BOARD OF REGENTS

EASTERN MICHIGAN UNIVERSITY

RECOMMENDATION

NEW ACADEMIC PROGRAM: CYBER SECURITY, MASTER OF SCIENCE

ACTION REQUESTED

It is recommended that the Board of Regents approve a New Academic Program: Cyber Security (Master of Science).

STAFF SUMMARY

The *Master of Science in Cyber Security* program aims to establish a quality and sustainable graduate program in cyber security to produce the much needed post-graduate level professionals for the public and private sectors to better protect local, regional, and national security.

PROPOSAL ELEMENTS

Rationale Cyber security is a fast-growing field, and there is a high demand for skilled individuals in this area. The Enterprise Strategy Group reported that 46% of organizations in 2016 stated that they have a "problematic shortage" of cyber security skills.

America's economic prosperity in the 21st century will depend on cyber security. According to the 2015 Michigan Cyber Initiative Report, "The State of Michigan blocks more than 650,000 cyber-attacks daily. Annually, the state blocks: 2.5 million web Browser attacks, 179.5 million http-based attacks, 79.5 million network scams, and 5.2 million intrusions."

The program will serve the needs of the State of Michigan and the nation by offering a high-quality master's program that produces cyber security professionals who can serve as computer and information assurance research scientists and leaders in the field. The Bureau of Labor Statistics reported that such a position requires a master's degree as an entry-level and provides a median salary of $118,840 as of 2016. This program not only will provide highly qualified cyber security experts but will also contribute significantly to the economic growth and security in Michigan and the nation.

Program	The proposed program will stand apart from similar programs offered by
Distinction	universities in the region because of the variety of course delivery options

Program Distinction   The proposed program will stand apart from similar programs offered by universities in the region because of the variety of course delivery options available to students in the program. All required courses will be offered online, in a hybrid mode, or face-to-face during weekdays on the main campus. All courses will be supported with a live stream for off-campus students to view simultaneously. The sessions will also be recorded and posted online for students who could not attend the live session. To serve a variety of populations, courses may be offered on weekends and/or in short semesters (i.e., 7.5 and 4 weeks sessions).

Curriculum Design   The program aims to offer a high-quality educational program for cyber security professionals and researchers. The core requirements provide the students with the knowledge and skills needed to successfully evaluate information security needs, identify appropriate countermeasures, and implement security technologies. The focus area courses enable the students to concentrate on specific areas of interest, such as Offensive and Defensive Security; Data Analytics for Cyber Security; Risk Management, Assessment, and Mitigation; Cyber Law, Privacy, Policy, and Compliance; and Cyber Security Project Management. The program will strive to seek a balance between the leadership, managerial and technical skills of cyber security. The proposed graduate program requires students to complete 30 credit hours. One new course was created for this program.

Projected Enrollment   The Department expects at least 20 students at initial enrollment and an average of 60 students within the first three years. With that anticipation, the average number of students per year will be around 15-20 once the program is established.

FISCAL IMPLICATIONS

The current Academic Affairs budget will absorb program costs.

ADMINISTRATIVE RECOMMENDATION

The proposed Board action has been reviewed and is recommended for Board approval.

11/15/2018
Date

University Executive Officer
Rhonda Longworth, Ph.D.

Cyber Security [M.S.]

New Program | effective date TBD

The effective date will be determined following consideration by the Academic Officers Committee, Michigan Association of State Universities and the Eastern Michigan University Board of Regents.

The **Master of Science in Cyber Security** program establishes well-informed and practically grounded graduates in cyber security to meet the needs of cyber security professionals in public and private sectors to contribute effectively in protecting local, regional, and national security. In addition, the program will equip cyber security professionals to serve as leaders and computer and information assurance research scientists. The program is designed to be flexible and meet the needs of research-oriented students and professionals by offering two tracks with thesis and project options. By completing the program requirements, students will be able to analyze complex cyber security problems and apply security principles of cyber security to identify solutions; analyze and evaluate systems with respect to maintaining operations in the presence of risks and threats; design, implement, and evaluate a computing-based solution to meet a given set of cyber security requirements; develop and implement cryptography for information systems; understand and implement advanced security to networks and software; recognize professional responsibilities and make informed judgments in cyber security practice based on legal and ethical principles; and be active in state-of-the-art research activities and scholarly funded research activities.

Program Admission

Applicants must:

- Meet the Graduate School <u>admission requirements</u>
- Have at least 24 hours of Information Assurance and Cyber Security courses, including and not limited to networking, digital and network forensics, incident response, operating system security, database management and security, malware analysis, and reverse engineering, defensive and/or offensive security, and policy development and legal issues in information systems. Students must have a minimum GPA of 3. 0 in information system coursework.
- Preference is given to applicants with an undergraduate degree in information system and cyber security or closely related area.
- Students with non-U.S. post-secondary credentials must submit an evaluation of their international transcripts from one of four approved evaluation services for a detailed, course-by-course report.

International Applicants

Official English Language skills test-IBT, IELTS, MELAB, Pearson's Test of English (PTE) are required for all international applicants whose native language is not English. The minimum scores required are as follows:

<u>Test</u>	<u>Overall Score</u>	<u>Writing Score</u>
IBT	79	19
IELTS	6.5	5.5
CGT	213	5.0
MELAB	83	No minimum

For international graduate student additional admission requirements, please visit Internationa1 Admissions.

Conditional Admission

The admission shall be conditional following the rules and regulations of the Eastern Michigan University Graduate School. In addition, admission shall be conditional if the students did not have the required background coursework for full admission and will be required to take IA 601, and earn a minimum grade of "C-," to be fully admitted. In some cases, however, the courses work may be replaced by a credential placement test for students who have extensive work experiences in the area of cyber security. For those students who are not academically ready, the advisor will decide on the required courses that shall be completed before full admission is granted.

School Information

Information Security and Applied Computing, *College of Technology*

Suleiman Ashur, Ph.D. | Interim Director | 206 Roosevelt Hall | 734.487.2490 | sashur@emich.edu

Advisor Information

Please contact the department for advisor information

Degree Requirements: 30 hours

Core Courses: 18 hours

- IA 544 - Cyber Law, Privacy, Policy and Compliance 3 hrs
- IA 622 - Risk Management and Incident Response 3 hrs
- IA 642 - Defensive Security 3 hrs
- IA 645 - Data Analytics for Cybersecurity 3 hrs
- IA 651 - Cyber Security Project Management 3 hrs
- IA 650 - Offensive Security 3 hrs

Restricted Electives: 6 hours

Choose six hours from the following
- IA 533 - Cybercrime & Information Warfare 3 hrs
- IA 558 - Advanced Digital Forensics 3 hrs
- IA 643 - Disaster Recovery - Business Continuity 3 hrs

Students can apply an independent study, special topic, or any graduate seminar course offered by the School of Information Security and Applied Computing, or any graduate-level course, with the approval of their advisor. *Independent Studies are limited to three credit hours.*

Capstone: 6 hours

Choose one of the following capstone options

Option I - Thesis
- IA 690 - Thesis 1 hr
- IA 691 - Thesis 2 hrs
- IA 692 - Thesis 3 hrs

Option II - Project

- IA 694 - Project Design and Implementations 3 hrs
- An additional elective course 3 hrs