total over Five Years									**543**

*The CIP code and HEGIS as well as the number of degrees awarded, as listed in the MHEC trend database, is for all engineering degrees at UMCP. The data is not available for this Cybersecurity program alone.

The columns on the right of Table 5 show the annual number of degrees awarded by these programs in Maryland. These data demonstrate that these programs yielded a total of 543 Master's degrees in the years 2012-2016. This level of degree production is insufficient to meet the employment projections presented in Table 3 for occupations that are aligned with the Cyber Operations program being proposed. The cyber security jobs required for the military, intelligence and law enforcement communities cannot be outsourced, and critical shortage of these skills is expected to continue.

2. Program justification/Reasonableness of Program Duplication

At the outset, the M.S. program in Cyber Operations is being designed to meet the requirements of NSA Centers of Excellence in Cyber Operations. It covers both cyber defense and cyber offense techniques, with a particular emphasis on secure software engineering and exploiting software vulnerabilities. It is a hands-on program to train those who will be defending the nation in cyber space. The program is targeted to meet the needs of law enforcement, military, and intelligence communities of the nation. The programs that are listed in Table 5 and to which the UMUC program is compared in more detail in the subsequent tables are mostly focused on cyber defense, as opposed to cyber operations more broadly, which is the focus of the

[6] Source: MHEC Higher Education Trend Data, http://data.mhec.state.md.us/macAux.asp#api

proposed UMUC program. Consequently, the proposed UMUC program is well positioned to fill a major void in the nation's cybersecurity education. These programs, however, do have some overlap with topic areas of the Cyber Operations program.

Table 6 contrasts UMUC's proposed M.S. in Cyber Operations with the CTU's M.S. in Cyber and Information Security

Table 6: Comparison of UMUC Master's in Cyber Operations to Capitol Technology University (CTU)'s Master's in Cyber and Information Security

	UMUC M.S. in Cyber Operations	**Capitol Technology University (CTU)'s Master's in Cyber and Information Security**
Degree Requirements and Structure (number of credits, a single required sequence vs. electives)	36 credits A single sequence of six 6-credit courses, no electives	36-39 credits; all courses are 3-credit courses 24 to 27 credit core curriculum, plus 12 credits of electives The program is designated as an NSA/DHS Center of Excellence in Cyber Defense (but not Cyber Operations).
Delivery (onsite vs. online)	Online (asynchronous); no on site requirements	Online with a synchronous component, i.e., live sessions on Saturdays and weekday evenings.
Enrollment (full-time vs. part-time)	Most students are part-time (6 credits per term)	Full-time and part-time students
Admissions Requirements/Target Audience	UMUC is an open-admission institution. For the MS COP, students must demonstrate competencies in real-world computer sciences, specifically in the following areas: (1) C, assembler and system programming, (2) operating systems, (3) computer architecture, (4) mobile and cellular communications and networking, (5) virtualization & cloud computing, and (6) discrete mathematics. (A missing proficiency can be	Background in computer information systems, computer networking, telecommunications, information technology, network security, or computer science. Undergraduate degree with a cumulative GPA of no less than 3.0 on a 4.0 scale. Targeted at both full-time, and part-time working professionals

	acquired from one or more courses from UMUC's undergraduate school.) Targeted at working professionals with prior experience in the field	
Primary Points of Differentiation in Requirements and Target Audience: The UMUC program is completely asynchronous. This provides extreme flexibility for working professionals and active military and intelligence personnel stationed throughout the world.		
CIP Code	111003 Title: Computer and Information Systems Security/Information Assurance Definition: A program that prepares individuals to assess the security needs of computer and network systems, recommend safeguard solutions, and manage the implementation and maintenance of security devices, systems, and procedures. Includes instruction in computer architecture, programming, and systems analysis; networking; telecommunications; cryptography; security system design; applicable law and regulations; risk assessment and policy analysis; contingency planning; user access issues; investigation techniques; and troubleshooting.	119999 Title: Computer and Information Sciences and Support Services, Other. Definition: Any instructional program in computer and information sciences and support services not listed in other programs under the broad category, 11: Computer and Information Sciences and Support Services.
Primary Points of Differentiation in CIP: This CTU program began in 2002. The CIP code 119999 has been used to capture the then-evolving area, Cyber and Information Security, in the broader category of Computer and Information Sciences. The CIP code for the UMUC program, 111003, captures skills and technologies for the current state of cybersecurity.		

Pedagogy and Learning Model	The curriculum is based on principles of competency- and performance-based learning and authentic assessments are embedded throughout; students "learn by doing" through scenario-based projects grounded in real-world situations and problems and using interactive tools and case studies which incorporate applied learning. Foundational to the program is a first course that covers the core competencies of written and oral communications, critical thinking, quantitative reasoning and leadership. Five additional 6-credit courses for domain-specific competency and skills.	The program focuses on domain-specific skills and project management; the program emphasizes application-based laboratory exercises.
Program Content	The M.S. in Cyber Operations focuses on both cyber offense and cyber defense. Grounded in real-world, authentic projects, it is an interdisciplinary program that provides a solid foundation in competencies and skills related to: security principles and architecture; networks security; risk analysis; applied cryptography; digital forensics; design, implementation and analysis of secure software; reverse engineering for malware analysis; laws and ethics related to cyber offensive campaigns; and cyber offense skills that include surveillance, targeting,	24-27 credit core curriculum in Information Assurance and Cybersecurity with 12 credits of electives from the areas of Network Operations, Network Engineering, Information Assurance, Software Assurance, and Project management and Writing.

	penetration, and exploitation.	
Primary Points of Differentiation in Pedagogy/Learning Model and Content: UMUC's program uses a learning model based on the principles of competency- and performance-based learning. Its content is a blend of courses in both cyber defense and offense to satisfy the requirements of the NSA Centers of Excellence in Cyber Operations. The core courses of the CTU program are in cyber defense only.		

Table 7 contrasts UMUC's M.S. in Cyber Operations with the JHU's M.S. in Cyber and Information Security.

Table 7: Comparison of UMUC M.S. in Cyber Operations to Johns Hopkins University (JHU)'s Master of Science in Security Informatics

	UMUC M.S. in Cyber Operations	**Johns Hopkins University (JHU)'s Master of Science in Security Informatics (MSSI)**
Degree Requirements and Structure (number of credits, a single required sequence vs. electives)	36 credits A single sequence of six 6-credit courses, no electives	10 courses, each of 3 or more credit hours, plus a capstone project; students can choose between two tracks – Technology & Research Track or Policy & Management Track.
Delivery (onsite vs. online)	Online (asynchronous); no on site requirements	Onsite
Enrollment (full-time vs. part-time)	Most students are part-time (6 credits per term)	Full-time, three-semester program
Admissions Requirements/Target Audience	UMUC is an open-admission institution. For the MS COP, students must demonstrate competencies in real-world computer sciences, specifically in the following areas: (1) C, assembler and system programming, (2) operating systems, (3) computer architecture, (4) mobile and cellular communications and networking, (5) virtualization	Knowledge in computer architecture/networking, programming, data structures, and discrete math. This can be shown through courses and in some cases through working experience and professional certification. GRE General Test – Verbal: 153 (62%), Quantitative: 160 (84%), Analytical: 3.5. Targeted at full-time students

	& cloud computing, and (6) discrete mathematics. (A missing proficiency can be acquired from one or more courses from UMUC's undergraduate school.) Targeted at part-time, working adults with prior experience in the field.	
Primary Points of Differentiation in Requirements and Target Audience: The UMUC program's structure and admissions requirements target working adults whereas the JHU program is a full-time, on-site, three-semester program.		
CIP Code	111003 (same)	111003 (same)
Pedagogy and Learning Model	The curriculum is based on principles of competency- and performance-based learning and authentic assessments are embedded throughout; students "learn by doing." Foundational to the program is a first course that covers the core competencies of written and oral communications, critical thinking, quantitative reasoning and leadership. Five additional 6-credit courses for domain-specific competency and skills.	The program focus is on the domain-specific skills using the Instructor-led onsite classroom-learning model. Research and professional opportunities to supplement classroom learning
Program Content	The M.S. in Cyber Operations focuses on both cyber offense and cyber defense. Grounded in real-world, authentic projects, it is an interdisciplinary program that provides a solid foundation in competencies and skills related to: security principles and architecture; networks security; risk analysis; applied cryptography; digital	Courses are divided into several categories including: (1) Core Technology, (2) Elective Technology, (3) Core Policy, and (4) Elective Policy/Health/Management. For both Policy and Technology tracks, courses are required from both cores.

	forensics; design, implementation and analysis of secure software; reverse engineering for malware analysis; laws and ethics related to cyber offensive campaigns; and cyber offense skills that include surveillance, targeting, penetration, and exploitation.	
Primary Points of Differentiation in Pedagogy/Learning Model and Content: UMUC's program uses a learning model based on the principles of competency- and performance-based learning. It is a blend of courses in both cyber defense and offense to satisfy the requirements of the NSA Centers of Excellence in Cyber Operations. Students receive broad training in cyber offense laws, reverse engineering and exploitation through software vulnerabilities, giving the program an emphasis on cyber offense as well as defense. The JHU MSSI program focuses primarily on cyber defense with courses required in both technology and policy tracks, with one core technology course on ethical hacking at JHU. It is not clear to what extent the JHU program can be tailored to meet the NSA Center of Excellence in Cyber Operations within 30 credit hours given other existing requirements.		

Note: Johns Hopkins University also offers an online Master's program in cybersecurity with specialization in one of three tracks: (1) Analysis, (2) Networks and (3) Systems, with flexibility to tailor the program to one's own needs. It is not clear to what extent this program can be tailored to meet the NSA Center of Excellence in Cyber Operations within 30 credit hours. Additionally, certain key areas of cyber offense, including malware analysis and exploitation, and laws or cyber offense do not appear to be covered in this program's course offerings.

Table 8 contrasts UMUC's M.S. in Cyber Operations with UMCP's M.S. in Cyber and Information Security.

Table 8: Comparison of UMUC M.S. in Cyber Operations to University of Maryland, College Park (UMCP)'s Master of Engineering in Cybersecurity		
	UMUC M.S. in Cyber Operations	**University of Maryland, College Park (UMCP)'s Professional Master of Engineering (M. Eng.) in Cybersecurity**

Degree Requirements and Structure (number of credits, a single required sequence vs. electives)	36 credits A single sequence of six 6-credit courses, no electives.	30 credits with six required 3 credit-hour courses and 12 credit-hours of electives
Delivery (onsite vs. online)	Online (asynchronous); no on site requirements	Courses are offered onsite with video conferencing for remote campuses and webcast for delayed viewing.
Enrollment (full-time vs. part-time)	Most students are part-time (6 credits per term)	Part-time and full-time
Admissions Requirements/Target Audience	UMUC is an open-admission institution. For the MS COP, students must demonstrate competencies in real-world computer sciences, specifically in the following areas: (1) C, assembler and system programming, (2) operating systems, (3) computer architecture, (4) mobile and cellular communications and networking, (5) virtualization & cloud computing, and (6) discrete mathematics. (A missing proficiency can be acquired from one or more courses from UMUC's undergraduate school.) Targeted at working professionals with prior experience in the field	Full Admission: Bachelor's degree in Engineering, Computer Science, Applied Mathematics, or Physics, from an accredited institution, with a GPA of 3.0 or better; Provisional Admission: Bachelor's in a related field of study (i.e. Information Technology, Information Assurance, and Computer Information Systems), and a GPA of 3.0 or better. Must also possess at least one (1) of the following certifications: CompTIA Security+, GIAC GSEC, or Certified Ethical Hacker certification. Applicants admitted with Provisional Admission will need to complete two core courses with at least a B or better in each course. Special Admission: Bachelor's degree in other fields of study with a minimum 3.0 GPA, one of the certifications: CompTIA Security+, GIAC GSEC, or Certified Ethical Hacker certification, and 2+ years' work experience (after the completion of the Bachelor's degree) in Information

		Technology or other closely related field. Applicants admitted through Special admission will need to complete two core courses with at least a B or better in each course to be fully admitted. Targeted at working professionals
Primary Points of Differentiation in Requirements and Target Audience: The UMCP program emphasizes the attainment of specific skills, certifications, and educational experience for admissions. The UMUC program takes a different approach, requiring that certain competencies be demonstrated to enter the program. The UMUC program does not require specific credentials.		
Pedagogy and Learning Model	The curriculum is based on principles of competency- and performance-based learning and authentic assessments are embedded throughout; students "learn by doing" through scenario-based projects grounded in real-world situations and problems and using interactive simulation tools and case studies which incorporate applied learning. Foundational to the program is a first course that covers the core competencies of written and oral communications, critical thinking, quantitative reasoning and leadership. Five additional 6-credit courses for domain-specific competency and skills.	The program focus is on the domain-specific skills. Onsite classroom instructional model extended to support distance and time-delayed content presentation and interaction. The learning model also uses several asynchronous forms of interactions: chat, bulletin board, video chat, group presentation, and discussion sessions
Program Content	The M.S. in Cyber Operations focuses on both cyber offense and cyber defense. Grounded in real-world, authentic projects, it is an interdisciplinary program that provides a solid foundation in competencies and skills related to: security principles	The five core courses emphasize cyber defense. The core courses are: Security Tools for Information Security; Information Assurance; Programming in C for Cybersecurity Applications; Network Security; Networks and

	and architecture; networks security; risk analysis; applied cryptography; digital forensics; design, implementation and analysis of secure software; reverse engineering for malware analysis; laws and ethics related to cyber offensive campaigns; and cyber offense skills that include surveillance, targeting, penetration, and exploitation.	Protocols; Secure Operating Systems; 12 credits of electives
Primary Points of Differentiation in Pedagogy/Learning Model and Content: The UMUC program meets the requirements of the NSA Centers of Excellence in Cyber Operations. The UMCP Master of Engineering in Cybersecurity program does not appear to be structured to meet the requirements of the NSA Centers of Excellence in Cyber Operations (as described on UMCP program website, not all skills and topics identified by the Center as key to cyber operations appear to be offered in the program; many of those that are appear to be covered through elective courses and no course is offered on cyber offense techniques and laws).		

Three other cyber-related programs in the state are very different from UMUC's proposed program. Below is a synopsis of how UMUC's proposed program differs from these programs:

- Master of Professional Studies, University of Maryland, Baltimore County (UMBC): The UMBC Cybersecurity program is a 10 course, 30 credit program that balances technical and non-technical aspects of cybersecurity. It includes a policy course on cyber warfare but does not appear to include courses to train cyber warriors in areas such as software security, digital forensics, and malware analysis and exploitation. UMUC's fully online program provides flexibility in time and space for working professionals compared to the onsite instructional model at UMBC.
- M.S. in Cybersecurity Engineering Technology, University of Maryland Eastern Shore: The focus of the University of Maryland, Eastern Shore program is network security and security administration. There is no emphasis on offense, software security, forensics and other areas emphasized in the UMUC Cyber Operations program.
- M.S. in Cyber Forensics, Stevenson University: The Stevenson University program is devoted to cyber forensics. The program goal, as stated on the program's website, is to train technology professionals to preserve, acquire, analyze, interpret, and document critical forensic findings for use in legal and computer security proceedings. Forensics plays an important role in cyber operations, but cyber operations encompass many other dimensions and domains.

F. Relevance to Historically Black Institutions (HBIs)

A search of the MHEC inventory of approved academic programs in Maryland found no graduate programs in Cyber Operations or Cybersecurity Operations that would be considered duplicative with this proposed UMUC program. This includes the four Historically Black Institutions in Maryland (Bowie State University, Coppin State University, University of Maryland Eastern Shore, or Morgan State University). Thus, UMUC's proposed program will have no impact on the uniqueness and institutional identities and missions of the HBIs, and will not harm these schools or other institutions in Maryland.

G. Evidence of Principles of Good Practice

The proposed program will be offered fully online. UMUC's approach to online learning is to provide a highly interactive environment that supports the development of competencies in written and oral communication, critical thinking, quantitative reasoning, leadership and discipline knowledge – the five graduate learning areas identified as institutional-level learning outcomes by the university's *Institutional Plan for the Assessment of Student Learning* (http://www.umuc.edu/visitors/about/ipra/learning-outcomes.cfm).

1. Curriculum and Instruction

UMUC is committed to providing the best online teaching and learning possible and to excellence in all of its programs. There is no difference in coherence, cohesiveness, or academic rigor between programs offered in traditional instructional formats and those offered online. Each program is designed to result in learning outcomes appropriate to the rigor and breadth of the program and all programs assess student achievement of defined learning outcomes through regular and formal assessment planning. Online and onsite courses and programs are fully aligned and integrated -- designed around the same learning outcomes and principles, overseen and taught by the same faculty, held to the same standards, and assessed in the same way.

All of UMUC's online courses have been designed by faculty members in appropriate disciplines in collaboration with instructional designers and other experts in the field. Course learning outcomes and course descriptions are the same for every section of the course. The learning outcomes for each course are the foundation of the course; the teaching and learning activities, assessments and content of the course are in alignment with the outcomes and provide a clear pathway for mastery of the outcomes.

2. Role and Mission

All programs at UMUC are designed to be consistent with the mission of the institution. Each program has a mission and program outcomes aligned to the university mission as described in the catalog.

All existing UMUC programs are subject to periodic academic program reviews, including the review of the appropriateness of the technology being used to meet a program's objectives. The schedule and results of periodic academic program reviews are reported to the University System of Maryland (USM).

3. Faculty Support

All UMUC faculty are trained to teach online, including training in the use of the learning management system as well as in the pedagogy of distance education. Additionally, faculty have the opportunity for additional trainings throughout the course of their employment with UMUC. All faculty have 24/7 access to support services for both on-site and on-line courses, including the learning management system.

As part of their formal training, new graduate faculty become familiar with the expectations that The Graduate School has set for them as well as their students. Program Chairs, the administrators responsible for managing the faculty and all aspects of an academic program, reinforce these expectations in their regular reviews of and communications with their faculty.

Additional support is provided through workshops offered by the University's Faculty Development unit, as well as online coaching and mentoring programs for faculty (http://www.umuc.edu/faculty/facsupport/). UMUC's learning management system provides appropriate real-time and asynchronous interaction between faculty and students in online classes, as well as access to course materials and a wide array of online library resources. All online classes have conferences in which students interact with faculty and with each other.

4. Students and Student Services

UMUC provides all students with clear, complete, and timely information on the curriculum, course and degree requirements, nature of faculty/student interaction, assumptions about technology competence and skills, technical equipment requirements, learning management system, availability of academic support services and financial aid resources, and costs and payment policies. Students have access to the complete range of student services available at UMUC in support of their distance education activities. All students are provided with the academic support they need to be successful in the online environment.

The program builds on a 6-credit foundational course that provides a springboard for academic and professional success. Students begin to practice prerequisite skills related their professions, create beneficial social networks and presence, and develop and exercise moral and ethical decision-making. Through these activities, they refresh and refine their skills in communication, critical thinking, quantitative reasoning and team leadership.

All advertising, recruiting, and admissions materials are the same for all students, and accurately represent programs and services available. Full information is available at www.UMUC.edu.

5. Commitment to Support

In accordance with UMUC policies, the teaching effectiveness of all faculty is evaluated on an ongoing basis. Further, faculty research, publications and other forms of scholarship, as well as administrative, professional and service activities and contributions commensurate with the program, school and institution missions are considered as part of faculty promotion.

Inherent in pursuit of the institutional mission and reflected in institutional business practices, UMUC is committed to investing the requisite resources to delivering high-quality academic programs that are directly career-relevant, and supporting the needs of students, employers and other stakeholders to continually review and refine those programs to facilitate student degree completion and career-readiness.

6. Evaluation and Assessment

Students have the opportunity to evaluate courses and faculty through a standard evaluation process. In addition, faculty are evaluated by their supervisors on a pre-determined schedule using a standard evaluation instrument employing direct observation.

Formal evaluation of student learning occurs within courses and programs via annual review of student performance in authentic learning demonstrations. Learning goals and competencies are aligned to learning demonstrations that comprise the curriculum. Annually, student performance across learning demonstrations is evaluated to determine where improvements may be required. Changes are made to curriculum and/or student support models. The process supports a continuous cycle of improvement.

Additional evaluation includes tracking of student retention, grade distributions and cost- effectiveness. Regular academic program reviews consider all factors related to academic quality, curriculum currency and relevance, student support and adequacy of facilities.

H. Adequacy of Faculty Resources

UMUC's model employs full-time faculty (known as collegiate faculty) in faculty leadership roles, such as Vice Deans and Program Chairs, who have responsibility for the overall intellectual coherence and integrity of the program. Other collegiate faculty teach and serve in other roles that maintain and support the academic programs, providing input into the design and content of the program and their

courses.

This core group of collegiate faculty is small (about 10 percent of the total faculty). In keeping with UMUC's emphasis on workplace relevance, most teaching faculty are professionals in their field who teach part-time for UMUC. These adjunct faculty provide instruction for the great majority of courses at all levels and in all programs. This model is responsible for one of UMUC's greatest strengths: scholar-practitioner faculty who have solid academic credentials but continue to work outside the university, providing a continuous infusion of current workplace knowledge as well as maximum flexibility for adapting to changing student demand. In this way, UMUC supports students in a learning experience that is practical and relevant to today's competitive and evolving global marketplace. Many adjuncts have considerable experience with UMUC. As of 2015, the average longevity for an adjunct faculty member is six years, and 17 percent of current adjunct faculty have been with UMUC more than 10 years. Collegiate and adjunct faculty both hold academic rank and title, based on their academic qualifications and professional experience, including teaching experience at UMUC. Since 1996 UMUC has held a MHEC-approved waiver of the Code of Maryland (COMAR) requirements for total credit hours taught by full-time faculty (Appendix B).

The centrality and appropriateness of UMUC's faculty model relative to its educational mandate and mission was reaffirmed by MHEC in the most recent review of mission statements, as evidenced in the following excerpt from the Commission's report:

> *UMUC intentionally seeks highly-qualified full-time and adjunct faculty who have hands-on experience in the disciplines they teach and who can leverage that experience to provide a richer learning experience for students. The university's mission to serve adult students is supported by adjunct faculty who are scholar-practitioners engaged daily in their profession. The ability to employ adjunct faculty is critical to UMUC's capacity to quickly deploy academic and continuing education programs in response to workforce-related needs. This entrepreneurship and flexibility in establishing new programs is particularly important to the university: given its history of very limited state support, the university's financial model is based on tuition revenues, and all programs must be self-supporting.*[7]

Consistent with this model, UMUC has a substantial roster of faculty with expertise in areas related to cybersecurity, including cyber operations. A terminal degree is generally required to teach at the graduate level, although an occasional exception can be made in the case of an individual with a master's degree and exceptional professional credentials. Teaching effectiveness is monitored by class observation and student course evaluations. Because this revised degree is an expansion of an existing A.O.C., the program already has an active unit of faculty prepared to teach courses in the revised curriculum.

Table 9 provides a partial list of faculty with their highest degree title, academic title/rank, and the courses they will teach:

[7] Maryland Higher Education Commission (December 2015), Mission Statement Review: http://mhec.maryland.gov/institutions_training/Documents/acadaff/2016MissionStatementReview.pdf

Table 9: Faculty Resources				
Name	**Appointment Type and Rank**	**Terminal Degree and Field**	**Status**	**Course(s) to be Taught**
Mansurul Hasib	Collegiate Faculty, Associate Professor	PhD, Information Assurance	Full-time	CBR 600
Balakrishnan Dasarathy	Collegiate Faculty, Professor	PhD, Computer and Information Sciences	Full-time	COP 610, COP 620, COP 640
Jim Chen	Adjunct Faculty, Professor	PhD, Linguistics	Part-Time	COP 610, COP 620
Stephen Gantz	Adjunct Faculty, Professor	DM, Management	Part-Time	COP 610, COP 620
Nicholas Oldham	Adjunct Faculty, Assistant Professor	JD	Part-Time	COP 630
Douglas Kelly	Adjunct Faculty, Associate Professor	PhD, Computer Science	Part-Time	COP 610, COP 620, COP 640
Michelle Hansen	Collegiate Faculty, Assistant Professor	PhD, Computer Information Systems	Full-Time	COP 630, COP 670

I. Adequacy of Library Resources

No new library resources are needed to serve the proposed program. The UMUC Library provides access to a vast array of library resources and services to UMUC students, faculty, and staff worldwide to meet their academic needs and include a wide and varied collection of journal articles, reports, case studies, and, in some instances, complete books available electronically via a comprehensive selection of online library databases. Library services include instruction, reference, electronic reserves, and document delivery for materials not otherwise available in the library databases. The UMUC Library relies on technology as its primary mechanism to provide online access to resources and services to UMUC's widely dispersed, nontraditional student population.

The curated collection of online academic research databases available to UMUC faculty and students provides access to hundreds of thousands of full text articles as well as reports, statistics, case studies, book chapters and complete books in a wide range of subject areas. In addition, students have access to the full text of dissertations and theses via the *ProQuest Dissertations and Theses* database. The Library assists faculty in providing links to Library materials directly in online classes.

The UMUC Library also offers other resources and services. UMUC students, faculty, and staff within the continental United States have access to more than ten million volumes in print from the 16-member University System of Maryland and Affiliated Institutions (USMAI) library consortium. The UMUC Library offers document delivery services to all UMUC students, faculty, and staff worldwide for a variety of materials, including journal articles and book chapters. UMUC's expanding collection of 75,000 electronic books (e-books) has significantly increased the ability to meet the needs of UMUC's global population.

The UMUC Library provides faculty and students with research assistance in creating search strategies, selecting relevant databases, and evaluating and citing resources in a variety of formats via its *Ask a Librarian* service at https://www.umuc.edu/library/libask/index.cfm, which includes 24/7 chat and e- mail. A guide to locating scholarly articles and using UMUC's library databases is available at http://www.umuc.edu/library/libhow/articles.cfm. The UMUC Library *OneSearch* tool allows users to simultaneously search for scholarly articles, books, and/or other research resources via a single search engine in most of the databases to which the UMUC Library subscribes, either directly or as additional resources (http://www.umuc.edu/library/index.cfm).

In addition, UMUC faculty can request customized library instruction sessions for both on-site and online classes, and can also add UMUC Library tutorials and materials to their learning management system classrooms and refer students to them through the Webgateway.

A librarian liaison assigned to each academic department assists faculty with resource identification and other program needs. The Subject Guides area of the library's Web site at http://www.umuc.edu/library/libresources/subjects.cfm provides a listing of resource guides for each subject area, with each guide containing relevant databases, Web sites, books, and other resources along with technical and citation assistance.

J. Adequacy of Facilities, Infrastructure, and Equipment

Existing resources related to facilities, infrastructure, and equipment are adequate to meet the program needs. This program draws on existing faculty who are currently equipped with the necessary facilities, resources and equipment. Further, the nature of UMUC's distance education delivery modality negates the need for any physical classroom.

K. Adequacy of Financial Resources

No new general funds are required for implementation of the proposed revision to this program. As shown in the following tables, the program is expected to be self-supporting from inception. If necessary, resources will be reallocated from the existing program to support the restructured program in year one. The financial tables that follow are based only on students entering the restructured program and do not include revenue and expenses related to the teach-out of students in the existing program.

Resources					
Resource Categories	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**
1. Reallocated Funds	**0**	**0**	**0**	**0**	**0**
2. Tuition/Fee Revenue	$624,600	$1,286,676	$1,411,596	$1,536,516	$1,661,436
a. # Students	50	103	113	123	133
b. Credit Hour Rate	$694	$694	$694	$694	$694
c. Credit Hours per student per	18	18	18	18	18
d. Total Tuition Revenue (a x b x c)	$624,600	$1,286,676	$1,411,596	$1,536,516	$1,661,436
3. Grants, Contracts, & Other External	$0	$0	$0	$0	$0
4. Other Sources	$0	$0	$0	$0	$0
TOTAL (Add 1 - 4)	**$624,600**	**$1,286,676**	**$1,411,596**	**$1,536,516**	**$1,661,436**

Expenditures					
Expenditure Categories	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**
1. Total Faculty Expenses (b + c below)	$45,756	$91,512	$114,390	$114,390	$137,268
a. Total sections taught	6	12	15	15	18
b. Total Salary (Adjunct faculty salary at average of $7626 per 6-credit course)[8]	$45,756	$91,512	$114,390	$114,390	$137,268
c. Total Benefits	N/A	N/A	N/A	N/A	N/A
2. Total Administrative Staff Expenses (b + c below)	$25,300	$25,300	$25,300	$25,300	$25,300
a. # FTE	0.2	0.2	0.2	0.2	0.2
b. Total Salary	$20,000	$20,000	$20,000	$20,000	$20,000
c. Total Benefits (26.5%)	$5,300	$5,300	$5,300	$5,300	$5,300
3. Total Support Staff Expenses (b + c below)	$12,650	$12,650	$12,650	$12,650	$12,650

[8] This field has been modified from #FTE to the total number of program course sections taught per year, consistent with UMUC's faculty model.

a. # FTE	0.2	0.2	0.2	0.2	0.2
b. Total Salary	$10,000	$10,000	$10,000	$10,000	$10,000
c. Total Benefits (26.5%)	$2,650	$2,650	$2,650	$2,650	$2,650
4. Equipment	0	0	0	0	0
5. Library	0	0	0	0	0
6. New or Renovated Space	0	0	0	0	0
7. Other Expenses (Course development, marketing, overhead)	$35,000	$35,000	$25,000	$25,000	$25,000
TOTAL (Add 1 - 7)	**$118,706**	**$164,462**	**$177,340**	**$177,340**	**$200,218**

L. Adequacy of provisions for evaluation of program

As discussed above under "Evaluation and Assessment," all UMUC programs are subject to comprehensive and multi-pronged evaluations. These include course and faculty assessment, program- specific student-level competency assessment, institution-wide student learning outcomes, and program outcomes among others. Assessment is a dynamic and engaged process at UMUC; the university's Assessment Steering Committee provides coordination and advisement, and disseminates best practices throughout the institution. Faculty, administrators, and the Office of Accreditation, Compliance and Reporting in the Provost's Office collaborate to implement assessment activities, review results and make appropriate resource, curriculum or other modifications accordingly.

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

UMUC seeks to reflect the diversity of the global community within which it exists. Cultural differences are recognized, valued, and considered essential to the educational process. UMUC provides an academic environment in which diversity is not only articulated as one of the institutional core values, but it is reflected in the University's ethnically and racially diverse student body and its proven record of providing higher education access to minority students.

- As of Fall 2015, 44% of all undergraduate students and 51% of all graduate students are minority students*.
- Additionally, UMUC enrolls more African American students (14,348) than any other institution in Maryland, including any single one of the four Maryland HBIs. Morgan State University is second with 6,280 African American students[9].
- In Fiscal Year 2016, 41% of bachelor's degrees, 50% of master's degrees, and 39% of doctoral degrees were awarded to minority students*.
- Annually, UMUC awards more degrees to African American students than any other Maryland institution, including the four Maryland HBIs in Maryland.

[9] Source: 2016 MHEC Data Book, http://mhec.maryland.gov/publications/Documents/Research/AnnualPublications/2016Databook.pdf

**Minority students* is defined here as Blacks/African Americans, Latino/Hispanics, Asian, Pacific Islander, and Native Americans, plus those of two or more races.

N. Relationship to low productivity programs identified by the Commission

Not applicable.

Appendix A
Course Descriptions

Required Foundation Course

CBR 600 Communicating, Problem Solving, and Leading in Cybersecurity (6)
(Required for students in the MS in Cyber Operations, Cybersecurity Technology, Cybersecurity Management and Policy, and Digital Forensics and Cyber Investigation programs.) Make yourself more valuable to an employer by gaining and improving skills in communication and problem solving. Explore the field of cybersecurity by developing connections to your career aspirations, creating a professional social network presence, and using critical thinking to inform decisions. Improve and refine your skills in communication, critical thinking, quantitative reasoning, and team leadership. Hone your professional writing and oral communication skills to produce effective presentations and become proficient with current technology.

Required Program Courses

COP 610 Foundations of Cyber Operations (6)
Prerequisite: CBR 600. Gain the foundational information security knowledge and skills needed to work in cyber operations, including security first principles, access control, and layered defense. Apply risk analysis of information and information systems, integrate cryptographic techniques for protecting information, and crack codes through the use of cryptanalysis.

COP 620 Cybersecurity Defense (6)
Prerequisite: COP 610. Master the application of defense-in-depth architecture in system design and deployment, and counteract threats and vulnerabilities in networks, devices, operating systems, data management systems, and applications. Identify cloud and virtualization security issues and respond to them using appropriate countermeasures. Apply intrusion and attack detection techniques in a laboratory.

COP 630 Cyber Law and Digital Forensics (6)
Prerequisite: COP 620. Explore U.S. and international laws governing cyber operations and digital evidence. Design a cyber-offense campaign that complies with U.S laws. Master digital forensics tools and techniques for network, media, and RAM of common operating systems and devices in a virtual laboratory environment.

COP 640 Secure Software (6)
Prerequisite: COP 630. Explore secure design and operation principles by examining classes of well- known defects that lead to security vulnerabilities, and utilize both static and dynamic analysis tools to find those vulnerabilities. Apply secure design principles to design software in a virtual laboratory environment.

COP 670 Capstone in Cyber Offense (6)
Prerequisite: COP 640. Assume the role of a cyber-warrior. Apply reverse engineering techniques to

analyze malware and system software, and implement cyber-offense techniques in a laboratory to penetrate and infect a system that lacks cyber defenses.

Appendix B

90.2.1.001

cc: LEL
Bob S.

MHEC
Creating a state of achievement

MEMORANDUM

Office of the Provost
UMUC
JAN 10 2005

DATE: January 6, 2005

TO: Dr. Nicholas H. Allen
Provost and Chief Academic Officer, UMUC

FROM: Michael J. Kiphart, Ph.D. MJK
Assistant Secretary for Planning and Academic Affairs

SUBJECT: UMUC Waiver of Full-Time Faculty and Library/Learning Resources Center

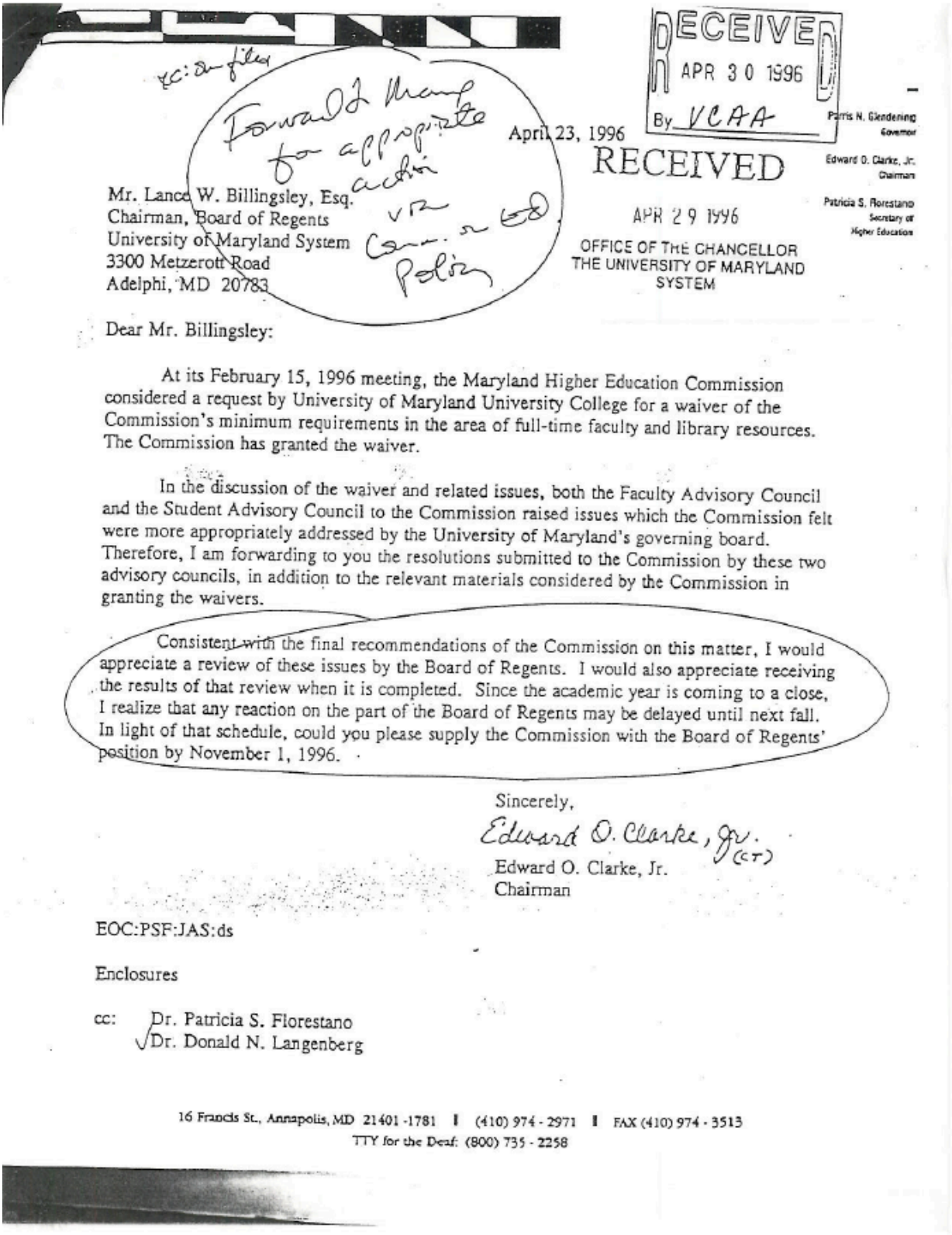
According to our records, UMUC's request for a waiver of full-time faculty and library/learning resource center went before the Education Policy Committee on January 16, 1996. The Education Policy Committee approved for the University a waiver of the definition of full-time faculty and library/learning resource center as provided for in the Commission's *Minimum Requirements for Degree-Granting Institutions*, and further, that the Commission instruct the Secretary of Higher Education to review the University at regular intervals to assure that the University was in compliance with the applicable provisions of the waiver to the minimum requirements.

On February 15, 1996, the matter went before the Commission and an amended recommendation was approved. The Commission approved for the University a waiver of the requirements for total credit hours taught by full-time faculty and for a waiver of the requirements for a minimum library collection for the Library/Learning Resource Center as provided for in the Commission's *Minimum Requirements for Degree-Granting Institutions*. Further, the Commission instructed the Secretary of Higher Education to review the University at regular intervals to assure that the University was in compliance with the applicable provisions of the waiver to the minimum requirements. The Commission also approved a recommendation that the Faulty Advisory Council and Student Advisory Council recommendations be referred to the University of Maryland System Board of Regents.

Enclosed are documents supporting the approval of the waiver. Should you require additional assistance, please contact David Sumler, Director of Academic Affairs – Planning and Policy, at 410-260-4533 or dsumler@mhec.state.md.us.

MJK:aaw
Enclosures

MARYLAND HIGHER EDUCATION COMMISSION
839 Bestgate Rd. • Suite 400 • Annapolis, MD 21401-3013
T 410.260.4500 • 800.974.0203 • F 410.260.3200 • TTY for the Deaf 800.735.2258 • www.mhec.state.md.us



cc: Dr. file

Forward for appropriate action VCAA Comm. re Ed Policy

RECEIVED
APR 30 1996
By VCAA

April 23, 1996

RECEIVED
APR 29 1996
OFFICE OF THE CHANCELLOR
THE UNIVERSITY OF MARYLAND SYSTEM

Parris N. Glendening
Governor

Edward O. Clarke, Jr.
Chairman

Patricia S. Florestano
Secretary of
Higher Education

Mr. Lance W. Billingsley, Esq.
Chairman, Board of Regents
University of Maryland System
3300 Metzerott Road
Adelphi, MD 20783

Dear Mr. Billingsley:

At its February 15, 1996 meeting, the Maryland Higher Education Commission considered a request by University of Maryland University College for a waiver of the Commission's minimum requirements in the area of full-time faculty and library resources. The Commission has granted the waiver.

In the discussion of the waiver and related issues, both the Faculty Advisory Council and the Student Advisory Council to the Commission raised issues which the Commission felt were more appropriately addressed by the University of Maryland's governing board. Therefore, I am forwarding to you the resolutions submitted to the Commission by these two advisory councils, in addition to the relevant materials considered by the Commission in granting the waivers.

Consistent with the final recommendations of the Commission on this matter, I would appreciate a review of these issues by the Board of Regents. I would also appreciate receiving the results of that review when it is completed. Since the academic year is coming to a close, I realize that any reaction on the part of the Board of Regents may be delayed until next fall. In light of that schedule, could you please supply the Commission with the Board of Regents' position by November 1, 1996.

Sincerely,

Edward O. Clarke, Jr. (ET)

Edward O. Clarke, Jr.
Chairman

EOC:PSF:JAS:ds

Enclosures

cc: Dr. Patricia S. Florestano
Dr. Donald N. Langenberg

16 Francis St., Annapolis, MD 21401-1781 | (410) 974-2971 | FAX (410) 974-3513
TTY for the Deaf: (800) 735-2258