Interdisciplinarity@WMU- Phase One planning Template

1. **Brief Overview**: Provide a brief overview of the proposed interdisciplinary initiative. What types of questions would the initiative ask? What types of complex problems would it seek to solve?

   The interdisciplinary programs in Cybersecurity are well-established at the Graduate level and are growing at the Undergraduate level. The initial collaboration among the College of Engineering and Applied Sciences, Extended University Programs (now WMUx), and the Haworth College of Business demonstrates that interdisciplinary programs bring more to WMU and its students and are greater than the sum of their parts. Both CEAS and HCOB remain committed to supporting the Cybersecurity programs.

   To advance the Cybersecurity programs we must create a named Institute of Cybersecurity Studies. This will enable WMU to increase teaching, learning, and collaborative initiatives within the existing BS, MS, and Graduate Certificate by facilitating cooperation among additional departments and programs within the existing colleges within Cybersecurity. For example, Cybersecurity faculty might choose to work with ISM faculty to create a course on Cyber-Physical systems and how the supply chain has been impacted. The Institute would also enable faculty from other WMU colleges to develop and offer Cybersecurity courses that would not have been possible otherwise. For example, Criminal Justice Studies faculty could collaborate with Cybersecurity faculty to bring new courses in cybercrime to students.

   Collaboration would also occur in research. Cybersecurity impacts a multiple of disciplines: Education, Ethics, ISM, Law, Leadership, Philosophy, Sociology, and many additional possibilities. The newly formed Institute of Cybersecurity Studies would provide a fertile ground for collaborative interdisciplinary research and grant activities.

   The Institute would manage accreditation and certification initiatives that would benefit both existing and future students, attract faculty, and promote WMU and the Institute in Michigan and surrounding areas, and online internationally.

2. **Impacted units**: What existing units, programs, and colleges would be involved in the proposed initiative? What other possibilities for collaboration across campus or in the broader community might exist now or in the future?

   The initial colleges and departments--CEAS/CS and HCOB/BIS--that developed and now manage the Cybersecurity programs would be the primary facilitators. However, a major initiative of this transition to an Institute would be to bring in additional WMU colleges and departments. We readily see partnerships with Criminal Justice Studies, Economics, Education (especially K-12), and Philosophy, and are open to additional partnerships that could bring a more diverse perspectives to Cybersecurity studies. For example, there is a dearth of diversity in the

Cybersecurity field. The Institute would want to work with various faculty in departments such as African American and African Studies and Gender and Women's Studies to help develop classes and propose a multitude of research initiatives to address this diversity challenge.

3. **Impact on teaching, learning, and curricula**: Describe the anticipated impact of the proposed initiative on teaching, learning, and curricula. How might this initiative help to grow enrollment, including by reaching new audiences of learners through continuing education, dual enrollment, or professional certification? How will the proposed initiative positively impact the training of undergraduate and graduate students? How does it enhance our institutional commitment to diversity, equity, and inclusion?

   Currently the Cybersecurity Programs has plans to accomplish the following. Becoming an Institute would not only accommodate but also streamline these initiatives:

   • Working to get the MS and BS recognized as an NSA/DHS Center of Excellence.

   • Working to get ABET accreditation for the BS.

   • Collaborating with WMUx Professional Programs to offer local and online programs, workshops, and certifications. All of these classes use official materials from recognized professional certification organizations (CompTIA and EC-Council). We have been meeting with these organizations and have established ourselves as a CompTIA and EC-Council academic partner.

   • Classes for IT professionals wanting to work toward specific certifications such as CompTIA Security+ and EC-Council Certified Ethical Hacker.

   Further out, we have plans for the following:

   • Focused seminars to help businesses increase their overall Cybersecurity posture.

   • Summer Camps for local middle and high school students to help them learn about Cybersecurity and the career potential.

   • Summer Camps and/or Courses for K-12 teachers to help them learn how to teach Cybersecurity in the classroom. These would be both remote and local.

   • Remote and local offerings for the Air National Guard in Battle Creek, as well as other military initiatives.

4. **Impact on research and creative activity:** Describe the anticipated impact of the proposed initiative on research and creative activity. How will this initiative promote discovery and creative scholarship? How might it result in increased external funding?

   The Institute of Cybersecurity Studies would become a resource for faculty who want to collaborate on any aspect of cybersecurity. As our worldwide connectivity grows, technology impacts every aspect of our lives. Although we tend to think of cybersecurity's main goals of protecting our information, systems, integrated networks, and utilities, we also must realize that cybersecurity researchers study bias in Artificial Intelligence, Machine Learning, and Big

Data. For example, we might protect a large event with facial recognition software but must not fail to study implicit algorithm bias against gender and race.

Without faculty working together to research multiple aspects of cybersecurity such as overarching algorithmic bias, educating K-12 students and their teachers, protecting our local, state, and national governments, and a multitude of other aspects, we cannot create a truly secure, yet inclusive society.

The Institute of Cybersecurity Studies would be the catalyst through a variety of regular faculty and staff meetings, training sessions, colloquia, invited speakers, and grant initiatives to enable all disciplines to play a role in creating viable security initiatives.

5. **Efficiencies and/or cost savings**: How might the proposed initiative contribute to increased efficiencies and/or cost savings, for example by reducing administrative positions (e.g. chairs/directors), sharing staff support services and/or by sharing facilities?

   The Cybersecurity program currently includes two co-directors, Jason Johnson (CEAS/CS) and Alan Rea (HCoB/BIS) who have secondary appointments in each other's departments. The program currently has been assigned one WMUx staff member, Kristin Hrynczuk, for a few hours each week. In addition, each college has tasked marketing staff to work on current recruitment initiatives. Both colleges also help advise students.

   Most of the above allocations are outlined in a Memorandum of Understanding between CEAS and HCOB. There may need to be adjustments as WMUx shifts its focus to other university areas, but the collaboration among both colleges and WMUx has demonstrated we are able to allocate existing resources as needed. An Institute would most likely require more faculty and staff time, but new faculty and staff would not be needed in the initial phases until additional funding (external grants and gifts) is secured.

   Currently the entire Cybersecurity program takes place online. This may shift somewhat with the Institute over time, but not until additional funding is secured.

6. **Impact on course offerings and workload**: At present, proposed initiatives will only be feasible and sustainable if they can be supported by existing resources, including instructional capacity, faculty and staff time, and facilities. Will the proposed initiative streamline existing course or program offerings? Could the initiative help create more equitable and sustainable workload for faculty, for example, by reducing the need to offer under enrolled courses, reducing the frequency of course offerings or eliminating the need to teach some courses?

   The Cybersecurity program is currently offered online only using existing faculty and staff. This would continue for the Institute as well in its initial phases. Interdisciplinary faculty collaborations on teaching, curriculum development, grants, and other initiatives would take place virtually or in small meetings in a post-pandemic environment.

7. **Additional Information**: What additional information would you like to provide in support of this proposal?

   The Cybersecurity degrees and initiatives developed and managed by CEAS and HCOB are already interdisciplinary in nature. We have a successful MS program and a growing BS program. We maintain about 25 graduate students at any time and have started with 12 BS

students in our initial offering in Fall 2020 with an additional 15 committed to start in Summer/Fall 2021.

As an established and growing interdisciplinary program, we see the creation of a named Institute as the next step in increasing our program offerings beyond two colleges to include a variety of classes, minors, certificates, etc. We also see an Institute as the catalyst to grow faculty research and finding initiatives in this massive field that includes disciplines in sciences, engineering, business, humanities, and the arts. The Institute for Cybersecurity Studies would differentiate WMU from other colleges in Michigan and beyond.

8. Contact

Alan Rea, HCoB, Business Information Systems
Jason Johnson, CEAS, Computer Science