



NEW PROGRAM PROPOSAL FORM

Sponsoring Institution(s): Missouri State University

Program Title: Cybersecurity

Degree/Certificate: Masters of Science

Options: N/A

Delivery Site(s): Springfield, MO

CIP Classification: 11103

*CIP code can be cross-referenced with programs offered in your region on MDHE's program inventory higher.mo.gov/ProgramInventory/search.jsp

Implementation Date: Fall 2015

Cooperative Partners: N/A

*If this is a collaborative program, form CL must be included with this proposal

AUTHORIZATION:

Frank Einhelig - Provost

Name/Title of Institutional Officer

Frank Einhelig
Signature

11-24-14
Date

Shannon McMurtrey

Person to Contact for More Information

417-836-4177

Telephone

II. Table of contents (optional)

III. Executive Summary

Students in the Master of Science in Cybersecurity degree program will complete 30 credit hours. Twenty-one of these hours will be taught within the CIS department. The remaining 9 credits will consist of a course each in Accounting, Management and Project Leadership. The research requirement (3 credits) will be met in a capstone class (CIS 770 Seminar Course in Cybersecurity). All of the courses comprising this program will be taught online.

The department anticipates 20 students during the first year of the program (18 full-time; 2 part-time) and 40 students by the fifth year (30 full-time and 10 part-time).

Given the critical shortage of Cybersecurity professionals, the department anticipates more than a 90% placement rate in security related positions.

IV. Introduction

V. Alignment With Mission and Goals

1. Need: .

A. Student Demand:

i. Estimated enrollment each year for the first five years for full-time and part-time students (Please complete table below)

Year	1	2	3	4	5
Full Time	18	21	24	27	30
Part Time	2	4	6	8	10
Total	20	25	30	35	40

ii. Will enrollment be capped in the future? No

iii. Please provide a rationale regarding how student enrollment projections were calculated

Forbes magazine recently estimated that spending on IT security is poised to grow tenfold in ten years (Forbes, 2013). Employment of Information Security Analysts is projected to grow by 37 percent through 2020 according to the Bureau of Labor Statistics (BLS, 2014)). Missouri State University currently offers one course in the area of Information Security, CIS 626. Enrollment for

that course in the Spring of 2014 is 20. We feel that through aggressive marketing of our program we should be able to attract 40 students to the program over the next five years.

(Forbes, 2013) <http://www.forbes.com/sites/richardstiennon/2013/08/14/it-security-industry-to-expand-tenfold/>

(BLS, 2014) <http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm>

B. Market Demand:

- i. National, state, regional, or local assessment of labor need for citizens with these skills.

In order to assess the need for a program such as the one we are proposing, we formed an advisory board consisting of Cybersecurity professionals from retail, education, healthcare, law enforcement, and the military. We invited them to share their thoughts on the need for a program such as the one we are proposing.

One of our advisory board members, Col. Gregory Breazile, is the Director of Cyber and Electronic warfare integration division for the United States Marine Corp. This was his response;

"Cybersecurity is currently the strategic Achilles Heel of our nation. All of our national and economic systems, to include the defense department systems, are dependent on reliable secure connectivity, which as an enterprise, are extremely vulnerable. The constant changes in our information systems and the vast scale of the management of these systems demonstrate the need for a skilled professional force of cyber defenders. As a nation we have a critical shortage of these Cybersecurity professionals and need to educate more of our citizens on Cybersecurity tactics, techniques, and procedures. This problem set will only become more complex in the future and therefore we need our educational institutions to build enduring programs to produce enough skilled leaders in Cybersecurity to meet tomorrow's threat. The Cybersecurity program being established at Missouri State University is exactly the type of education pipeline we need to fill this critical need."

Another advisory board member, Marisa Viveros, Vice President at IBM Corporation, leading the Cyber Security Innovation initiative globally, submitted the letter that is appended to this proposal.

Employment of Information Security Analysts is projected to grow by 37 percent through 2020 according to the Bureau of Labor Statistics (BLS, 2014):

Quick Facts: Information Security Analysts	
2012 Median Pay ⓘ	\$86,170 per year \$41.43 per hour
Entry-Level Education ⓘ	Bachelor's degree
Work Experience in a Related Occupation ⓘ	Less than 5 years
On-the-job Training ⓘ	None
Number of Jobs, 2012 ⓘ	75,100
Job Outlook, 2012-22 ⓘ	37% (Much faster than average)
Employment Change, 2012-22 ⓘ	27,400

(BLS, 2014) <http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm>

(Carnegie Mellon, 2013) <http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=83504>

- ii. Support letter(s) from potential employers (optional; append to proposal)

C. Societal Need:

- i. General needs which are not directly related to employment

A recent report from Carnegie Mellon described the current situation as this, "The United States is arguably in a dire situation in terms of cyber preparedness. Cyber attacks and their sophistication are growing exponentially, while the cyber workforce is struggling to develop and sustain the talent needed to protect, detect, defend, and respond to these attacks. Since the nation has become deeply dependent on cyberspace, the realization of an attack is a risk with detrimental consequences to critical services and every sector." (Carnegie Mellon, 2013)

- ii. Support letter(s) from community leaders (optional; append to proposal)

- D. Methodology used to determine "A" and "B" and "C" above.
Market research and interviews with advisory board members.

2. Duplication and Collaboration (Form CL):

If similar programs currently exist in Missouri, what makes the proposed program necessary and/or distinct from the others at public institutions, area vocational technical schools, and private career schools?

N/A

Does delivery of the program involve a collaborative effort with any external institution or organization? If yes, please complete the rest of this section (Form CL. If no, state not applicable and go to item 3.

N/A

Length of agreement (open-ended or limited): _____

- A. Which institution(s) will have degree-granting authority?
- B. Which institution(s) will have the authority for faculty hiring, course assignment, evaluation, and reappointment decisions?
- C. What agreements exist to ensure that faculty from all participating institutions will be involved in decisions about the curriculum, admissions standards, exit requirements?
- D. Which institution(s) will be responsible for academic and student-support services, e.g., registration, advising, library, academic assistance, financial aid, etc.?
- E. What agreements exist to ensure that the academic calendars of the participating institutions have been aligned as needed?
- F. In addition to the information provided by each participating institution regarding Financial Projections (item 4 below), please address the following items:
 - I. How will tuition rates be determined if they differ among the institutions?
 - II. Has a formal agreement been developed regarding cost-sharing policies? If yes, please include it as part of the proposal. If no, please summarize the current understanding between all parties and the plans for developing a formal agreement.
 - III. What arrangements, if any, have been made for exchange of money between participating institutions?
- G. What commitments have been made by all participants to evaluate the program systematically?
- H. If one institution wishes to discontinue the program, what agreements exist for terminating the offering?

3. Program Structure (form PS):

- A. What are the total credits required for graduation? This should match C+D+E below.

30

- B. Are there any residency requirements? 21 credit hours are required from Missouri State University with 9 additional hours of transfer credit allowable.

Total Credits by Category

- C. General Education courses: Total credits required: Bachelor's degree from a regionally accredited College or University

Total above should be the same as item 3.C.

- D. Major requirements: total credits required: 30

Course Number	Credits	Course Title
CIS 626	3	Fundamentals of Information Security
CIS 683	3	Cloud Computing
ACC 751	3	Computer Forensics and I.T. Auditing
CIS 762	3	I.T. Legal Issues in Cybersecurity
CIS 763	3	Telecommunications and Network Security
CIS 764	3	Hacker Techniques and Incident Response
MGT 764	3	Organizational Behavior
CIS 766	3	Web Application Security
TCM 710	3	Project Leadership
CIS 770	3	Seminar Course in Cybersecurity

Total above should be the same as item 3.C.

- E. Free elective credits: N/A
- F. Describe any requirements for thesis, internship or other capstone experience.

CIS 770 Seminar In Cybersecurity: Prerequisite: 15 hours of graduate Cybersecurity courses and permission from the Cybersecurity Program Director.

Critical evaluation and interpretation of research and literature in Cybersecurity and completion of significant research project.

- G. Describe any unique features such as interdepartmental cooperation.
 Students are required to take one course each in Accounting, Management, and Project Leadership. This will add to their technical skills, the ability to communicate with, and understand the needs of users throughout the organization. These courses are housed in the following departments of the College of Business: Accounting, Management, and Technology and Construction Management respectively. All College of Business departments at Missouri State University are supportive of the proposed Cybersecurity program.

4. Financial Projections (for public institutions only; Form FP): Please complete table at the end of this document. Additional narrative may be added as needed. If more than one institution is providing support, please complete a separate table for each institution.

The table at the end of this document has been completed.

5. Program Characteristics and Performance Goals (form PG). For collaborative programs, responsibility for program evaluation and assessment rests with the institution(s) granting the degree(s).

Although all of the following guidelines may not be applicable to the proposed program, please carefully consider the elements in each area and respond as completely as possible in the format below. Quantification of performance goals should be included wherever possible.

A. Student Preparation

- Any special admissions procedures or student qualifications required for this program which exceed regular university admissions, standards, e.g., ACT score, completion of core curriculum, portfolio, personal interview, etc. Please note if no special preparation will be required.

No requirements beyond university admission standards will be required.

- Characteristics of a specific population to be served, if applicable. N/A

B. Faculty Characteristics

- Any special requirements (degree status, training, etc.) for assignment of teaching for this degree/certificate.

AACSB (Association to Advance Collegiate Schools of Business) dictates that faculty teaching in the program be academic and/or professionally qualified.

- Estimated percentage of credit hours that will be assigned to full time faculty. Please use the term "full time faculty" (and not FTE) in your descriptions here.

75% full time faculty, 25% per course instructors.

- Expectations for professional activities, special student contact, teaching/learning innovation.

Faculty are expected to have a strong interest in Cybersecurity demonstrated through educational training, professional and/or community involvement.

C. Enrollment Projections (repeat section 1.A.I)

- Student FTE majoring in program by the end of five years.

40

- Percent of full time and part time enrollment by the end of five years.

75% full time, 25% part time.

D. Student and Program Outcomes

- Number of graduates per annum at three and five years after implementation.

30 students at the third year, 40 by the fifth year.

- Special skills specific to the program.

Students graduating from our program will have a combination of hands-on Cybersecurity skills and business knowledge enabling them to understand the needs and priorities of the businesses they serve. This will position them as business leaders with Cybersecurity skills and knowledge.

- Proportion of students who will achieve licensing, certification, or registration.

At this time there are no certification requirements for students although students will be prepared to test for Certified Information Security Manager (CISM) and the Certified Information Systems Security Professional (CISSP) certification, both of which could be granted after the requisite number of years of professional experience has been attained.

- Performance on national and/or local assessments, e.g., percent of students scoring above the 50th percentile on normed tests; percent of students achieving minimal cut-scores on criterion-referenced tests. Include expected results on assessments of general education and on exit assessments in a particular discipline as well as the name of any nationally recognized assessments used.

We will have program assessment in place to monitor student learning outcomes.

- Placement rates in related fields, in other fields, unemployed.

We anticipate 90%+ placement in security related positions.

- Transfer rates, continuous study.

N/A

E. Program Accreditation

- Institutional plans for accreditation, if applicable, including accrediting agency and timeline. If there are no plans to seek specialized accreditation, please provide reasons.

This program will be part of the existing College of Business AACSB accreditation.

F. Alumni and Employer Survey

- Expected satisfaction rates for alumni, including timing and method of surveys

We anticipate an 80%+ satisfaction rate to be measured through online surveys every three years.

- Expected satisfaction rates for employers, including timing and method of surveys

We expect high levels of satisfaction that will be assessed through the corporate relations staff of the College of Business.

6. No Program Specific Accreditation: If accreditation is not a goal for this program, provide a brief rationale for your decision. If the institution is seeking program accreditation, provide any additional information that supports your program.

This program will be part of the existing College of Business AACSB accreditation with no program specific accreditation.

7. Will this program be offered primarily at an off-campus location? If yes, complete this section. If no, skip to Item 9. N/A

Quality Assurance for Off-Site Programs:

- A. General Oversight: Describe the manner in which this program will be managed. How does the management of this program fit within the institution's academic administrative structure?
- B. Faculty Qualifications: How do the qualifications of faculty at this site compare with those of faculty for this program at the main campus? Please also note the comparable data regarding the proportion of course-section coverage by full-time faculty at each site.

- C. **Support Services:** Describe how the institution will ensure that students at this site will be able to access services such as academic support, library, computing, and financial aid, as well as other administrative functions, at a level of quality comparable to that of on-campus programs.

8. **Institutional Characteristics:** Please describe succinctly why your institution is particularly well equipped or well suited to support the proposed program.

The College of Business (COB) at Missouri State University holds the Association to Advance Collegiate Schools of Business (AACSB) international accreditation. The CIS department within the COB consists of academically and professionally qualified faculty who will be involved in the delivery of this program. The program director has completed extensive professional development programs to establish currency in the field. In addition to the excellent foundation provided by our faculty, we have formed an advisory board consisting of Cybersecurity experts with retail, law enforcement, healthcare, government, education, and military backgrounds to assist us crafting a curriculum that will ensure real world success for our graduates. Our advisory board members include:

Col. Greg Breazile. Colonel Breazile is currently serving as the Director, Cyber & Electronic Warfare Integration Division, Capabilities Development Directorate, Deputy Commandant Combat Development & Integration.

Kerry Killker, VP and Chief Information Security Officer, Wal-Mart

Marisa Viveros, Vice President at IBM Corporation, leading the Cybersecurity Innovation initiative globally.

Michael Green, Senior Vice President at MasterCard, Group head Cybersecurity global.

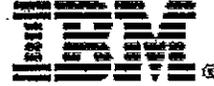
Dan Henke, Chief Information Security Officer Mercy Health Systems

Will Spencer, Chief Information Security Officer Missouri State University

Angela Morelock, Partner, Board Member, BKD, LLC

Christopher Lamb, Special Agent, FBI

9. **Any Other Relevant Information**



March 21, 2014

Dr. Stephanie M. Bryant
Dean, College of Business
Missouri State University
901 S. National Avenue
Springfield MO 65897

Dear Dean Bryant:

IBM is pleased to express our enthusiastic support for Missouri State University's proposal for new education programs in Cybersecurity. While security threats are growing at an exponential rate, affecting everyone, and putting at risk the nation's financial, energy, health care and other critical infrastructure; there is a need for professionals that have the knowledge and insights to counteract such threats.

We believe the proposed Graduate Certificate Program in Cybersecurity and the Master Degree in Cybersecurity will assist in closing the nation's cybersecurity skills gap. To support Missouri State University programs, IBM has a 21st Century Skills initiative that includes Big Data, Analytics, and Cyber Security. Established procedures make resources accessible to our academic partners, such as software, course materials, case studies, and other valuable teaching materials, as part of *IBM Academic Initiatives*. IBM is also honored to participate in the Missouri State University's *Cybersecurity Advisory Board*.

As we move forward, we recognize that the future of economies and societies will depend upon trusted systems, trusted data, and trusted people. We can only achieve this future by continuously innovating in systems, technologies, policies and standards that allow us to build a more secure digital world. Pivotal to such developments are an educated and smart workforce in Cybersecurity fundamentals and practices.

With our utmost recommendation, we hope Missouri State University's proposal for new Cybersecurity education programs is approved, as these will increase the number of critical skills and build the talent pipeline for the future.

Sincerely,

A handwritten signature in black ink, appearing to read "Marisa Viveros", is written over a horizontal line.

Marisa Viveros
Vice President, Cyber Security Innovation
IBM Corporate Strategy



STUDENT ENROLLMENT PROJECTIONS

Year	1	2	3	4	5
Full Time	18	21	24	27	30
Part Time	2	4	6	8	10
Total	29	25	30	35	40

Please provide a rationale regarding how student enrollment projections were calculated:

Forbes magazine recently estimated that spending on IT security is poised to grow tenfold in ten years (Forbes, 2013). Employment of Information Security Analysts is projected to grow by 37 percent through 2020 according to the Bureau of Labor Statistics (BLS, 2014). Missouri State University currently offers one course in the area of Information Security, CIS 626. Enrollment for that course in the spring of 2014 is 20. We feel that through aggressive marketing of our program we should be able to attract 40 students to the program over the next five years.

(Forbes, 2013) <http://www.forbes.com/sites/richardstiennon/2013/08/14/it---security--industry--to---expand---tenfold/>

(BLS, 2014) <http://www.bls.gov/ooh/computer---and---information---technology/information---security---analysts.htm>

Provide a rationale for proposing this program, including evidence of market demand and societal need supported by research:



National, state, regional, or local assessment of labor need for citizens with these skills.

In order to assess the need for a program such as the one we are proposing, we formed an advisory board consisting of Cybersecurity professionals from retail, education, healthcare, law enforcement, and the military. We invited them to share their thoughts on the need for a program such as the one we are proposing.

One of our advisory board members, Col. Gregory Breazile, is the Director of Cyber and Electronic warfare integration division for the United States Marine Corp. This was his response;

"Cybersecurity is currently the strategic Achilles Heel of our nation. All of our national and economic systems, to include the defense department systems, are dependent on reliable secure connectivity, which as an enterprise, are extremely vulnerable. The constant changes in our information systems and the vast scale of the management of these systems demonstrate the need for a skilled professional force of cyber defenders. As a nation we have a critical shortage of these Cybersecurity professionals and need to educate more of our citizens on Cybersecurity tactics, techniques, and procedures. This problem set will only become more complex in the future and therefore we need our educational institutions to build enduring programs to produce enough skilled leaders in Cybersecurity to meet tomorrow's threat. The Cybersecurity program being established at Missouri State University is exactly the type of education pipeline we need to fill this critical need."

Another advisory board member, Marisa Viveros, Vice President at IBM Corporation, leading the Cyber Security Innovation initiative globally, submitted the letter that is appended to this proposal.

Employment of Information Security Analysts is projected to grow by 37 percent through 2020 according to the Bureau of Labor Statistics (BLS, 2014)).



PROGRAM CHARACTERISTICS AND PERFORMANCE GOALS

Institution Name Missouri State University
Program Name Cybersecurity Masters of Science
Date 11/20/14

(Although all of the following guidelines may not be applicable to the proposed program, please carefully consider the elements in each area and respond as completely as possible in the format below. Quantification of performance goals should be included wherever possible.)

1. Student Preparation

- Any special admissions procedures or student qualifications required for this program which exceed regular university admissions, standards, e.g., ACT score, completion of core curriculum, portfolio, personal interview, etc. Please note if no special preparation will be required.
No requirement beyond university admission standards will be required.
- Characteristics of a specific population to be served, if applicable.
N/A

2. Faculty Characteristics

- Any special requirements (degree status, training, etc.) for assignment of teaching for this degree/certificate.
AACSB (Association to Advance Collegiate Schools of Business) dictates that faculty teaching in the program be academic and/or professionally qualified
- Estimated percentage of credit hours that will be assigned to full time faculty. Please use the term "full time faculty" (and not FTE) in your descriptions here.
75% full time faculty, 25% per course instructors.
- Expectations for professional activities, special student contact, teaching/learning innovation.
Faculty are expected to have a strong interest in cybersecurity demonstrated through educational training, professional and/or community involvement.

3. Enrollment Projections

- Student FTE majoring in program by the end of five years.
40
- Percent of full time and part time enrollment by the end of five years.

www.dhe.mo.gov • Info@dhe.mo.gov

205 Jefferson Street, P. O. Box 1469, Jefferson City, MO 65102 • (573) 751-2361 • (800) 473-6757 • Fax (573) 751-6635

75% full time, 25% part time.

4. Student and Program Outcomes

- Number of graduates per annum at three and five years after implementation.
30 students at the third year, 40 by the fifth year.
- Special skills specific to the program.
Students graduating from the program will have a combination of hands-on Cybersecurity skills and business knowledge enabling them to understand the needs and priorities of the businesses they serve. This will position them as business leaders with Cybersecurity skills and knowledge.
- Proportion of students who will achieve licensing, certification, or registration.
At this time there are no certification requirements for students, although students will be prepared to test for Certified Information Security Manager (CISM) and the Certified Information Systems Security Professional (CISSP) certification, both of which could be granted after the requisite number of years of professional experience has been attained.
- Performance on national and/or local assessments, e.g., percent of students scoring above the 50th percentile on normed tests; percent of students achieving minimal cut-scores on criterion-referenced tests. Include expected results on assessments of general education and on exit assessments in a particular discipline as well as the name of any nationally recognized assessments used.
We will have program assessment in place to monitor student learning outcomes.
- Placement rates in related fields, in other fields, unemployed.
We anticipate 90%+ placement in security related positions.
- Transfer rates, continuous study.
N/A

5. Program Accreditation

- Institutional plans for accreditation, if applicable, including accrediting agency and timeline. **If there are no plans to seek specialized accreditation, please provide a rationale.**
This program will be part of the existing College of Business AACSB accreditation

6. Alumni and Employer Survey

- Expected satisfaction rates for alumni, *including timing and method of surveys.*
We anticipate an 80%+ satisfaction rate to be measured through online surveys every three years.
- Expected satisfaction rates for employers, including timing and method of surveys.

www.dhe.mo.gov • info@dhe.mo.gov

205 Jefferson Street, P. O. Box 1469, Jefferson City, MO 65102 • (573) 751-2361 • (800) 473-6757 • Fax (573) 751-6635

We expect high levels of satisfaction that will be assessed through the corporate relations staff of the College of Business.

7. Institutional Characteristics

- Characteristics demonstrating why your institution is particularly well-equipped to support the program.

The College of Business (COB) at Missouri State University holds the Association to Advance Collegiate Schools of Business (AACSB) international accreditation. The CIS department within the OCB consists of academically and professionally qualified faculty who will be involved in the delivery of this program. The program director has completed extensive professional development programs to establish currency in the field. In addition to the excellent foundation provided by our faculty, we have formed an advisory board consisting of cybersecurity experts with retail, law enforcement, healthcare, government, education, and military backgrounds to assist us crafting a curriculum that will ensure real world success for our graduates. Our advisory board members include: Col. Greg Breazile, currently serving as the Director, Cyber & Electronic Warfare Integration Division, Capabilities Development Directorate, Deputy Commandant Combat Development & Integration. Kerry Kilker, VP and Chief Information Security Officer, Wal-Mart. Marisa Viveros, Vice President at IBM Corporation, leading the Cybersecurity Innovation initiative globally. Michael Green, Senior Vice President at MasterCard, group head Cybersecurity global. Dan Henke, Chief Information Security Officer Mercy Health Systems. Will Spencer, Chief Information Security Officer Missouri State University. Angela Morelock, Partner, Board Member, BKD, LLC. Christopher Lamb, Special Agent, FBI.