PROGRAM REVIEW REPORT SUMMARY

1. **Reporting Institution**: Eastern Illinois University
2. **Program Reviewed**: MS Degree in Cybersecurity
3. **Date:** November 3, 2020
4. **Contact Person**: Rigoberto Chinchilla
    - **4.1.** **Telephone:** 217 581 8534
    - **4.2.** **E-mail**: rchinchilla@eiu.edu

5. Summary of Program Goals and Objectives and Progress at Meeting Them

I. Overview

In response to a call from the Illinois Board of Higher Education (IBHE), the EIU School of Technology developed in 2005 a post-baccalaureate certificate in Technology Security. Eastern Illinois University was the only state institution in Illinois to respond to the call from IBHE, and received the Caterpillar Homeland Security Fund, which grants scholarships annually to students pursuing studies in Technology Security. Since the certificate's inception several other security-related courses have been developed within both the School of Technology and School of Business at EIU. By building upon this strong foundation, the EIU School of Technology and School of Business have collaborated in developing the M.S. in Cybersecurity with the modification of existing classes for online or hybrid delivery and the creation of three new courses in order to complement the cyber education of our students.

Consistent with the mission of the University, the M.S. in Cybersecurity employs a part-time, cohort program model for working professionals with a computer/information technology or related undergraduate degree. A full time on and off-campus program is also available for domestic and international students. The program started in the Fall, 2017. The two-year program completion requirement (inclusive of two summers) has had a two day residential component upon completion of the second semester, and a four day residential component at the conclusion of the fourth semester for both laboratory experiences and a 4-day residential capstone experience immediately following those laboratory sessions. The program has had an average of 25 students per year (2018-2019-2020).

Students are prepared to become leaders and technical managers in cybersecurity, which requires solid understanding of security technology and organizational management principles and practices in order for graduates to make sensible and responsible decisions. Typical positions our graduate students are working now include:

Cybersecurity Consultants
Network Security Specialists
Information Assurance Specialists
Computer Security System Analysts
Web Security Engineers
Information Security Officers
Information Security Operations Managers
Cybersecurity Administrators
Identity Management Analysts
IT Security Managers

In addition to addressing four main objectives of the EIU Graduate School by the Council of graduate Studies (CGS): 1) Depth of content knowledge, 2) Critical thinking and problem solving skills, 3) Effective oral and written communication skills, and 4) Evidence of advanced scholarship through research and/or creative activity, the M.S. in Cybersecurity has six main program objectives to prepare students for these positions/careers. At the conclusion of the program, graduates will be able to:

1) Assess, by analyzing technical and operational requirements, and enterprise level information cybersecurity system.
2) Construct the architecture of a typical cybersecurity system; identify significant vulnerabilities, risks, and points at which specific security technologies/methods should be employed.
3) Conduct network penetration tests, troubleshoot, and implement attack countermeasures in a typical information system.
4) Identify the components of cybersecurity layered structure for:
    a. Network defense architecture
    b. Access control and auditing
    c. Continuous network monitoring
    d. Real-time security solutions
5) Describe and apply the fundamental and advanced technologies, components, and issues related to communications, data networks, and information systems.
6) Analyze network designs, topologies, architectures, protocols, communications, administration, operations, and resource management, for wired and wireless networks that affect security of the cyberspace.

The graduate program in Cybersecurity steadily serves around 25 students per year on average. One of the major strengths of our program is the diversity of our student body including gender and nationality; about 35% of our students are women, international students, and minorities. Our program's flexibility allows students to take either an online modality or a face-to-face modality, part or full time, or on campus or off-campus.

By the end of Spring 2020, seventeen students have graduated from the program and all of them are employed in cybersecurity-related areas at this time, the demand for professionals in this area certainly give us the confidence of the need for this program.

II. Program Modifications/Improvements

The major changes in the M.S. in Cybersecurity have been related with changes in cybersecurity technologies through the last three years. Our courses must be constantly evolving to reflect those changes. Also, we have developed a few dozens of new laboratory practices to accommodate to those changes and challenges in cybersecurity. The MS. n Cybersecurity collaborates with the MS in Technology program, providing several cybersecurity courses not only to MS. In Cybersecurity students but also to MS in Technology students. The cybersecurity field is now core content offered by the School of Technology courses.

Originally, we planned our students to spend many days in our facilities (for example, a week after the first year and two weeks at the end of the program). Fortunately due to the advances in Cloud

Computing and remote learning, we were able to reduce the residency of the first year just to a two-full days and the final residency to 4 days of intensive laboratory practices and practical projects. Another notable change is the incorporation of a new area within the field, which is Cybersecurity forensics. Beginning Spring 2021, cybersecurity forensics will be incorporated as a core in our program. Studies in this area will significantly enhance program offering in the field. These two upgrades are described in more detail below.

We discovered after the first semester that our prospective students demanded a more flexible program. We started just with an online modality off-campus. But very quickly, it was clear that many needed a full time on-campus modality (mainly international students**)** and the possibility to take combination of courses on campus and off campus for domestic students. We quickly responded to that demand by adapting our course rotations to meet the demand. Also, we discovered that our program needed more flexibility in the courses offered, therefore we gave students different options according to their particular interest. As an example, some students wanted to focus on Wed Development and Programming/Coding Security, and we used the current courses of the MS in Technology to offer this flexibility. The major recommendations for the program are within the following four areas:

- Cloud Cybersecurity Based Systems
- Cybersecurity Forensics
- Cybersecurity Compliance According to ISO Standards
- Improvement of Laboratory Facilities

We believe the program is lacking behind in these four areas and we are looking ways to incorporate these areas within our existing courses or to create new courses to improve our program.

Although this is the first review/evaluation of the program we have taken specific actions in two of the above four areas. The first one was to incorporate a specialist in computer forensics to our faculty. This specialist has decades of experience in this field, who will teach the Cyber-forensics course for the first time in Spring 2021.

The second action taken was to design a cloud-based laboratory for the program. Using VMWARE, cloud computing and virtual images of the equipment in our laboratory, we are migrating to a cloud-based laboratory that will begins its operations in Spring 2021 (partially) and in Summer 2021 (fully implemented).

Regarding the Cloud Base Cybersecurity Based Systems as well Cybersecurity Compliance, we still need to prepare a faculty or hire a new one that can cover these areas of expertise, which is a potential plan for year 2022.

EIU School of Technology is constantly seeking improvement even with limited resources. The very creation of this program, the support given by the institution and the excellent response of the faculty teaching and supporting the program have made the MS in Cybersecurity already a stable program within our institution. Particularly the creation of a cloud-based laboratory has been outstanding it will give us flexibility in designing and changing our practices as per changes in technology and the market.

To implement this cloud-base laboratory several units within the Institution were involved, the Information Technology Services, The Management of Information System program in the School of Business, and the School of technology as a whole and the EIU administration with their support. Although the improvements and challenges are never ending in this field, the institution has responded with flexibility and resources to keep with the challenges of the field. The cloud-base laboratory and the development of the Cybersecurity Forensics area within the program have been the most noteworthy activities of the program.

6.1 Decision

__X___ Program in Good Standing

______ Program flagged for Priority Review

______ Program Enrollment Suspended

6.2 Explanation

Program enrollments exceed critical IBHE benchmarks and no concerns are noted. As a result, the program is recognized as in “good standing”. With respect to state need, the program responds to critical technical workforce needs in the area of cyber-security. Further, I note that the program has well defined student learning outcomes and is encouraged to marshal evidence of student learning when the next full support is submitted. With respect to program modification, the faculty and program describe tactical and strategic responses over the past few years that no doubt have enabled the program to be more efficient and more effectively train learners.

Jay Gatrell
Provost & VPAA