University of Detroit Mercy

PROPOSAL FOR CLAE CIS MINOR IN CYBERSECURITY

APPROVED 3/28/16: UNDERGRADUATE STANDARDS COMMITTEE
APPROVED 5/5/16: MCNICHOLS FACULTY ASSEMBLY
APPROVED 5/19/16: ACADEMIC LEADERSHIP TEAM

March 14, 2016
**Document History**

09/01/2014  CLAE Curriculum and Standards
10/27/2014  Review CLAE Curriculum and Standards
11/01/2014  Changes Submitted and Approved
01/28/2015  Submission to MFA
01/28/2016  Undergraduate Standards Committee Review
02/04/2016  Revisions sent to Undergraduate Standards Committee
02/11/2016  Presentation to Undergraduate Standards Committee
02/12/2016  Revisions sent to Undergraduate Standards Committee
03/14/2016  Revisions sent to Undergraduate Standards Committee
3/24/2016   Undergraduate Standards Committee Unanimously Voted to Approve.
3/28/2016   Forwarded to MFA

**Document Authors**

Dr. Gregory Laidlaw

Dr. Rita Barrios

Dr. Dan Shoemaker
Contents

Document History ........................................................................................................................... 1
Document Authors .......................................................................................................................... 1
A. Summary ..................................................................................................................................... 3
B. Description of the Minor ............................................................................................................. 4
  B1: Narrative description of the program ................................................................................... 4
  B2: List all courses in the curriculum ......................................................................................... 5
  B3: Indicate the delivery format of all new courses ................................................................... 5
  B4: Describe how the program demonstrates academic integrity ............................................. 6
  B5: Indicate unusual or unique characteristics of the proposed minor ..................................... 6
  B6: Indicate how any changes to the curriculum of the minor will be made ............................. 6
  B7: Describe how the proposed minor affects related departments or fields of concentration 6
C. Mission ....................................................................................................................................... 7
D. Objectives, Outcomes and Assessment ..................................................................................... 8
  D1: Indicate the program objectives and learning outcomes ..................................................... 8
  D2: Indicate how the learning outcomes and the objectives of the minor will be assessed ..... 9
Appendix A: Course Descriptions .............................................................................................. 11
Appendix B: Minor Tracking Form ............................................................................................ 12
A. Summary
The proposed Cybersecurity Minor in the department of Computer and Information Systems (CIS) leverages UDM’s designation as a NSA Center of Excellence in Information Assurance Education (CAE/IAE).

The primary advantage of the proposed minor is that, with no additional investment UDM will be able to provide access to one of the fastest growing 21st century areas of employment. Moreover, given that a Minor in Cybersecurity could provide a pathway for the Masters of Science in Information Assurance, this proposed Minor will strongly complement recruitment for that program.

The Obama administration has declared the critical shortage of properly trained Cybersecurity professionals a national crisis. The National certification of the courses amalgamated into this minor as well as the fact that this study meets an important National necessity will ensure the value of such a minor. In addition, it is certain that given the current global concerns with respect to privacy and access to information, this program will continue to remain relevant into the near future.

It is well known and acknowledged in the profession that Cybersecurity work represents the merging of topics areas that range from advanced technology, to law to the principles of physical information protection. This unique minor will rest on all of these foundations.

More importantly, the interdisciplinary nature of Cybersecurity knowledge will provide the UDM student body with a broader range of opportunities when they enter their chosen field.

The minor is unusual in that it demonstrates a strong collaboration between the degree programs already in place in the College of Liberal Arts and Education. This minor would not be possible without the expertise available within the Computer Information Systems program and its sub-specialty of Information Assurance, Criminal Justice, and the Social Sciences.

The commonly accepted body of knowledge in Cybersecurity is the NIST-NICE model as encompassing seven topic areas.

1. **Securely Provision**: Secure Software Development and Acquisition
2. **Operate and Maintain**: IT Operations and Sustainment Security, Database Security
3. **Protect and Defend**: Network Security
4. **Investigate**: Forensics
5. **Oversee and Govern**: Human Factors and Risk Management
6. **Analyze**: Incident Response
7. **Collect and Operate**: Information Assurance
B. Description of the Minor

B1: Narrative description of the program

A minor in Cybersecurity will add value to professionals in a range of occupations including criminal justice, psychology, business, engineering and the law. The minor will allow the student to integrate basic knowledge, skills and abilities of Cybersecurity with the in-depth knowledge and training of their chosen profession.

Students who are prepared in Cybersecurity will be uniquely able to defend our Nation against cyber threats. Given UDM’s mission, graduates of the program will be able to do that without overstepping the rights and freedoms of the everyday citizen. With respect to the current geopolitical situation, it is possible that UDM would be laying the cornerstone for an area of study that will bring an enhanced reputation and greater resources to the University for many years to come.

The Minor in Cybersecurity is available to Non-Cybersecurity students who must maintain a cumulative GPA of 2.0 in all minor courses; all courses must be taken for a grade (no courses for the minor may be taken on a pass/fail basis). A maximum of 6 credits may be counted toward both the major and the minor. At least 12 credits in the minor must be taken at UDM, unless they are taken as part of a consortium agreement. Students must declare a major before declaring a minor, and must declare the minor by the first semester of the junior year.
B2: List all courses in the curriculum

The curriculum will involve the completion of 18 credits (six courses) 12 of which will be taken in addition to the student’s major requirements and those of the University core curriculum.

Besides the five standard areas of NICE, a sixth course capstone course will also be required. That course will be CIS 4850 Information Assurance. In order to satisfy the Minor requirement and underwrite a diversity of interests, students will take the following courses in the five standard areas of NICE as well as a capstone course:

<table>
<thead>
<tr>
<th>Course</th>
<th>Standard Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIS 4840 Software Assurance</td>
<td>Securely Provision</td>
</tr>
<tr>
<td>CIS 3870 Secure Database Programming</td>
<td>Operate and Maintain</td>
</tr>
<tr>
<td>CIS 4570 Networks</td>
<td>Protect and Defend</td>
</tr>
<tr>
<td>CIS 4710 Ethical Hacking</td>
<td>Forensics</td>
</tr>
<tr>
<td>CIS 4650 Information and Society</td>
<td>Oversee and Govern</td>
</tr>
<tr>
<td>CIS 4850 Information Assurance</td>
<td>Capstone</td>
</tr>
</tbody>
</table>

B3: Indicate the delivery format of all new courses

The courses are part of the existing Computer and Information Systems undergraduate program. Consequently, the offering of the Minor will utilize excess capacity in the existing program rather than require an increase in existing resources. Initially, the course material will be offered in the traditional sense with day and evening classes though efforts will be made to develop the online delivery component upon the programs implementation.

Courses are scheduled in a regular rotation that will ensure completion of the Minor requirements in conjunction with the student’s major undergraduate degree study; e.g., the course of study will be within the conventional 126 credit limits.

Appendix B provides a matrix of the recommended course sequence for full and part time students. Appendix A provides a listing of the courses in the curriculum, including the catalog number, title, description and units of credit.
B4: Describe how the program demonstrates academic integrity
Consistent with the UDM mission, the Cybersecurity program emphasizes service to others and skills that will ensure responsible citizenship in a changing world. Cybersecurity minors will support Presidential Directive 54, the Comprehensive National Cybersecurity Initiative (CNCI). The CNCI directs higher education to prepare citizens to ensure that the boarders of cyberspace are secure. That contribution both addresses the current and future needs of the citizens of the US as well as serving the global community.

The proposed program respects academic integrity and intellectual merit put forth at UDM through the adherence to all applicable student policies, procedures and honor codes.

B5: Indicate unusual or unique characteristics of the proposed minor
Because the field is relatively new, a minor in Cybersecurity would be unique. One university in the area (Eastern Michigan) has a Minor program under the Information Assurance rubric. In reviewing their approach to this subject area, there appears to be a lack of the interdisciplinary approach as presented in this proposal. Our diversity of contributors and the flexibility of the program provides for a unique feature as compared to the EMU approach, which is much more technical.

B6: Indicate how any changes to the curriculum of the minor will be made
The Cybersecurity minor will be reviewed yearly, as is the Cybersecurity major, to ensure that the most up-to-date concepts in cyber security and information technology are incorporated into the curriculum. New Industry best practices and NIST KSA’s will be adopted within the existing course requirements.

B7: Describe how the proposed minor affects related departments or fields of concentration
Since the Cybersecurity program is looking to merge the body of knowledge of Cybersecurity with the in-depth Major study of other programs, the Cybersecurity Minor could potentially attract students into those other programs. That is particularly true given that the job outlook in the coming decade is very favorable for Cybersecurity and the ongoing need for security specialists with domain knowledge in other specialized areas of study.
C. Mission

The mission of University of Detroit Mercy (UDM) is to provide excellent student-centered undergraduate and graduate education in an urban context following in the Jesuit and Mercy Traditions. The College of Liberal Arts and Education builds on this mission by preparing students in a changing world following these traditions to be “men and women for others”.

The Major in Cybersecurity, underwrites that stated mission by preparing cyber-defenders who are ready to serve and protect not only the organizations but also the critical infrastructure of the United States. These professionals will have a direct impact to the well-being of America’s citizens. More importantly, because of the growing impact and popularity of this study it will also serve to enhance opportunity within the urban communities that UDM serves.

A Minor in Cybersecurity will also fulfill the mission of the College of Liberal Arts and Education. That mission focuses its efforts on fulfilling the intellectual, spiritual and ethical development of the student within the College, which ultimately leads to the service of others. The ability to protect the ‘everyday’ citizen from cyber intrusions and attacks on the infrastructure that underlies our way of life, as well as support the on-going fight against cybercrime is a significant contribution to society at-large.

Because the proposed Minor entails an extremely broad understanding of the field, it will place an emphasis on the development of the whole person through the combined efforts of the multi-disciplined approach. It will require the successful student to exhibit the fundamental capability to integrate concepts from diverse areas and carryout critical thinking and problem solving. This intellectual mastery is in keeping with the Jesuit and Mercy traditions.

Finally, the proposed Minor encompasses a complete and standard knowledge base, which is a necessary component of an authoritative curriculum. The successful student will be uniquely able to exhibit effective leadership skills in an advance organizational setting, which in turn will serve the community as well as the general population of the nation.

Since the proposed degree requires the student to internalize an authoritative body of knowledge (BOK), it will require mastery of a published set of professional standards. That will satisfy both the ethical and moral requirements of the university as well as those of the professional community at large. Since the Social Sciences are an important part of the Cybersecurity profession, there will be a more than adequate study of human behavior integrated into the content of the Minor.
In addition, given that ethical considerations are a central concept in Cybersecurity practice, the direct study of ethics will be required. The integration of this topic into the Minor will not be an issue as the proposed curriculum incorporates CIS 4650 Information and Society.

D. Objectives, Outcomes and Assessment

D1: Indicate the program objectives and learning outcomes

The learning objectives, outcomes and assessment were developed in conjunction with the recommendations of the NIST-NICE Framework. NICE has published this complete definition of the field with the aim of providing a point of reference for the definition of the academic curriculum of a Cybersecurity study at a college, or university. This Framework is the national standard for Cybersecurity education.

NICE is composed of seven general areas of concentration. There are 31 specialty areas distributed within these specialty areas, supported by 2,000 well-defined KSAs. The level of definition and acceptance of the NICE framework provides an easy point of reference for confirming that the detail of the proposed courses will satisfy the guidelines of the University Curriculum as put forth by the McNichols Faculty Assembly.

The General Objectives of the Minor are to:

- Provide a comprehensive and fully integrated understanding of the body of knowledge in Cybersecurity as captured in the Securely Provision, Operate and Maintain, Protect and Defend, Investigate and Oversee and Govern Areas. The other two areas are part of Intelligence Analysis and will not be covered in this Minor
- Through focused discussion and hands-on assignments ensure integration of knowledge obtained from Minor with student’s Major area of study
- Develop an understanding of the ethical issues associated with the collection and use of information, as well as instill the ability to respond appropriately when confronted by new ethical challenges
- Develop a practical skill set that can be referenced to one of the job task categories in NICE.
- Develop conceptual and human relations capabilities sufficient to ensure our graduate’s leadership status within the community.
D2: Indicate how the learning outcomes and the objectives of the minor will be assessed

The CIS Department will utilize a standard outcomes-based process to evaluate and improve the performance of its proposed minor. We believe that a focus on outcomes will provide the best assessment of program performance. The evaluation will determine the impacts and benefits of our work. The aim is to help us document and understand the changes that occurred due to our specific curricular and mentoring efforts.

Consequently, we will focus on increases in knowledge reflected in the academic performance of students in these classes over the short-term. We will also examine intermediate-term outcomes through a yearly performance review. In essence, we view the proposed minor as a system that will involve a reliable set of outcomes defined by a set of planned processes, activities and tasks. The assessment will include the outcomes of courses aimed at fostering specialized knowledge characterized by the KSAs of NIST-NICE standard.

The Cybersecurity minor will be reviewed annually, as is the Cybersecurity major, to ensure that the most up-to-date concepts in cyber security and information technology are incorporated into the curriculum. The aim is to ensure that the outcomes of the program align with the needs of our students and their employers. This assessment will keep us focused on the current situation as well as help ensure the most suitable long-term results. The evaluation process will take place in the following eight steps:

1. Designate evaluation units and standard milestones for course, as well as the expected entry and the eventual end-state.
2. Select appropriate, short-, intermediate- and long-term outcomes to evaluate. Short-term outcomes will focus on the KSAs for a given course. Intermediate outcomes will focus on in-process changes from initial KSA and attitudinal baselines.
3. Identify criteria to document the achievement of the outcomes in step two, including meaningful indicators of increases in KSAs for a given course.
4. Creation of a measurement process including defining the sources of change baselines as well as the definition of how behavior and attitudinal change data will be factored into the evaluation. Data collection methods will include academic tests, and attitudinal questionnaires. We will also standardize the data for each indicator.
5. Validation of the outcomes will be through ongoing assessment of how well the results of the testing align with the actual achievement of Minor program goals.
6. Provide an analysis of the results for the overall program as well as a formal report of the outcomes for each short-term, intermediate-term and long-term indicator.
7. Reports will be prepared for each individual course as a whole. Reports will include a statement of evaluation goals, performance measures utilized to measure
progress, the desired outcomes for each goal, the activities and technologies employed to conduct exercises, the personnel involved, as well as evaluation methodology for each goal.

8. Results from each step of the evaluative process will be used to modify courses, curriculum and program procedures as indicated by the findings.
Appendix A: Course Descriptions

**CIS 3870 Secure Database Programming** 3 credits
Implementation of secure access control. Course emphasis is on ensuring access control in a database environment. Content emphasizes IDS and access control methods and principles.

**CIS 4570 Networks** 3 credits
Course emphasis is on the principles of distributed design and development of secure data communications and network systems for business. Focus is on understanding the technology and commonly accepted standards, protocols and topologies, emphasizes security plus certification.

**CIS 4650 Information and Society** 3 credits
This course is open to all majors, it explores the role of the information professional in today’s society, topics include roles, values and norms, accountability in information use, human and social responsibility, protection and security, legal, and ethical concerns such as rights of privacy and access.

**CIS 4710 Ethical Hacking** 3 credits
This course introduces particular genres of cyber-attack tools and techniques, examining the most widely used and most damaging from each category at a high level. Ways to design and implement the most effective defenses to ensure the confidentiality, availability, and integrity of software systems and data will be explored both in lecture and in basic laboratory exercises. Emphasis will be placed on ethical and professional conduct.

**CIS 4840 Software Assurance** 3 credits
This course presents verification (review) and validation (testing) principles and methods in depth and identification of software project risk. In addition, it provides the body of knowledge in configuration management as a related process. Students will be able to prescribe an effective monitoring and control system for any kind of IT work.

**CIS 4850 Information Assurance** 3 credits
This course takes the perspective that information assurance is a strategic function. Consequently, the concepts, principles and application of all of the NICE areas will be examined. The student will be able to conduct a security risk analysis, balance resource requirements against identified weaknesses, formulate a coherent policy framework for information security using an accepted standard and deploy the appropriate set of security control objectives to meet the requirements of the defined policy framework.
Appendix B: Minor Tracking Form

TRACKING FORM
REQUIREMENTS FOR
Minor in Cybersecurity
18 CREDIT HOURS

Name: ___________________________ Date: ___________________________
Entry Status: __________________ Student Number: ___________________
College/Program: ___________________ Major Advisor: ___________________

Required Courses (18 cr.)

<table>
<thead>
<tr>
<th>Course</th>
<th>Term Taken</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIS 3870 Secure Database Programing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIS 4570 Networks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIS 4650 Information and Society</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIS 4710 Ethical Hacking</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIS 4840 Software Assurance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIS 4850 Information Assurance</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Major Advisor: ___________________________
Minor Advisor: ___________________________
Expected Date of Graduation: ___________________