BOARD OF REGENTS

SUMMARY OF ITEM FOR ACTION,
INFORMATION, OR DISCUSSION

TOPIC: University of Maryland Eastern Shore: Master of Science in Cybersecurity Engineering Technology

COMMITTEE: Education Policy and Student Life

DATE OF COMMITTEE MEETING: March 3, 2015

SUMMARY: The proposed Master of Science in Cybersecurity Engineering Technology is designed to be accredited by the Association of Technology, Management, and Applied Engineering (ATMAE), which UMES is planning to pursue during the 2020/2021 academic year. A Master's degree in Cybersecurity Engineering Technology that can be formally accredited by ATMAE stands to serve as a regional role model for producing high-quality leaders for professional services and industries in cybersecurity and related fields. ATMAE accredits graduate programs/options that prepare individuals for career advancement that involve the management of complex technological systems.

There are a tremendous number of unfilled cybersecurity positions within the federal government and Cybersecurity is expected to continue to be a vital area of need for most government agencies and federally funded research and development centers (FFRDC). Due to the shortage of cybersecurity professionals, there are excellent opportunities for job placement for graduates of the proposed graduate degree program. To support the proposed graduate program, due to its location, UMES is uniquely positioned to develop a strong working relationship with agencies such as: National Security Agency (NSA), Central Intelligence Agency (CIA), Department of the Navy: the Space and Naval Warfare Systems Command (SPAWAR), Department of Homeland Security (DHS), Federal Emergency Management (FEMA) Institute, Johns Hopkins University's Applied Physics Lab, United States Army Intelligence and Security Command (INSCOM). Institutions of higher education have also expressed a need for cybersecurity staff members. And, the national shortage of technical cybersecurity staff continues to grow at the same rate as the shortage of competent cybersecurity professionals in federal agencies.

Cybersecurity Engineering Technology as a career field has specific synergies with current University of Maryland Eastern Shore (UMES) academic programs such as Engineering Technology – Electrical/Electronic Engineering Technology, Computer Science, and Engineering. As such, it is anticipated that no new full-time faculty or facility resources will be needed in the first two years of the program.

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

FISCAL IMPACT: No additional funding is necessary. The program will be supported through tuition.

CHANCELLOR'S RECOMMENDATION: That the Committee on Education Policy and Student Life recommend that the Board of Regents approve the proposal from the University of Maryland Eastern Shore to offer the Master of Science in Cybersecurity Engineering Technology.

COMMITTEE RECOMMENDATION:	DATE
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 Eastern Shore

Institution Submitting Proposal

Cybersecurity Engineering Technology

Title of Proposed Program

Master of Science	Spring 2016
Award to be Offered	Projected Implementation Date
070210	111003
Proposed HEGIS Code	Proposed CIP Code
Department of Technology	Derrek Butler Dunn
Department in which program will be located	Department Contact
(410) 651-6465	ddunn@umes.edu
Contact Phone Number	Contact E-Mail Address
Signature of President or Designee	Date

A. Centrality to institutional mission statement and planning priorities:

University of Maryland Eastern Shore (UMES), the State's Historically Black 1890 Land-Grant institution, emphasizes baccalaureate and graduate programs in the liberal arts, health professions, sciences, engineering and technology, and teacher education. In keeping with its land-grant mandate, the University's purpose and uniqueness are grounded in distinctive learning, discovery, and engagement opportunities in agriculture, human ecology, marine and environmental sciences, technology, engineering and aviation sciences, health professions, business, and hospitality management. Degrees are offered at the bachelor's, master's and doctoral levels.

UMES is committed to providing access to high quality, value-based, educational experiences, including individuals who are first-generation college students of all races, while emphasizing multicultural diversity and international perspectives. In addition, the University serves the education and research needs of businesses, industries, government and non-government organizations. The University is committed to meeting the economic development needs on the Eastern Shore; workforce development needs of the State; international development priorities of the nation; and commercialization and entrepreneurial ventures of the University, through engagement activities, and partnerships.

A Master's degree in Cybersecurity Engineering Technology that is designed to be accredited by the Association of Technology, Management, and Applied Engineering (ATMAE), which UMES is planning to pursue during the 2020/2021 academic year, falls directly in-line with the type of academic program the university currently offers. Cybersecurity Engineering Technology as a career field has specific synergies with current University of Maryland Eastern Shore (UMES) academic programs such as Engineering Technology – Electrical/Electronic Engineering Technology, Computer Science, and Engineering. UMES' mandate as a land grant university is to provide economic development and workforce development support for Maryland's businesses and citizenry. To that end, it is a natural progression that UMES should provide support for Maryland's economic role in the tri-state Delmarva region. Moreover, the University's mission as a Historically Black University is to provide opportunities for students from under-served populations and first generation college students. A Master's degree in Cybersecurity Engineering Technology that can be formally accredited by ATMAE stands to serve as a regional role model for producing high-quality leaders for professional services and industries in cybersecurity and related fields. Expansion of the Engineering Technology program at UMES has been part of the strategic plan of the University for the growth of STEM related majors for more than five years.

The addition of the proposed degree program supports the following goals from UMES President's 2011-2016 strategic plan:

Goal I: Develop, strengthen, and implement academic programs that are responsive to the UMES mission and are systematically reviewed for sustained quality, relevance, and excellence to meet the challenges of a highly competitive and global workforce.

In particular this request for this proposed program supports the following sub-goals of the President's 2011-2016 strategic plan:

Sub-Goal 1.2: Expand the capacity to offer unique and/or critical undergraduate, graduate, and professional academic programs that address regional workforce needs.

Sub-Goal 1.4: Increase student enrollment, retention and graduation rates in the Science, Technology, Engineering, Agriculture, and Mathematics (STEAM) fields.

Sub-Goal: 1.7: Obtain national program accreditations for eligible programs and reaffirmation of accreditation for existing programs.

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

The departmental faculty researched several graduate Cybersecurity programs from around the country and selected the best elements of those programs to formulate the graduate program proposed in this document. The program will consist of a 34 credit hour curriculum: 12 credits in required core courses; 21 credits in elective cybersecurity engineering technology related courses; and a 1 credit seminar course.

Total number of credits and their distribution:

Required Core Technology Courses	12 Credits
Elective Cybersecurity Engineering Technology Courses	21 Credits
Seminar Course	1 Credit
Total Credits Required	34 Credits

Master of Science in Cybersecurity Engineering Technology Curriculum Overview

Core Courses (12 Semester Hours)
ETCS 600 Statistical Applications for Technology
ETCS 606 Applied Research for Technology
ETCS 620 Project Management for Technology
ETCS 687 Legal and Ethical Issues in Cybersecurity

Elective Courses (21 Semester Hours)
ETCS 678 Mobile Wireless Networking and Security
ETCS 680 Networking Technology for Industry
ETCS 681 System Integrity for Cybersecurity
ETCS 682 Cybersecurity Administration
ETCS 683 Network Intrusion, Detection and Incidence Response
ETCS 685 Fundamentals of Network Security
ETCS 686 Advanced Network Security

Seminar Course (1 Semester Hour)
ETCS 690 Master's Seminar

The requirements for a non-thesis Master of Science degree vary among the graduate programs at UMES. Standards for admission are similar to those for any other Master's program. The quality of work expected of each student is also similar to that expected in the thesis program.

The general requirements for those of the non-thesis program are:

1. A minimum of 34 semester credit hours in courses approved for graduate credit with a minimum average grade of "B" in all course work taken.

2. A minimum of 18 semester credit hours in courses numbered 600 or above.

3. Successful submission of a seminar paper is required.

Admission Requirements
Admission requirements include a bachelor's degree in a technology related field, such as: Engineering Technology, Computer Science, Information Technology, Software or Computer Engineering, Networking, Information Security or related disciplines. Applications from candidates with bachelor's degrees in non-technical fields may be considered for admission if they provide evidence of work experience in the field of cybersecurity (such as a letter from their current supervisor) and possess one or more industry standard security certifications such as CompTia Security+, Certified Information Systems Security Professional (CISSP), Global Information Assurance Certification (GIAC) Security Expert (SE), Cybersecurity Program Plan (CSPP), or Certified Cyber Forensics Professional (CCFP). All applicants must show a strong record of academic achievement, as indicated by official transcript(s), three letters of recommendation, and satisfactory scores on either the Graduate Record Examination (GRE) or the Graduate Management Admission Test (GMAT).

Cybersecurity Engineering Technology Course Descriptions

ETCS 600 Statistical Applications for Technology Credits 3(3, 0)
This course presents a broad treatment of statistics, concentrating on specific statistical techniques used in science and industry. Prerequisite(s): Graduate Standing

ETCS 606 Applied Research for Technology Credits 3(3, 0)
This course studies the research methods and processes applicable to engineering and technology. Emphasis will be placed on defining research problems, collecting, analyzing, recording, and interpreting data. Students will be required to conduct a research project. Prerequisite(s): Graduate Standing

ETCS 620 Project Management for Technology Credits 3(3, 0)
This is the introductory project management course, which is a core course in the Master's degree programs. Prerequisite(s): Graduate Standing

ETCS 678 Mobile Wireless Networking and Security Credits 3(3, 0)
This course is a comprehensive examination of wireless local area networks, with an emphasis on the IEEE P802.11 family of WLAN standards. Prerequisite(s): Graduate Status or Permission of Instructor

ETCS 680 Networking Technology for Industry Credits 3(3, 0)
An advanced study of network technology fundamentals. The course stresses the state of the art developments that support the World Wide Web and a wide array of specific applications. Prerequisite(s): Graduate Standing

ETCS 681 System Integrity for Cybersecurity Credits 3(3, 0)
This course identifies elements of system integrity for cybersecurity including firewall design, types of security threats and responses to security attacks. This course also studies the use best practices design, implement, and monitor a network security plan. This course also examines security incident postmortem reporting and ongoing network security activities. Prerequisite(s): Graduate Status or Permission of Instructor

ETCS 682 Cybersecurity Administration Credits 3(3, 0)
This course explores the concepts of governance and how it applies to information systems. Discussion includes the importance of compliance with laws, regulations, policies, and procedures

as a means of minimizing risk through mandated security and control measures. Through this course, students also gain an understanding of Cybersecurity Auditing processes and principles. Prerequisite(s): Graduate Standing

ETCS 683 Network Intrusion, Detection and Incidence Response Credits 3(3, 0)
This course presents an exploration of the theory and implementation of intrusion detection and intrusion prevention. Prerequisite(s): ETCS 685 or Permission of Instructor

ETCS 685 Fundamentals of Network Security Credits 3(3, 0)
This course presents topics include cryptography, cipher systems, practical security schemes, confidentiality, authentication, integrity, access control, nonrepudiation, and their integration across telecommunications (i.e., computer) networks Prerequisite(s): Graduate Status or Permission of Instructor

ETCS 686 Advance Network Security Credits 3(3, 0)
This course covers advance information from topics presented in ETCS 685. Topics include cryptography, cipher systems, practical security schemes, confidentiality, authentication, integrity, access control, nonrepudiation, and their integration across telecommunications (i.e., computer) networks. Prerequisite(s): ETCS 685 or Permission of Instructor

ETCS 687 Legal and Ethical Issues in Cybersecurity Credits 3(3, 0)
This course focuses on the ways that law, ethics and cybersecurity overlap and intersect. Besides laws related to cybersecurity, the course examines laws related to intellectual property, civil litigation, criminal prosecutions, and privacy. Prerequisite(s): Graduate Standing

ETCS 690 Master's Seminar Credits 1(1, 0)
This course serves a dual role. First and foremost, this is a graduate seminar course with the major objective of preparing students for research in practical applications. It will challenge students with a critical and philosophical exploration of the ideas of cybersecurity, and will consist of lectures, readings and class discussions in which every student is expected be an active participant. Since students come to this course with diverse interests in graduate work in cybersecurity, the scope of readings and discussions on research and practical applications will be broad. The second role of this course is a capstone graduation requirement for all Masters' students. For that purpose, the goal is to learn the practical skills of giving a presentation and writing a research paper. Prerequisite(s): Permission of Instructor

Educational Objectives
The educational objective of the proposed Cybersecurity Engineering Technology master's degree are as follows:

1. To prepare graduates with the technical knowledge and skills needed protect and defend computer systems and networks by ensuring availability, integrity, authentication, confidentiality of digital information;
2. To develop graduates who can plan, implement, upgrade, and monitor cybersecurity measures for the protection of computing infrastructure; and
3. To develop graduates who are able to analyze and address computer security breaches.

Student Learning Outcomes
Upon completion of the graduate program students will be able to:

- Evaluate cybersecurity needs of an organization.

- Assess cybersecurity risk management policies.
- Measure the performance of cybersecurity systems.
- Troubleshoot, maintain, and update cybersecurity systems.
- Implement real-time cybersecurity solutions.
- Design short- and long-term Cybersecurity strategies and policies.

Specialized Accreditation

The proposed Master of Science in Cybersecurity Engineering Technology is designed to be accredited by the Association of Technology, Management, and Applied Engineering (ATMAE), which UMES is planning to pursue during the 2020/2021 academic year. A Master's degree in Cybersecurity Engineering Technology that can be formally accredited by ATMAE stands to serve as a regional role model for producing high-quality leaders for professional services and industries in cybersecurity and related fields. ATMAE accredits graduate programs/options that prepare individuals for career advancement that involve the management of complex technological systems. For ATMAE to consider accrediting a Master's Degree: programs/options, the graduate program shall be a minimum of 30 semester hours and shall meet the following minimum/maximum foundation semester hour requirements: Communications and/or Problem Solving, 6-12 credits; Research, 6-12 credits; Management and/or Technical, 12-18 credits, Electives, 0-6 credits and students must successfully complete a minimum of 10 semester hours of graduate level coursework at the institution seeking accreditation. Additional details about the ATMAE accreditation process can be found at following URL: http://www.atmae.org/.

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

The degree in Cybersecurity Engineering Technology will expand the educational opportunities of minority students in the State of Maryland. Our mission is to provide opportunity to students from under-served populations and to first generation college students. The branding associated with the Cybersecurity Engineering Technology major combined with planned ATMAE accreditation will provide positive entry credentials for our graduates. Our graduates are expected to provide leadership in minority information security firm development that will benefit the State in the near and long terms. The expansion of STEM education in Cybersecurity Engineering Technology is supported by the USM Strategic Plan 2020 under Theme I: College Completion, and Theme 3: Academic Transformation.

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

There are a tremendous number of unfilled cybersecurity positions within the federal government and cybersecurity is expected to continue to be a vital area of need for most government agencies and federally funded research and development centers (FFRDC). Due to the shortage of cybersecurity professionals, there are excellent opportunities for job placement for graduates of the proposed graduate degree program. To support the proposed graduate program, due to its location, UMES is uniquely positioned to develop a strong working relationship with:

- National Security Agency (NSA)
- Central Intelligence Agency (CIA)
- Department of the Navy: the Space and Naval Warfare Systems Command (SPAWAR)
- Department of Homeland Security (DHS)
- Federal Emergency Management (FEMA) Institute
- Johns Hopkins University's Applied Physics Lab

- United States Army Intelligence and Security Command (INSCOM)

Institutions of higher education have also expressed a need for cybersecurity staff members. And, the national shortage of technical cybersecurity staff continues to grow at the same rate as the shortage of competent cybersecurity professionals in federal agencies.

The table below, from the U.S. Bureau of Labor Statistics, provides a summary of employment demands nation-wide. All the occupations below (with the exception of computer programmers) are expected to have exceptional job opportunities through 2020.

Employment Projections for U.S. Cybersecurity/Computer Science Professionals

Occupation	Current 2010 employment		Projected 2020 employment		Change, 2010-2020	
	Number	Percent of Industry	Number	Percent of Industry	Number	Percent
Computer software engineers, applications	174000	12.1	273900	13.0	99900	57.4
Computer systems analysts	135400	9.4	193500	9.2	58300	43.1
Computer programmers	116800	8.1	150400	7.1	33600	28.8
Computer software engineers, systems software	117800	8.2	202200	9.6	84500	71.1
Computer and information systems managers	52200	3.6	74700	3.5	22500	43.1
Computer support specialists	107400	7.5	152700	7.3	46300	43.1
Computer and Information Scientist, Research	6500	.5	9300	.4	2800	43.1

United States Bureau of Labor Statistics:
http://data.bls.gov/oep/servlet/oep.nioem.servlet.ActionServlet
Note: Percentage change (last column in the table above) is calculated by dividing the projected change in employment (2010 to 2020) by the 2010 employment number. Example: 99,900/174,000 = 57.4%. The percent distribution columns are not intended to add to 100%.

We believe that UMES is uniquely positioned to contribute to that number from our targeted student body.

E. Reasonableness of program duplication:

The University of Maryland Eastern Shore is the only university in the entire USM system that offers a degree in Engineering Technology. Due to this fact, there is no duplication of programs by adding an additional program in Cybersecurity Engineering Technology to the Department of Technology curriculum offerings.

F. Relevance to Historically Black Institutions (HBIs)

UMES has historically served students who are either first generation college students and/or come from socially and economically disadvantaged backgrounds. The proposed program will serve those students and others who wish to pursue the many career opportunities made possible by obtaining a graduate degree in Cybersecurity Engineering Technology. This program compliments the existing STEM graduate programs at UMES in engineering, technology and applied computer science by attracting a diverse population of students who have an interest in pursuing a career path related to cybersecurity. The mission of UMES and the Department of Technology is to provide

opportunities to individuals who may come from socially and economically disadvantaged background and/or maybe first generation college students, who might not otherwise have a chance to earn an advanced college degree in Engineering Technology. The addition of the Cybersecurity Engineering Technology in the department only enhances that mission.

In terms of the presence of women and minorities who have formal training and education in the field of cybersecurity, the website of the National Initiative for Cybersecurity Careers and Studies (NICCS) states the following information about the need for women and minorities to be trained and educated in the field of Cybersecurity. "Similar to the scarcity of women in Information Technology (IT) and cybersecurity, minorities are also underrepresented in this field. IT and cybersecurity continue to have a need for professionals with technical skills which can be taught inside and outside the classroom. According to the National Science Foundation (NSF), minorities make up a ----mere 29% of the Science and Engineering workforce. The Information Technology Association of America (ITAA) report also found that Hispanics made up 12.9% of the U.S. workforce, but were only 6.4% of the information technology workforce. African Americans, constituting 10.7% of the U.S. workforce in 2004, only constituted 8.3% of the IT workforce. A more concerted effort on STEM education for minority students could open up a whole new set of opportunities for their careers."

Currently, no HBI offers a graduate degree in Cybersecurity Engineering Technology. Hence due to the historical mission of UMES, approval of the proposed graduate program will allow the university to positively impact the above mentioned statistics in a favorable way by producing more women and minorities with training and education in this important field.

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

I. Curriculum and Instruction

A. A distance education program shall be established and overseen by qualified faculty.

The University of Maryland Eastern Shore (UMES) is submitting a proposal for a Master of Science in Cybersecurity Engineering Technology. The proposed program will be offered both online and in a traditional face-to-face format. The current faculty in the department will also serve as the majority of the instructors in the new program. Any new instructors recruited to teach online would be required to meet the same qualifications as the full-time faculty. All faculty teaching in the online program will be required to complete UMES Online Learning Training and Quality Matters training.

B. The program's curriculum is coherent, cohesive, and comparable in academic rigor to programs offered in traditional instructional formats.

The same curriculum of courses that is taught in the traditional face-to-face format is taught in the online delivery format. The courses must have the same approvals to be offered to students, which includes internal curriculum committee approvals and external accreditation standards. An established online course development process is followed to include the direction and expertise of instructional designers, instructional technologists, and subject matter experts in the development of instruction for delivery at a distance. The online courses must successfully complete a Quality Matters review. UMES is a certified Quality Matters site. Quality Matters research-based set of eight standards for quality online

course design to ensure the academic rigor of the online course is comparable or better to the traditionally offered course (Quality Matters, 2014).

C. The program shall result in learning outcomes appropriate to the rigor and breadth of the program.

The measurable learning goals of each course are identified within the course syllabus.

D. The program shall provide for appropriate real-time or delayed interaction between faculty and students.

The curriculum will be delivered with Blackboard learning management system. This platform supports asynchronous interaction between faculty and students. "Real-time" interaction is available with the incorporated web-conference tool, supported by Blackboard Collaborate.

E. Faculty members in appropriate disciplines, in collaboration with other institutional personnel, shall participate in the design of courses offered through a distance education program.

All the faculty are selected based on discipline expertise, professional experience and completion of an online course development training course. The training course is a two-part session with an instructional designer that focuses on proper implementation of Blackboard and effective online pedagogy.

II. Role and Mission

A. A distance education program shall be consistent with the institution's mission.

Refer to Section A.1 in the main body of the proposal.

B. Review and approval processes shall ensure the appropriateness of the technology being used to meet a program's objectives.

The courses in the program are designed with the support of an instructional designer working in conjunction with the faculty. The instructional designer assists the faculty in identifying and recommending the most effective technologies for accomplishing the learning objectives.

The course development period first identifies all the learning components of the course, and how the course will be facilitated to achieve the optimal learning outcome. This is an iterative process that goes through several levels of review prior to the course actually being developed. Once the courses launch, the design team continually monitors the courses, and consults with the instructors to make adjustments to the course, if needed. All new online courses participate in end-of-term course evaluation process as designated by the Online Learning Policy and Procedures Committee.

III. Faculty Support

A. An institution shall provide for training for faculty who teach with the use of technology in a distance education format, including training in the learning management system and the pedagogy of distance education.

Faculty members in the proposed online program are supported by UMES' Center for Instructional Technology (CIT), as well as by the department chairperson. The CIT provides oversight for all online course developments, including faculty training and development. The CIT has a formal, structured faculty development approach for preparing faculty to develop and teach an online course. All faculty members are required to complete the training for online course development and instr

B. Principles of best practice for teaching in a distance education format shall be developed and maintained by the faculty.

Principles of best practice for teaching in a distance education format will be developed and maintained by requiring distance education faculty to attend on-line seminars and face-to-face workshops to enhance and maintain their knowledge of on-line teaching pedagogy. Faculty will be required to attend at least one such seminar and/or workshop every academic year.

C. An institution shall provide faculty support services specifically related to teaching through a distance education format.

Faculty members have access to a dedicated faculty computer lab, instructional designers, and information technology specialists. A help desk line is available via email and telephone for technical support issues. The CIT offers online and in-person workshops that are designed for faculty that implement Blackboard and other technologies in the classroom.

D. An institution shall ensure that appropriate learning resources are available to students including appropriate and adequate library services and resources.

The Frederick Douglass Library houses a multiplicity of print and non-print resources to support the mission and academic programs of the university; the collection includes over 211,000 volumes. As a member of University System of Maryland and Affiliated Institutions (USMAI) consortium, the library is affiliated with the University's thirteen campuses and seventeen libraries for the purpose of sharing library resources. The integrated, comprehensive library system, ALEPH makes it possible for our patrons to have 24/7 access to USMAI library collections and electronic resources. These collections and resources include the library catalog and over 120 research databases often including full text journals, books and newspapers.

The Library provides sessions to enhance students' research skills. Library instruction sessions are tailored to the needs of the class to assist students and may range from an overview of basic library resources to the use of advanced or subject research materials and techniques. The library also offers a one-credit online Information Literacy course taught by the Reference Department Faculty.

IV. Students and Student Services

A. A distance education program shall provide students with clear, complete, and timely information on the curriculum, course and degree requirements, nature of faculty/student interaction, assumptions about technology competence and skills, technical equipment requirements, learning management system, availability of academic support services and financial aid resources, and costs and payment policies.

UMES maintains numerous web-based resources to inform prospective students on the information they may need as an online student. These resources include the main website (http://www.umes.edu) and the online catalog, which includes detailed programmatic information, academic support services, financial aid, costs, policies, etc. and specific information for online learning. As new online students are admitted and enrolled, they receive timely emails with important information to help them prepare to become an online student. These emails include information on how to access Blackboard and university email, technical requirements, available academic support services and the online student orientation course available within Blackboard.

B. Enrolled students shall have reasonable and adequate access to the range of student services to support their distance education activities.

Academic Advising. Students are assigned an advisor when accepted. Students work individually with the advisor to develop a course of study that meets the requirements of the program and the career goals of the student. The advisor contacts all the students each semester to check on progress and answer questions. Courses that deviate from the program plan and have not been approved by an advisor may not count toward degree requirements.

Library Services. Students have online access to the Frederick Douglass Library. The Interlibrary Loan Department allows students access to resources at any other university in the nation. The library also provides easy access to a wide selection of electronic information resources. Librarians are available to assist students remotely and the library maintains an extensive website to take visitors through all its services and materials.

Services with Students with Disabilities. The Disability Services Administrator of the campus works with students requiring accommodations to ensure all of those needs are met.

Transcript Access. Official transcripts are available upon written request of the student.

Student ID Card. The identification card serves as the student's university identification. The card acts as the university library card and provides access to student software discounts where available.

C. Accepted students shall have the background, knowledge, and technical skills needed to undertake a distance education program.

All accepted online students must meet the admissions requirements of the program. New online students are offered an orientation course within Blackboard prior to beginning their first online course. This course covers a broad range of topics on how to be a successful

online student such as: Blackboard basics, online student learning expectations, how to access the library, how to conduct online research, and how to participate in online discussions.

D. Advertising, recruiting, and admissions materials shall clearly and accurately represent the program and the services available.

All relevant program information is keep up-to-date on the UMES website (http://www.umes.edu).

V. Commitment to Support

A. Policies for faculty evaluation shall include appropriate consideration of teaching and scholarly activities related to distance education programs.

Faculty teaching online courses are encouraged to participate in the professional development opportunities provided each semester by the CIT.

B. An institution shall demonstrate a commitment to ongoing support, both financial and technical, and to continuation of a program for a period sufficient to enable students to complete a degree or certificate.

UMES' commitment to online teaching is demonstrated by the resources of its Center for Instructional Technology that provides a faculty computer lab, course development, instructional, and technical support to new and current faculty.

VI. Evaluation and Assessment

A. An institution shall evaluate a distance education program's educational effectiveness, including assessments of student learning outcomes, student retention, student and faculty satisfaction, and cost-effectiveness.

Refer to Section L in the main body in the proposal.

B. An institution shall demonstrate an evidence-based approach to best online teaching practices.

The staff of the CIT continually participates in professional development activities to keep abreast of evidence-based approaches to online teaching practices. These online teaching practices are then incorporated into future workshops and one-on-one trainings.

C. An institution shall provide for assessment and documentation of student achievement of learning outcomes in a distance education program.

As part of the online course design process, course assessments are required to be aligned with stated course learning outcomes.

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

There are currently two full-time faculty members who are qualified to teach cybersecurity related courses:

Dr. Derrek Dunn is currently a tenured Full Professor and Chairperson of the Department of Technology in the School of Business and Technology at University of Maryland at Eastern Shore (UMES). Dr. Dunn has taught college level courses in such areas as Wireless Communication Systems, Computer Networks, Telecommunication Management, Global Positioning Systems and Optical Systems. Dr. Dunn received his Bachelor of Science in Electrical Engineering and a Bachelor of Science in Mathematics from North Carolina A&T State University. He received a Master of Science in Electrical Engineering and Master of Science in Mathematics from Virginia Polytechnic Institute and State University; and a Master of Construction Management from Western Carolina University. Dr. Dunn earned his Doctor of Philosophy in Electrical Engineering from Virginia Polytechnic Institute and State University. He brings nearly 15 years of experience in teaching and research on learners and learning at a distance and experience in the use of distance education in technology and engineering.

Dr. Kenny Fotouhi is a Professor in the Electrical Engineering Technology program. He has a Ph.D. in Electrical Engineering from the University of Missouri. Dr. Fotouhi has been actively involved in a joint research project at the University of Maryland College Park developing new semi conductor materials. Dr. Fotouhi teaches courses in circuit analysis, advanced computer networks, logic and switching and circuit design.

As the degree program grows in student enrollment, additional full-time faculty will be added to support the degree program. In the interim the use of adjunct faculty will supplement the current full-time faculty members.

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

The University assures that institutional library resources meet the new program needs. The Frederick Douglas Library currently houses over 211,000 volumes. Students and faculty can take advantage of the entire University of Maryland System's library holdings through inter-library loans. Electronic databases are available through the university itself, and also through the University of Maryland System. The University continually updates and adds to its information security holdings in the library as needed for existing programs. It is expected that library resources will continue to meet all needs of existing and future programs.

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

The University assures that institutional facilities and equipment meet the new program needs. The Department of Technology is housed in the Briggs and Thomas Art and Technologies Center on the UMES campus. Built during the summer of 1984, the 50,000 square foot Briggs and Thomas Arts and Technologies Center was constructed with an allocation of over $5 million from the State of Maryland. Currently over 25,000 square feet of the building plus a 1.5 acre outdoor construction laboratory is dedicated exclusively to the Department of Technology. Hence, this facility will also be made available to the proposed Cybersecurity Engineering Technology program.

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

Current departmental resources are adequate to support the proposal for the Cybersecurity Engineering Technology program. No new full-time faculty will be needed for the first two years of

the program. The university has allocated funding for Adjunct faculty for the startup of the program. An additional full-time faculty may be required to assist with teaching the proposed program's courses during the third and subsequent years, depending on enrollment numbers. Expenditures related to faculty resources are listed under the category of Total Faculty Expenses. Under the category of administrative staff expenses, the department has requested funding for an Administrative Support Associate to work with the distance learning students in the program to help them navigate the various UMES processes such as adding, dropping and withdrawing from courses and the submission of graduation applications. Also the Administrative Support Associate will be charged with maintaining students' records and assisting the faculty with advisement to ensure on-time graduation of the Master's students. The Administrative Support Associate will provide ongoing support and program guidance for distance learning students. In this capacity, the Administrative Support Associate is expected to represent the students in solving complex issues and needs and coordinate solutions or remedies with academic and administrative units as needed. Lastly, since the proposed program will be offered with a distance learning option, no additional facilities are required.

Based on the projected student enrollments in the proposed graduate program, resources generated by the program exceed expenditures over the initial five-years of the program's operation. In addition to the resources generated by the program from tuition dollars, the Department of Technology plans to submit a grant proposal to the Title III Office at UMES for supplemental support of the proposed program. Also, the department will submit applications to fellowship and grant programs from the National Security Agency, Department of Defense, and other federal agencies to supplement the tuition dollars generated by the Cybersecurity Engineering Technology program.

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

Based on established department standards, we have established an ongoing program evaluation where we,

- Assess samples of student performance on computer based problems and projects.
- Assess samples of the use of technology in student presentations.
- Assess samples of group and individual case analyses.
- Assess student design projects.
- Assess written and oral student presentations, written assignments and research projects.
- Track analytical performance in the seminar course.
- Evaluate student performance in exams, quizzes and assignments in required core courses.
- Assess comprehensive final exams in advanced elective courses.

The intent of accessing the above mentioned components is to ensure the proposed program is meeting the learning outcomes required by Association of Technology, Management, and Applied Engineering (ATMAE) for a Cybersecurity Engineering Technology program under the requirements for Master's program.

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

As stated above, a Master of Science in Cybersecurity Engineering Technology will expand the UMES mission and institutional identity. The program will expand educational opportunities and choices for underrepresented minorities and other citizens of the State of Maryland by offering a

unique degree program in a field where there is a shortage of minority and women in the workforce.

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

The Engineering Technology programs offered by the Department of Technology at UMES are not considered low productivity programs by the Commission.

TABLE 1: RESOURCES

Resources Categories	(Year 1)	(Year 2)	(Year 3)	(Year 4)	(Year 5)
1. Reallocated Funds[1]	**$0**	**$0**	**$0**	**$0**	**$0**
2. Tuition/Fee Revenue[2]	99,760	117,820	172,000	172,000	190,060
(c+g below)					
a. #F.T Students	**10**	**10**	**10**	**10**	**10**
b. Annual Tuition/Fee					
Rate/unit	**301**	**301**	**301**	**301**	**301**
Number units	**9**	**9**	**9**	**9**	**9**
Subtotal Tuition	2,709	2,709	2,709	2,709	2,709
Fees	**43**	**43**	**43**	**43**	**43**
Total Tuition/Fees	2,752	2,752	2,752	2,752	2,752
c. Annual Full Time Revenue	27,520	27,520	27,520	27,520	27,520
(a x b)					
d. # Part Time Students	**20**	**25**	**40**	**40**	**45**
e. Credit Hour Rate	**301**	**301**	**301**	**301**	**301**
f. Annual Credit Hours	12	12	12	12	12
g. Total Part Time Revenue	72,240	90,300	144,480	144,480	162,540
(d x e x f)					
3. Grants, Contracts, & Other					
External Sources[3]					
4. Other Sources					
TOTAL (Add 1 - 4)	$99,760	$117,820	$172,000	$172,000	$190,060

TABLE 2: EXPENDITURES

Fill in blue shaded areas only.

Expenditure Categories	(Year 1)	(Year 2)	(Year 3)	(Year 4)	(Year 5)
1. Total Faculty Expenses	$27,930	$27,930	$93,100	$93,100	$93,100
(b + c below)					
a. #FTE	**0.3**	**0.3**	**1.0**	**1.0**	**1.0**
b. Total Salary	**21,000**	**21,000**	**70,000**	**70,000**	**70,000**
c. Total Benefits	6,930	6,930	23,100	23,100	23,100
2. Total Administrative Staff Expenses	66,500	66,500	66,500	66,500	66,500
(b + c below)					
a. #FTE	**1.0**	**1.0**	**1.0**	**1.0**	**1.0**
b. Total Salary	**50,000**	**50,000**	**50,000**	**50,000**	**50,000**
c. Total Benefits	16,500	16,500	16,500	16,500	16,500
3. Total Support Staff Expenses	0	0	0	0	0
(b + c below)					
a. #FTE					
b. Total Salary					
c. Total Benefits	0	0	0	0	0
4. Equipment					
5. Library					
6. New or Renovated Space					
7. Other Expenses					
TOTAL (1-7)	$94,430	$94,430	$159,600	$159,600	$159,600