University of Colorado Colorado Springs

Graduate Executive Committee
November 8, 2019
Minutes

Attendees:
Voting Members: Jeff Ferguson, Jeff Spicher, Mandi Elder, Andy Subudhi, Jon Caudill, Henriikka Weir, Cathy Simmons, Steve Tragesser, Karen Livesey, Janel Owens, Jeremy Bono, Kay Yoon, Roger Martinez, Beth Daniels, Esther Lamidi, David Fenell, Linda Button,
Non-Voting Members: Wendi Clouse, Amy Reynolds, Tina Ewald, Gurvirender Tejay, Janice Dowsett, Rob Block, Rosey Reidl-Smith, Ron Koch, Yang Xu, Sarah Elsey, Kelli Klebe, KrisAnn McBroom

- Sociology MA proposed Comprehensive examination addition and removal of oral examination option- Dr. Lamidi
    - Sociology would like to remove their oral examination option and add in a comprehensive examination which will include a written component and an oral component. See attached proposal.
    - The GEC voted to approve (15 yes, 0 no, 1 abstain) with the clarification that a comp exam failure requires a two month window between examination periods.
- Doctorate in Business Administration (Executive DBA) in Cybersecurity Management proposal- Dr. Tejay
    - See attached proposal for details.
    - GEC voted to recommend approval a new DBA with track in Cybersecurity management (13 yes, 1 no, 0 abstain)
- New emphasis in Cybersecurity for the MBA program- Dr. Tejay
    - See attached proposal.
    - GEC voted to recommend approval the new track in MBA (14 yes, 1 no, 1 abstain)
- New Gainful Employment Graduate Certificate in Cybersecurity under College of Business- Dr. Tejay
    - See attached proposal
    - GEC voted to recommend approval for the new GE in Cybersecurity (14 yes, 1 no, 1 abstain)
- Application fee waivers are live
    - See attached for wording on application. Please let us know if you have any questions or feedback.
- Discussion about travel awards
    - The graduate school currently gives out up to $400 travel awards for US travel and $800 for international travel to graduate students. Does this amount seem like enough to provide impact for students?
        - GEC generally felt this was a good amount. Balancing the need to support as many students as we can while providing a worthwhile amount of money. The funds do not work for all students/programs but in general is working.

<u>Announcements: PLEASE SHARE WITH FACULTY AND STUDENTS</u>

- **Mountain Lion Research Day** is December 13, 2019 8:30-11:30 am in Berger Hall
    - Submit your abstracts now! Deadline is December 2, 2019
    - Registration link: https://www.uccs.edu/research/mlrd-registration
- **Mountain Lion Grad Slam**- Please encourage your students to participate! Registration is open.
    - Preliminary rounds January 27 and 28. Finals are on Friday January 31st 12:00-1:00 in Berger Hall
    - Register here: https://www.uccs.edu/graduateschool/current-students/mountain-lion-grad-slam

- **Designing a Research Poster**
  Participating in Mountain Lion Research Day? This workshop will teach you how to design and create a professional poster with PowerPoint. Learn how to use color, design principles, and straightforward text to present your research in a compelling and eye-catching way.
    Tuesday November 19, 4:45 pm, EPC 237 - register here
    Wednesday November 20, 6 pm, EPC 237 - register here
- Commencement is Friday December 20th at the Broadmoor World Arena at 2:00
- New student welcome reception Spring
  - Friday January 24th at 5:00 location TBD
- Fall 2019 GEC Meetings (10:00-11:30; location Dwire 204)
  - Dec 13
- Spring 2020 GEC Meetings (10:00-11:30; location Dwire 204)
  - Feb 14, Mar 13, April 10, May 8 (UC Brooks 126, May only)

Department of Sociology Proposed MA Comprehensive Examination Policy

To: Graduate Executive Committee
23 October 2019

1) The Program & Degree Plan
The Sociology Department at UCCS offers two tracks that Master's student can follow in completion of the MA in sociology. One track is completing a thesis under the guidance of faculty and the other is a non-thesis track. Currently, the non-thesis track requires students to complete a total of 30 hours of approved course work and pass a comprehensive oral examination. The comprehensive examination is based on a discussion of the materials provided by the student in their graduate student portfolio. During the examination the student is asked to summarize their educational development in the program and relate this to further academic work and/or career plans. The graduate student portfolio should include: a self-statement detailing the student's goals and what they have learned; an academic resume and copies of papers from each of the required sociology courses.

The graduate faculty of the Sociology Department has determined that the comprehensive oral examination does not full the department's mission since it lacks consistency, rigor, and equity between students. Instead, we propose instituting a comprehensive examination that will directly test students' knowledge of the field. Students will be provided with a series of prompts designed to test their sociological knowledge that they will respond to in essays.

2) Resource Needed For Comprehensive Examination
We do not foresee need for additional resources for the comprehensive exam.

3) Student Demand for Comprehensive Examination
The students have not asked for a more a rigorous examination process than what currently exists. However, feedback collected from students suggest they would like clarity in the process of completing the degree and do not believe the current comprehensive oral examination is a rigorous test of their knowledge.

4) Faculty Expertise In the Area
All of the graduate faculty are professional sociologist holding the highest degree in our field; a PhD.

5) Other Information Relevant to the Discussion
The department sees the comprehensive examinations following these six steps:

Step 1. On or before the first day of classes of the semester that a student plans to complete the degree, they must submit their intent to graduate along with their transcripts.
Step 2. At the first Department meeting of the semester, the department will select a committee of three graduate faculty members, to be kept anonymous from the student, to create the questions and review their answers.

A. Each committee member will create 3 questions.
B. The committee will then select 6 questions to be given to the student.

Step 3. On Monday of week 9 of the semester, questions will be dispersed to the students. They must select 4 of 6 questions and write a 4 - 5 page response to each question.
Step 4. They will have two weeks to complete the essays (due Monday of Week 11). Essays must be submitted through Canvas and run through "Turn it in".
Step 5. The Committee will have 1 week (Monday of week 12) to approve or decline the work. If the committee declines to pass the work, the student will have 1 week to address the concerns and to rewrite the essays that need rectification. Rewritten work must be submitted by the Monday of week 13.

A. If the revised work still does not pass, the faculty have grounds to expel the student from the program.
B. The committee members will remain anonymous until the student passes the examination.

Step 6. An oral defense of their essays will occur in week 14. The student will schedule the oral defense and work with the department administrator to reserve a room. If the student fails the oral exam, they can have a second attempt in Week 15 to successfully pass the oral examination.

If the department's proposed change to the non-thesis track is approved, the graduate faculty will develop a rubric for grading the comprehensive examinations.

University of Colorado
Colorado Springs

Proposal for
EXECUTIVE DOCTOR OF BUSINESS ADMINISTRATION IN CYBERSECURITY MANAGEMENT

November 2019

Table of Contents

1. Program description

Cybercrime has become a societal menace with increasingly prevalent cybersecurity breaches nowadays. The organizations and governments are spending billions of dollars to address this problem with little impact on reducing security breaches. There is an imperative need in industry and government for rigorously trained reflective thinkers at executive level who are able to grasp the technical and organizational challenges inherent in security discipline. The Executive Doctor of Business Administration in Cybersecurity Management (EDBA-Cyber) is a unique terminal degree designed to develop scientist-practitioners who will be skilled in practice-focused research in cybersecurity.

The cybersecurity discipline encompasses business, technical, social, and scientific fields and requires multi-disciplinary knowledge to become successful practitioner. The three-year, part-time program is designed for the working executives, in particular, Senior Executives with Information Security, IT, Compliance or Auditing experience. The research approach for EDBA is the "engaged scholarship" model that focuses on topics at the intersection of theory and contemporary cybersecurity issues. The focus is on addressing complex security problems in organizations through understanding and application of latest research in information security.

The interdisciplinary EDBA-Cyber program aims to develop ethical security leaders who can improve security practice globally through applied, evidence-based analysis and rigorous evaluation of complex issues in play. This degree will enable our students to successfully employ skills learned to tackle the security problems in organizations. The program's instruction will follow blended learning approach involving a combination of traditional face-to-face lectures, online learning, discussions and seminars. The program will involve limited residency cohorts.

The EDBA degree provides potential students with appropriate educational credentials to gain vital edge in competitive environment. The graduates will benefit from knowledge improvement in cybersecurity, and potential opportunities for career differentiation and advancement into leadership positions. The program is not designed to train students to pursue an academic career as tenure-track faculty.

1.a. Student Learning Outcomes

The degree program is designed to equip students with the ability to:

1. Develop skills for cybersecurity scholarship and research competency.
2. Analyze and communicate issues impacting cybersecurity.
3. Demonstrate knowledge of information security research.
4. Apply current research to address complex problems of cybersecurity practice.

The student outcome will be assessed through successful completion of coursework, proposal defense, and successful defense and completion of the dissertation.

2. Workforce and Student Demand

This section presents workforce and student demand in cybersecurity management.

2a. Workforce demand

According to Burning Glass, cybersecurity jobs account for 13% of all IT jobs. The demand for cybersecurity skills has risen 255% since 2013, while demand for risk management rose by 133%. Employer demand for cybersecurity professionals across the United States continues to accelerate with the knowledge of public cloud security (170%) projected to be the fastest-growing cybersecurity skill in demand. According to CyberSeek, a project supported by the National Initiative for Cybersecurity Education (NICE), a program of the NIST in the U.S. Department of Commerce, there are 313,735 cybersecurity jobs openings across US, while 780,000 people were employed in various cybersecurity positions. The Bureau of Labor Statistics estimates that employment of Information Security Analysts is projected to grow by 32% from 2018 to 2028, much faster than the average for all occupations. Cybersecurity Ventures, Cybersecurity analytics and research company, predicts that there will be 3.5 million unfilled cybersecurity positions by 2021. Please refer to table 1 for current demand for cybersecurity jobs.

Table 1. Cybersecurity Demand (Source: www.cyberseek.org)

Role	**Job Openings**	**Average Salary**
Cybersecurity Job Openings in US	313,735	
Cybersecurity Analyst	26,013	$85,000
Cybersecurity Consultant	13,439	$100,00
Cybersecurity Manager or Administrator	14,320	$115,000
Chief Information Security Officer	5,130	$224,388
Cybersecurity PhD (Specialized Roles)	764	$259,000

The State of Colorado has currently 10,207 job openings in cybersecurity (Source: www.cyberseek.org). The Colorado Springs region is home to 125-plus cybersecurity companies as well as five NSA/DHS Centers of Academic Excellence (CAEs) in cybersecurity education. UCCS is one of the designated CAE-Cyber Defense Education institutions. The total cybersecurity industry employment in Colorado Springs is 3,371 with a projected total demand forecast at 6,967 by 2025.

There are about 5,130 job openings for Chief Information Security Officer (CISO) (Source: www.indeed.com). For CISOs, about 40% of them have a master's degree and 4% have a doctorate. While the average early and mid-career salaries of information assurance Ph.D.'s are quite strong, many C-Level information assurance roles can bring in $300,000+. The top 10% of jobs for Ph.D.'s in information assurance bring in $259,000 a year or more, making information assurance the highest paying Ph.D. surveyed in 2018 rankings (www.online-phd-degrees.com).

2b. Student demand

The proposed EDBA-Cyber program will target students who have completed their graduate degree (Masters) and satisfied the prerequisites for admission to the program. The program is designed for the working executives with a minimum of 5 years of managerial or consultative experience in cybersecurity, information systems, IT, or related field.

There is a significant demand in industry for doctoral programs in cybersecurity. Most professionals need the degree to advance in cybersecurity profession in terms of attaining higher roles/positions, become C-level executive, migrate to lucrative industry (finance, healthcare, consulting), or pursue research career in industry or government. At St. Thomas University, the Executive DBA in Information Security attracted quite a few students resulting in meeting the cap of 10 students per year from Year 1 itself. This program enrolled 20 students by the end of second year with recruitment from South Florida region only.

The EDBA-Cyber will recruit students from across the country focusing on 780,000 professionals currently employed in cybersecurity positions. We will initially target 10 states over three phases (see Table 2).

Table 2. Cybersecurity Workforce (Source: www.cyberseek.org)

Phase	State	Cybersecurity Workers	Total Cybersecurity Workers
I	Colorado	18,443	162,814
	California	78,886	
	Virginia	65,485	
II	New York	45,751	84,051
	Florida	13,465	
	Texas	24,835	
III	Georgia	25,418	86,484
	North Carolina	13,078	
	Maryland	31,386	
	Washington	16,602	

Among 10 states listed in Table 2, we will focus on holders of cybersecurity expert certifications of Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP), and Certified Information Systems Auditor (CISA). These certifications require significant work experience and understanding of information systems security. Please see Table 3 for breakdown of the number of cybersecurity certification holders across 10 states. We intend to enroll less than 0.1% of cybersecurity certification holders over three phases.

Table 3. EDBA-Cyber Target States (Source: www.cyberseek.org)							
Phase	**State**	**Cybersecurity Workers**	**Cybersecurity Certification Holders**				**Phase Total**
			CISM	**CISSP**	**CISA**	**Total**	
I	Colorado	18,443	312	2729	723	3764	**24625**
	California	78,886	1339	7017	3514	11870	
	Virginia	65,485	1625	4970	2396	8991	
II	New York	45,751	722	2373	1957	5052	**22546**
	Florida	13,465	901	4094	1861	6856	
	Texas	24,835	1136	6163	3339	10638	
III	Georgia	25,418	569	2793	1238	4600	**19574**
	North Carolina	13,078	377	2245	1144	3766	
	Maryland	31,386	846	6101	1180	8127	
	Washington	16,602	304	2062	715	3081	

The realistic enrollment projections for the EDBA-Cyber program for the first five years can be found in Appendix A. The EDBA-Cyber is a part-time program with limited residency cohorts. It is designed to handle three cohorts of 20 students, for a total of 60 students throughout the 3-year program. The program's instruction will follow blended learning approach involving a combination of in-person lectures, online learning, discussions and seminars.

3. Role and Mission Criteria

The mission of EDBA in Cybersecurity Management program is to develop scientist-practitioners who will be skilled in practice-focused cybersecurity research and can improve security practice globally through applied, evidence-based analysis and rigorous evaluation of complex issues in play.

The mission of the EDBA-Cyber is aligned with the mission of the University as well as the College of Business. The UCCS mission is to "be a comprehensive baccalaureate and specialized graduate research university…offer liberal arts and sciences, business, engineering…programs, and a selected number of master's and doctoral degree programs". The proposed EDBA-Cyber program fulfills this mission by providing a unique professional doctoral program for cybersecurity practitioners.

The mission of the College of Business includes offering "…select master's degrees and professional programs that emphasize principle-based ethical decision making…support innovation and impact in our teaching, research and service." The College realizes this mission by producing intellectual contributions that impact the theory, practice and teaching of business. The proposed EDBA-Cyber program fulfills this mission by offering a unique professional program focused on developing ethical cybersecurity leaders. The program is innovative in nature blending cybersecurity foundations and knowledge with business knowledge and scientific research methods delivered as a part-time program with busy executives. These scientist-practitioners will produce practice-focused intellectual contributions in cybersecurity research and impact the theory and practice of cybersecurity.

Further, the proposed EDBA-Cyber is aligned with UCCS' priority focus on cybersecurity discipline and initiatives. The program also addresses three of the strategic themes (or core strategies) identified for the UCCS 2030 Strategic Plan:

I. Strategy 2: Enhance strategic enrollment and retention efforts to drive long-term stability and sustainability.
II. Strategy 5: Strengthen and expand revenue sources to ensure future growth and improve student affordability and access.
III. Strategy 6: Support competitive programs and initiatives, both existing and new, that show the university's unique value and identity in the higher-education landscape

4. Duplication

There are 54 programs in EDBA across the world focused on general business that have already been launched or are in implementation stage. Please see table 4 for the programs offered by prominent US universities. There is only one EDBA in Information Security program offered by the St. Thomas University (Miami, FL). However, there is no EDBA program (general or cybersecurity) in the state of Colorado.

Table 4. Prominent EDBA Programs in the US (Source: Executive DBA Council)

University	**Tuition**
Case Western Reserve University	$150k
DePaul University	$129k
Drexel University	$120k
Florida Institute of Technology	$54k
Florida International University	$73k
Georgia State University	$109k
Oklahoma State University	$120k
Pepperdine University	$161k
Rollins College	$107k
Temple University	$124k
University of Florida	$108k
University of Missouri-St. Louis	$96k
University of North Carolina at Charlotte	$85k
University of South Florida	$90k

Further, the College of Business at UCCS does not offer any doctoral program. The proposed EDBA in Cybersecurity Management will be the first doctoral program to be offered by the College.

5. Statutory Requirements

The admission requirements for the EDBA-Cyber program are in line with the UCCS graduate admissions requirements for the College of Business and the UCCS Graduate school. The admission to the program is competitive and formal admission to the program will include a screening process, evaluation of credentials, and interview with the admissions committee.

The proposed EDBA-Cyber will require a total of 60 credit for graduation. The students are expected to complete all required coursework with grades and GPA stipulated by the College of Business and the Graduate School.

5.a. Transfer Credits

Graduate work completed at another accredited school or at UCCS may be accepted as transfer credit if the course work parallels courses offered in EDBA-Cyber. In general,

- Students may transfer a maximum of fifteen (15) hours of graduate level coursework completed at another accredited school to be applied to EDBA-Cyber.
- Students may transfer no more than fifteen (15) credits forward from one UCCS Master's degree to EDBA-Cyber.

Any transfer of credit has to adhere with UCCS Transfer Credit Policy as listed in the Graduate Catalog.

5.b. Admission Requirements

This section presents the *minimum* standards for admission of students to the Executive DBA in Cybersecurity Management degree program. The admission to the EDBA program is competitive and selections will be based on several factors including graduate GPA, academic background, professional experience, goals statement, writing skills, optional test scores, and/or letters of recommendation. Additionally, selected applicants should:

- Demonstrate familiarity with IT or cybersecurity profession
- Show evidence of the potential success in doctoral education
- Show evidence of potential success as a professional in the field of cybersecurity management

Formal admission to the EDBA-Cyber program will include a screening process, evaluation of credentials, and interview with the admissions committee.

The applicants for the program must meet the following requirements:

1. An earned Master's degree in information security, information systems, information technology, computer science or a related area with a minimum 3.0 GPA.
2. A minimum of five years of managerial or consultative experience in cybersecurity, information systems, IT, compliance, audit or related field.
3. Personal Goals Statement. This essay should include the following:
    a. Discuss your reasons for pursuing this degree.
    b. Please include information on your strengths and weaknesses.
    c. Describe how you plan to balance the time commitment required for the program (about 20 hours per week) with your personal and professional responsibilities.
    d. Any obstacles or anticipated impediments to successfully complete the program.
4. Resume or Curricular Vitae.
5. Two letters of recommendation (optional)

College of Business Admission Requirements

The Graduate School of Business Administration seeks to admit students who show a high likelihood of success in postgraduate business study. The following basic indicators are used to evaluate candidates for admission:

Prior Academic Experience. A graduate degree from a regionally accredited institution or foreign equivalent is a condition for application. The applicant's complete academic record from all institutions attended is examined.

Foundation Requirements. The applicants for EDBA program should have completed coursework in statistics as part of their undergraduate degree. The coursework must have been completed at a regionally accredited institution. If the above-mentioned course was not completed, the Graduate School of Business Administration provides the following foundation course as required background courses: QUAN 5500 - Fundamentals of Business Statistics.

Foundation Course Waiver: This course may be waived with prior academic coursework Waiver is based on a number of criteria, including the age of the prior coursework, the grade earned, and other considerations determined by the faculty. Foundation course waiver is made at the discretion of the Graduate School of Business Administration and are recorded on the student's degree plan.

Admission Test. Applicants may submit scores from either the Graduate Management Admission Test (GMAT) or Graduate Record Examination (GRE) to strengthen their application.

Additional Application Materials. Students must submit a personal goal statement and resume. The two letters of recommendation are optional and may be submitted for additional consideration.

Expected Software Skills. EDBA students are expected to be proficient with word processing, spreadsheet and presentation programs such as Microsoft Word, Excel and PowerPoint. If students are deficient in any of these skills, it is their responsibility to mitigate the deficiency before enrolling in the program.

5.c. New Applications

Applications for admission should be made online through the University of Colorado Colorado Springs Office of Admissions' graduate application. The complete application must include:

1. The graduate application.
2. Official transcripts from degree-granting institutions. Additional transcripts may be required to verify prerequisites or major coursework. A final official transcript from degree-granting institution must be verified.
3. A nonrefundable application processing fee.
4. (Optional) Test scores, letters of reference, and other materials as required by specific department/program/school/college.
5. For international applicants, a score on the TOEFL, IELTS, or an equivalent to use an alternative proof of language proficiency and proof of financial support.

5.d. Provisional Admission

An applicant not meeting the criteria for admission as a regular degree student may be recommended by the faculty for admission as a provisional student. The recommendation for admission as a provisional student must include a letter from the school stating the conditions which the student must meet in order to become a regular degree student.

6. Curriculum Description

This section provides the program requirements, program curriculum along with a sample curriculum.

6a. Program Requirements

The three-year part time EDBA-Cyber program will be an accredited program and the curriculum will meet the Association to Advance Collegiate Schools of Business (AACSB International) standards (see section 7a). The students will earn a Doctor of Business Administration in Cybersecurity Management degree with mode of delivery as an Executive format. The program's instruction will follow blended learning approach involving a combination of in-person lectures, online learning, discussions and seminars. The program will involve limited residency cohorts. The program focuses not only on providing cybersecurity foundations critical for practice but also emphasizes scientific research skills and applied, evidence-based analysis and rigorous evaluation of complex issues.

The EDBA-Cyber requires satisfactory completion of the 60 credits of coursework and dissertation research. The program involves five components of Cybersecurity Foundations (9 credits), Business Knowledge (12 credits), Research Methods (9 credits), Cybersecurity Research (12 credits), and Dissertation (18 credits). The students will complete 24 credits in year 1, 18 credits in year 2, and 18 credits in year 3. The students have to successfully complete dissertation proposal in order to advance to degree candidacy. All students are required to successfully complete their dissertation on cybersecurity management topics.

6b. Program Curriculum

The program curriculum is presented below. The description of all courses included in the curriculum is provided in the Appendix B.

Cybersecurity Foundations (9 credits)

INFS 6110 Fundamentals of Cybersecurity Technologies (3 credits)
INFS 6120 Enterprise Information Security (3 credits)
INFS 6130 Cybersecurity Governance (3 credits)

Business Knowledge (12 credits)

(Choose any four)
MGMT 6200 Managing Organizational Development, Change and Transformation (3 credits)
(New course, MGMT 7xxx) Organizational Theory and Research: Implications for Cybersecurity (3 credits)
(New course, MKTG 7xxx) Digital Strategy and Innovation (3 credits)
(New course, STRT 7xxx) Strategic Management (3 credits)
LEAD 8300 Leadership Excellence in Complex Organizations (3 credits)

Research Methods (9 credits)

LEAD 7100 Intermediate Quantitative Research and Statistics (3 credits)
LEAD 7150 Intermediate Qualitative Research (3 credits)
LEAD 8100 Advanced Quantitative Research and Statistics (3 credits)

Cybersecurity Research (12 credits)

(New course, QUAN 7xxx) Principles of Scientific Inquiry (3 credits)
(New course, INFS 7xxx) Research Seminar in Information Security Management (3 credits)
(New course, INFS 7xxx) Research Seminar in Information Privacy (3 credits)
(New course, INFS 7xxx) Research Project (3 credits)

Dissertation (18 credits)

(New course) Dissertation[1] (3 - 9 credits)
[1]Students should repeat this course up to required number of credits required

6c. Sample Curriculum

The sample program curriculum is provided in table below.

Table 3. Program Schedule

Semester	Year 1	Year 2	Year 3
Semester 1 (Fall)	INFS 6110 Fundamentals of Cybersecurity Technologies	LEAD 8300 Leadership Excellence in Complex Organizations, OR STRT 7xxx Strategic Management	Dissertation
	MKTG 7xxx Digital Strategy and Innovation	(New) Research Seminar in InfoSec Management	
	(Online) MGMT 6200 Managing Organizational Development, Change		
Semester 2 (Spring)	LEAD 7100 Intermediate Quantitative Research and Statistics	LEAD 8100 Advanced Quantitative Research and Statistics	Dissertation
	MGMT 7xxx Organizational Theory and Research	(New) Research Seminar in Information Privacy	
	(Online) INFS 6120 Enterprise Information Security		
Semester 3 (Summer)	(New) Principles of Scientific Inquiry	LEAD 7150 Intermediate Qualitative Research	Dissertation
	INFS 6130 Cybersecurity Governance	(New) Research Project	
Color Legend:			
Cybersecurity Foundations	Business Knowledge	Research Methods	Doctoral Research

7. Professional Requirements or Evaluations

This section provides information regarding professional Accrediting and associated timetable.

7a. Professional Accrediting

All degree programs in the UCCS College of Business have to abide by AACSB International accreditation, which is synonymous with highest standards of excellence in business education. The AACSB accreditation defines a set of rigorous criteria and standards, coordinating peer reviews and consultation, and recognizing high-quality business schools. The 15 standards are organized into four categories: strategic management and innovation; participants—students,

faculty, and professional staff; learning and teaching; and academic and professional engagement. The standards are built around the three themes of engagement, innovation, and impact. These themes are integrated throughout the standards to challenge and assist schools in striving for continuous quality improvement.

There is no additional professional accreditation requirement for the EDBA-Cyber program. We plan to voluntary apply for membership to the Executive DBA Council. The Council is an international association of thirty-five programs with a presence in thirteen countries. The Executive DBA Council was founded in 2011 with a mission to foster excellence and innovation in executive doctoral degree programs worldwide. The UCCS EDBA-Cyber program curriculum is influenced by the program guidelines provided by the Executive DBA Council. In particular, the guidelines effected the three-year length of the program, limited residency cohorts, mix of business and research courses, no comprehensive examination, and requirement of defense of the dissertation.

7b. Timetable

Upon approval of the EDBA-Cyber program by the University of Colorado Board of Regents, we will notify the Higher Learning Commission and AACSB International. We anticipate about 3 months to receive formal approval letter. The voluntary membership for the Executive DBA Council will take about 2 months for the approval and listing of the program.

7c. Qualifications of Faculty

All faculty teaching in the EDBA-Cyber program will possess terminal degrees (PhD) in their respective fields. The faculty teaching doctoral research courses and supervising doctoral student research will be active in cybersecurity research demonstrated through research publications in peer-reviewed journals.

8. Institutional Factors

This section addresses potential impact on other instructional, research or service programs; coordination with other UCCS programs; and, formal relationships with other parties.

8a. Impact on other instructional, research or service programs

There is no impact on other instructional, research or service programs. The UCCS College of Business does not offer any doctoral program. The College of Engineering and Applied Sciences offers a PhD program in Security focused on technical aspects of cybersecurity. As mentioned in section 4, there is no EDBA program (general or cybersecurity) in the State of Colorado.

The EDBA-Cyber program will utilize existing classroom, laboratory, faculty and student space available to the College of Business in Dwire Hall. The program will involve limited residency cohorts delivered on Friday, Saturday and Sunday. The College of Business does not offer regular

undergraduate or graduate courses during these days. The program classes will take advantage of unutilized classroom and other space in the Dwire Hall. The library already subscribes to journals and research databases that will be required for students in the EDBA-Cyber program.

8b. Coordination with other UCCS programs

The proposed EDBA-Cyber will coordinate with other graduate programs at UCCS and across CU system to develop a pathway for students graduating from these programs and offer them a career advancement pathway to purse doctoral education and become cybersecurity leaders.

8c. Formal relationships with other parties

Not applicable.

9. Physical Capacity & Needs

This section provides information regarding space requirements and program delivery.

9a. Space Requirements

The EDBA-Cyber program will utilize existing classroom, laboratory, faculty and student space available to the College of Business in Dwire Hall. The program's instruction will follow blended learning approach involving a combination of traditional face-to-face lectures, online learning, discussions and seminars. The program will involve limited residency cohorts delivered on Friday, Saturday and Sunday. The College of Business does not offer regular undergraduate or graduate courses during these days. The program classes will take advantage of unutilized classroom and other space in the Dwire Hall.

9b. Program Delivery

The program does not require any additional space other than already available to the College of Business. The classes will be offered on Friday, Saturday and Sunday of select weeks. This will enable use of unutilized classroom and other space currently available in the Dwire Hall. In terms of staffing, the admissions and other student support can be handled by existing staff.

Regarding faculty, we plan to readjust qualified faculty with terminal degrees (PhD) from undergraduate program to teach in the EDBA-Cyber program. We will hire adjunct faculty to teach necessary courses at the undergraduate level. The revenues generated from the cybersecurity program can help cover the costs associated with the hiring of adjunct faculty. Additionally, qualified faculty from other University of Colorado campuses may be considered to teach cybersecurity foundations, business knowledge or research method courses.

10. Cost Description and Source of Funds

a. **Financial Pro-Forma**
   Please see attached Pro-forma in the Appendix C.

b. Program Costs
Please see attached pro-forma

c. Written Statement from the Dean
To be update

11. Other Relevant Information

Not applicable

APPENDIX A. Estimated Enrollment and Degree Completions

We plan to cap the program at 20 students per cohort. For initial years, our aim is to enroll 10 students in year 1, followed by 15 students in year 2, and 20 students in year 3. Subsequently, we will enroll maximum 20 students per year to ensure quality supervision and faculty availability for each student in the program.

- Cohort 1: 10 students
- Cohort 2: 15 students
- Cohort 3: 20 students
- Cohort 4: 20 students

The FTE calculations in the table A.1 are based on the Colorado Commission on Higher Education Full-time Equivalent (FTE) Reporting Guidelines and Procedures (April 2019).

Table A.1 Estimated Enrollment and Degree Completions

	Year 1	Year 2	Year 3	Year 4	Year 5	Full Implementation
Resident Headcount	6	14	24	28	30	30
Nonresident Headcount	4	11	21	27	30	30
Total Headcount	10	25	45	55	60	60
Resident FTE (credits)	6	12.5	20.5	23.5	25	600
Nonresident FTE (credits)	4	10	18.25	22.75	25	600
Total FTE (credits)	10	22.5	38.75	46.25	50	1200
Degrees Awarded	0	0	10	15	20	20

APPENDIX B. Course Descriptions

INFS 6110 – Fundamentals of Cybersecurity Technologies (3 credits)
This course will examine fundamental cyber security technologies that are needed to ensure protection of critical information systems. The focus will be on the technical aspects of cybersecurity. We will discuss cryptography, operating systems security, application security, and network security. The course content also includes topics of principles of computer security, user authentication, access control, malicious software, denial-of-service attacks, intrusion detection, firewalls and Intrusion Prevention Systems. *Prerequisites:* Graduate students only.

INFS 6120 – Enterprise Information Security (3 credits)
This course will provide an understanding to effectively implement the information security vision and strategy set forth by the executive management. The emphasis will be on cybersecurity management including information security policy and development of security program. The course focuses on establishing security processes, information security standards, risk management (models), business continuity, contingency planning tools, and SETA (security education, training and awareness). *Prerequisites:* Graduate students only.

INFS 6130 Cybersecurity Governance
This course will investigate the challenges and opportunities of effectively governing an organization's information security requirements and resources. Cybersecurity governance lays out the vision for the cybersecurity program. This course will discuss what constitutes good cybersecurity governance, and development of an effective security strategy and policy. We will also focus on how to improve information security accountability and maturity. *Prerequisites:* INFS 6110, INFS 6120, Graduate students only.

INFS 6140 Cybersecurity Law and Cybercrime Investigation
This course examines the data security and privacy laws and regulations that govern the collection, use, storage, and destruction of sensitive information. An understanding of these laws can help a cybersecurity expert understand how organizations can implement a program that will minimize legal and business risks. Students enrolled in this course will also learn about the nature of cybercrime, methods of investigating cybercrime, securing the crime scene, and collecting evidence of cybercrime. Students will explore the challenges involved with international cooperation in pursuing cybercrime offenders, and problems of enforcement between different international legal systems. *Prerequisites:* Graduate students only.

INFS 7120 Research Seminar in Information Security Management (3 credits)
This course examines the philosophical and theoretical foundations of information systems security. The focus is on understanding distinctive research orientations regarding information security in organizations. The goal of the course is to provide an intellectual foundation for students to develop an appropriate research program in this area. *Prerequisites:* INFS 6120, INFS 6130, QUAN 7110

INFS 7130 Research Seminar in Information Privacy (3 credits)
This course examines the privacy issues regarding information systems. The focus is on understanding distinctive research orientations regarding information privacy. Discussions will emphasize critical evaluation of theoretical foundations of privacy in our modern technologically based society. The goal of the course is to provide an intellectual foundation for students to develop an appropriate research program in this area. *Prerequisites:* INFS 6110, QUAN 7110

INFS 7190 Research Project (3 credits)
This course focuses on developing a conceptual paper in an area of interest in information security. It aims to provide students with a mentored, structured approach to develop critical skills required for dissertation. Students will apply the concepts, theories and methods learned in various courses. The paper may include plan for data collection and analysis. This preliminary research paper can serve as a basis for the dissertation proposal. *Prerequisites:* INFS 7120, INFS 7130

INFS 8110 Dissertation (3 - 9 credits)
This course is designed to guide the students through various stages of the dissertation process beginning with the development of a proposal and ending with a successful dissertation defense. Students may repeat this course to meet the necessary requirements. *Prerequisites:* Instructor approval (program director or dissertation chair)

LEAD 7100 - Intermediate Quantitative Research and Statistics (3 credits)
Students learn and apply advanced methods of analyzing data with an emphasis on the use and interpretation of descriptive and inferential techniques. Topics covered include repeated measures ANOVA, power, multiple correlation, and regression, ANCOVA, MANCOVA, Factor Analysis, and selected packaged statistical programs. Open to Phd students only. *Prerequisites:* Introduction to Statistics or equivalent.

LEAD 7150 Intermediate Qualitative Research (3 credits)
Identify and discuss differing philosophical orientations in respect to knowledge and inquiry among qualitative researchers. Study traditions of qualitative research that have evolved within disciplines of anthropology, sociology, psychology, and organizational theory and critique various qualitative studies. Develop competency in various techniques for gathering, analyzing, and reporting qualitative data. Open to PhD students only. *Prerequisites:* Introduction to Statistics or equivalent.

LEAD 8100 - Advanced Quantitative Research and Statistics (3cr)
Advanced methods of developing and analyzing complex data sets through the application of appropriate statistical measures, including time series analysis, SEM, and HLM; and develop skills to conduct and submit critical analyses of published research studies. Students also design, implement, and conduct research projects followed by the completion of professional-level research reports. Open to PhD students only. *Prerequisites:* Intermediate Quantitative Research and Statistics or equivalent.

LEAD 8300 Leadership Excellence in Complex Organizations (3 credits)
Analyzes organizational metaphors and their application to complex organizations. Examines various theories on organizations and the role of process, structure, and communication in organizational effectiveness. Investigates the relationship between and among various systems. Students apply knowledge of adult human development and systems theory to organizational development and strategic planning. Open to PhD students only.

MGMT 6200 Managing Organizational Development, Change and Transformation (3 credits)
In an environment of dynamic, non-stop change and increasing competition, organizations that have the best skills in developing healthy, high-performance organizations and managing change will have a competitive advantage. People who are trained in these skills can significantly increase their value to organizations. Course provides sound theory and practical training in how to successfully manage change, develop high-performing individuals, teams, and organizations, and transform organizations. *Prerequisites:* MGMT 6000.

MGMT 7xxx Organizational Theory and Research: Implications for Cybersecurity (3 credits)
This course bridges organizational theory and research with the applied needs of contemporary cybersecurity professionals. The primary goal of this course is to survey the classical and contemporary theoretical perspectives and issues studied in organizational research. It provides a broad overview of the major theoretical debates within organization theory, and how they have influenced research in more applied fields. The overarching goal is to provide students with resources derived from organizational theory and research that will help develop innovative solutions to the multifaceted challenges inherent in the cybersecurity industry.

MKTG 7xxx Digital Strategy and Innovation (3 credits)
We are now living in a new era of business practice, value creation and delivery. Understanding the changes relevant in the research, design, and execution of digital business is only becoming more important for present and future managers. Whether the context is an existing business trying to figure out how to offer value in the transition to digital or a new, digital native business designing their value delivery and growth strategy, it is imperative to understand this new landscape. This class offers students the opportunity to become more familiar with digital business strategy and innovation through a close look at, 1) digital business models and revenue structures, 2) how to design and conduct a digital-business opportunity analysis, 3) how to create and deliver value through digital marketing channels, and 4) the unique parameters and tools for online growth. The students will develop the ability to evaluate research concerning the structural and strategic options for creating a digital business. *Prerequisites:* Graduate business students only.

QUAN 7110 Principles of Scientific Inquiry (3 credits)
This course explores the philosophy of science and applied scholarly research. It introduces the principles of scientific research along with different research paradigms. We discuss positivist, interpretive and critical research perspectives. Students will learn about design science research and its relevance to information security. The course also examines the effectiveness of various research approaches. *Prerequisites:* Graduate business students only.

STRT 7xxx Strategic Management (3 credits)
The drivers of competitive advantage have changed as the pace of innovation has accelerated. Traditional defensive tactics such as cornering the market for key material resources, or securing legally defensible property rights, offer little protection against hacking, espionage, and theft of intellectual property in this new information economy. Knowledge, discovery, innovation, and technology are the essential competitive resources for the modern era. However, this transition to a new form of competitive dominance based on information power creates new opportunities and challenges for managers of organizations. This course offers an orientation to strategic management issues surrounding technology, and the attainment of competitive advantage through information-based power. It provides an introduction to work in the field of strategic management. The students will learn about different theoretical approaches to strategy research that are based on different disciplines. Students will also explore different areas of strategy research including corporate governance, global strategy, and organizational design. *Prerequisites:* Graduate business students only.

APPENDIX C. Financial Pro-Forma and Program Costs

Table C.1 Revenue/Expenditure Estimates

	Year 0[1]	Year 1	Year 2	Year 3	Year 4	Year 5
Projected Revenues						
Resident Tuition Revenue	0	119,424	248,800	408,032	467,744	497,600
Nonresident Tuition Revenue	0	134,144	335,360	612,032	762,944	838,400
Fee Revenue	900	4,200	9,000	12,000	13,500	13,500
Total Tuition & Fee Revenue	900	257,768	593,160	1,032,064	1,244,188	1,349,500
Institutional Investment	0	0	0	0	0	0
Other Revenues	0	0	0	0	0	0
Institutional reallocation (explain)	0	0	0	0	0	0
TOTAL PROGRAM REVENUE	**900**	**593,160**	**593,160**	**1,032,064**	**1,244,188**	**1,349,500**
Start up Costs[1]						
Capital Construction	0	0	0	0	0	0
Equipment Acquisitions	0	0	0	0	0	0
Library Acquisitons	3,000	4,000	4,100	4,200	4,300	4,400
Other (Marketing)	20,000	20,000	20,000	20,000	20,000	20,000
Projected Expenditures						
Tenured/Tenure Track Faculty*	0	0	8,000	56,000	56,000	56,000
Non-Tenure Track Faculty	0	0	0	0	0	0
Financial Aid specific to program	0	0	0	0	0	0
Program Administration	20,000	21,000	22,000	23,000	24,000	25,000
Instructional Materials	0	6,000	6,000	6,000	6,000	6,000
Equipment/Supplies	3,000	4,000	5,000	5,000	5,000	5,000
Campus Overhead[2]	2,000	3,000	4000	5,000	5,000	5,000
Fee Expenses	3,000	3,000	3,000	3,000	3,000	3,000
Other Operating	2,500	3,000	3,500	4,000	4,000	4,000
TOTAL PROGRAM EXPENSES	**53500**	**64000**	**75600**	**126200**	**127300**	**128400**
NET REVENUE	**-52600**	**529,160**	**517,560**	**905,864**	**1,116,888**	**1,221,100**

[1] Costs that occur prior to enrolling students should be entered in the "Year 0" column.

[2] If no campus overhead, explain.

* Year 2: 1 course overload; Year 3 onwards: 7 course overloads per year

Assumptions

a. 7 course overloads per year = 1 research project, 3 dissertation courses supervising 10 students
b. Revenues have been calculated based on College of Business Graduate Tuition Rate for Residents as $2488 and Non-residents as $4192.

University of Colorado
Colorado Springs

Proposal for
MASTER OF BUSINESS ADMINISTRATION
EMPHASIS AREA: CYBERSECURITY MANAGEMENT

October 2019

Table of Contents

1. Program description

The Master of Business Administration (MBA) provides a broad curriculum preparing students for a variety of options in launching their career. It is designed to meet the needs of students with or without previous business education. The UCCS MBA program is devoted to the concepts, analytical tools, and communication skills required for competent and responsible management. The management of an enterprise is viewed in its entirety and within its social, political, and economic environment. We are proposing to build on the existing MBA program and add a new area of emphasis in Cybersecurity Management involving four courses.

The proposed new area of emphasis in Cybersecurity Management will provide professionals with foundations in the fundamental business disciplines along with a comprehensive understanding of cybersecurity concepts and technologies. Data breaches and cyber threats create significant risks for organizations dependent upon sensitive information. This area of emphasis will enhance students' understanding about complexities involved with the adoption of security technologies, achieving regulatory compliance, and implementing cybersecurity program to mitigate risks and secure information assets. Overall, the program will enable professionals to effectively govern cybersecurity in an organization.

1.a. Student Learning Outcomes

The proposed new Cybersecurity Management area of emphasis will follow existing student learning outcomes for existing MBA program offered by the UCCS College of Business.

2. Workforce and Student Demand

This section presents workforce and student demand in cybersecurity management.

2a. Workforce demand

According to Burning Glass, cybersecurity jobs account for 13% of all IT jobs. The demand for cybersecurity skills has risen 255% since 2013, while demand for risk management rose by 133%. Employer demand for cybersecurity professionals across the United States continues to accelerate with the knowledge of public cloud security (170%) projected to be the fastest-growing cybersecurity skill in demand. According to CyberSeek, a project supported by the National Initiative for Cybersecurity Education (NICE), a program of the NIST in the U.S. Department of Commerce, there are 313,735 cybersecurity jobs openings across US, while 780,000 people were employed in various cybersecurity positions.

The Bureau of Labor Statistics estimates that employment of Information Security Analysts is projected to grow by 32% from 2018 to 2028, much faster than the average for all occupations. Cybersecurity Ventures, Cybersecurity analytics and research company, predicts that there will be

3.5 million unfilled cybersecurity positions by 2021. Please refer to table 1 for current demand of cybersecurity jobs.

Table 1. Demand for Cybersecurity Management (Source: www.cyberseek.org)		
Role	**Job Openings**	**Average Salary**
Cybersecurity Job Openings in US	313,735	
Cybersecurity Analyst	26,013	$85,000
Cybersecurity Consultant	13,439	$100,00
IT Auditor	6,915	$86,000
Cybersecurity Manager or Administrator	14,320	$115,000
Chief Information Security Officer	5,130	$224,388

The State of Colorado has currently 10,207 job openings in cybersecurity (Source: www.cyberseek.org). The Colorado Springs region is home to 125-plus cybersecurity companies as well as five NSA/DHS Centers of Academic Excellence (CAEs) in cybersecurity education. UCCS is one of the designated CAE-Cyber Defense Education institutions. The total cybersecurity industry employment in Colorado Springs is 3,371 with a projected total demand forecast at 6,967 by 2025.

2b. Student demand

The proposed new Cybersecurity Management (MBA-Cyber) area of emphasis will target students who have completed their undergraduate degree and satisfied the prerequisites for admission to the program. The MBA-Cyber will recruit students from across the country with initial target of 10 states over three phases (see Table 2).

Table 2. Target States and Cybersecurity Job Openings (Source: Cyberseek.org)				
Phase	**State**	**CompTIA Security+ Certification Holders**	**Cybersecurity Job Openings**	**Total Job Openings**
I	Colorado	6,725	10,207	10,207
II	Arizona	3,530	7,867	48,090
	Florida	11,888	13,465	
	Nevada	1,566	1,923	
	Texas	13,407	24,835	
III	California	13,789	36,602	88,147
	Nebraska	1,284	2,026	
	North Carolina	5,997	13,078	
	Oregon	859	2,911	
	Virginia	24,894	33,530	

We plan to target holders of CompTIA Security+ certification, which is an entry level certification focused on low skills cybersecurity jobs. This certificate holders typically possess an undergraduate degree and are ideal candidates for the proposed MBA-Cyber program. The realistic enrollment projections for the MBA-Cyber program for the first five years can be found in Appendix A.

3. Role and Mission Criteria

The mission of the proposed Cybersecurity Management area of emphasis is aligned with the mission of the UCCS as well as the College of Business. The UCCS mission is to "be a comprehensive baccalaureate and specialized graduate research university…offer liberal arts and sciences, business, engineering…programs, and a selected number of master's and doctoral degree programs". The proposed MBA-Cyber program fulfills this mission by providing a unique professional graduate program for cybersecurity practitioners.

The mission of the College of Business includes offering "…select master's degrees and professional programs that emphasize principle-based ethical decision making…support innovation and impact in our teaching, research and service." The College realizes this mission by producing intellectual contributions that impact the theory, practice and teaching of business. The proposed MBA-Cyber program fulfills this mission by offering a unique professional graduate program focused on developing well-rounded cybersecurity management professionals. The program is innovative in nature blending cybersecurity fundamentals and knowledge with business courses providing strong foundations in managing different functions of organizations.

Further, the proposed MBA-Cyber is aligned with UCCS' priority focus on cybersecurity discipline and initiatives. The program also addresses three of the strategic themes (or core strategies) identified for the UCCS 2030 Strategic Plan:

I. Strategy 2: Enhance strategic enrollment and retention efforts to drive long-term stability and sustainability.
II. Strategy 5: Strengthen and expand revenue sources to ensure future growth and improve student affordability and access.
III. Strategy 6: Support competitive programs and initiatives, both existing and new, that show the university's unique value and identity in the higher-education landscape

4. Duplication

The proposed new MBA-Cyber area of emphasis does not duplicate any other program offered in the UC system. This new emphasis area is neither offered by the CU Boulder Leeds School of Business nor by the CU Denver School of Business. At UCCS, the College of Engineering and Applied Sciences (CEAS) offers Master of Engineering in Information Assurance (see UCCS catalog); however, CEAS website indicates offering a Master of Engineering in Cybersecurity

degree. These are technical cybersecurity degrees focused on producing (or training) cybersecurity engineers or technical professionals. In contrast, the proposed MBA-Cyber area of emphasis focuses on developing cybersecurity management professionals skilled at governing cybersecurity in an organization.

5. Statutory Requirements

The proposed MBA-Cyber area of emphasis will follow existing admission requirements for the College of Business MBA program. We are not proposing any changes to and plan to abide by the existing policies and requirements of College of Business and the UCCS Graduate School including admission requirements, transfer credits, new applications, and provisional admission.

6. Curriculum Description

This section provides the program requirements and program curriculum for the proposed MBA-Cyber area of emphasis.

6a. Program Requirements

The MBA at UCCS consists of 36 credit hours of graduate (6000-level) business coursework with 24 hours of core competency courses and 12 hours of electives. The applicants for MBA program should have completed coursework in accounting, economics and statistics as part of their undergraduate degree. If the above-mentioned courses were not completed, UCCS provides a series of three business foundation courses as required background courses to help develop competencies to be successful in the MBA program. Foundation courses may be waived based on prior academic work or through passing a waiver exam.

We are not proposing any changes to the existing MBA core, and are only proposing to add a Cybersecurity Management area of emphasis in lieu of elective courses. The existing MBA program already follows this approach by offering multiple areas of emphasis (such as accounting, finance and marketing) in lieu of elective courses. The MBA-Cyber area of emphasis will involve 24 hours of existing core competency courses and 12 hours of cybersecurity management courses (see Table 3).

Table 3. Degree Requirements for MBA with Cybersecurity Management Emphasis Area

Area	Credit Hours
MBA Core (*No changes*)	24
Cybersecurity Management Emphasis Area	12
TOTAL	36

6b. Program Curriculum

The MBA-Cyber program curriculum is presented below. The description of four new courses in the proposed Cybersecurity Management area of emphasis is provided in the Appendix B.

Core Courses (24 credits)

Core courses make up the heart of the MBA program and cover areas that are directly applicable in today's business world. The concepts in the following courses are the critical problem solving and decision-making skills that will define and shape MBA degree. All students complete the eight core courses as part of their MBA degree (see Table 4).

Table 4. Existing MBA Core Courses

Course Number	Course Title	Course Credits
STRT 6000	Strategic Foundations for Responsible Management	3
ACCT 6100	Accounting for Decision Making	3
FNCE 6000	Corporate Financial Management	3
INFS 6000	Information Systems	3
MGMT 6000	Leading & Managing in Changing Times	3
MKTG 6000	Marketing Strategy	3
OPTM 6000	Operations: Competing Through Capabilities	3
STRT 6500	Strategic Management	3

Cybersecurity Management Emphasis Area (12 credits)

The students pursuing this emphasis area are expected to complete four courses listed in table 5. The description of all courses is provided in the Appendix B.

Table 5. Proposed Cybersecurity Management Emphasis Courses

Course Number	Course Title	Course Credits
INFS 6110	Fundamentals of Cybersecurity Technologies	3
INFS 6120	Enterprise Information Security	3
INFS 6130	Cybersecurity Governance	3
INFS 6140	Cybersecurity Law and Cybercrime Investigation	3

7. Professional Requirements or Evaluations

This section provides information regarding professional Accrediting and associated timetable.

7a. Professional Accrediting

All degree programs in the UCCS College of Business have to abide by the AACSB accreditation. There is no additional professional accreditation requirement for the proposed MBA-Cyber program.

7b. Timetable

Upon approval of the MBA-Cyber program by the UCCS Administration and appropriate committees, we plan to start offering the MBA-Cyber area of emphasis from Fall 2020 onwards.

7c. Qualifications of Faculty

All faculty teaching in the MBA-Cyber program are expected to have terminal degrees (PhD) in their respective fields. Currently, the College of Business have following faculty expertise in cybersecurity area:

- Gurvirender Tejay, Ph.D.
- Morgan Shepherd, Ph.D.
- Bob Cook (Instructor)

Further, we plan to engage qualified cybersecurity professionals with terminal degrees as adjuncts or instructors for the program as needed.

8. Institutional Factors

This section addresses potential impact on other instructional, research or service programs; coordination with other UCCS programs; and, formal relationships with other parties.

8a. Impact on other instructional, research or service programs

There is no impact on other instructional, research or service programs. The proposed MBA with Cybersecurity Management area of emphasis does not duplicate any other program offered in the UC system. The College of Engineering and Applied Sciences (CEAS) offers Master of Engineering in Information Assurance (see UCCS catalog); however, CEAS website indicates offering Master of Engineering in Cybersecurity. These are technical cybersecurity degrees focused on producing (or training) cybersecurity engineers or technical professionals. In contrast, the proposed MBA-Cyber emphasis area focuses on developing cybersecurity management professionals skilled at governing cybersecurity in an organization.

The MBA-Cyber program will utilize existing classroom, laboratory, faculty and student space available to the College of Business in the Dwire Hall. The program will be delivered primarily online and will utilize existing technical infrastructure.

8b. Coordination with other UCCS programs

The proposed MBA-Cyber will coordinate with other undergraduate programs at UCCS and across CU system to develop a pathway for students graduating from these programs and offer them a career advancement pathway to purse graduate education and become cybersecurity management professionals.

8c. Formal relationships with other parties

Not applicable.

9. Physical Capacity & Needs

This section provides information regarding space requirements and program delivery.

9a. Space Requirements

The MBA-Cyber program will utilize existing classroom, laboratory, faculty and student space available to the College of Business in Dwire Hall. The program will be delivered primarily online and will utilize existing technical infrastructure.

9b. Program Delivery

The program does not require any additional space other than already available to the College of Business. In terms of staffing, the admissions and other student support can be handled by existing staff. Regarding faculty, we plan to readjust qualified faculty with terminal degrees (PhD) from undergraduate program to teach in the MBA-Cyber program.

The College of Business have following faculty expertise in cybersecurity area:

- Gurvirender Tejay, Ph.D.
- Morgan Shepherd, Ph.D.
- Bob Cook (Instructor)

Further, we plan to engage qualified cybersecurity professionals with terminal degrees as adjunct faculty or instructors for the program on need basis.

10. Required Resources

In terms of staffing, the admissions and other student support can be handled by existing staff at the College of Business. Regarding faculty, we plan to readjust qualified faculty with terminal degrees (PhD) from undergraduate program to teach in the MBA-Cyber program. Further, we plan

to engage qualified cybersecurity professionals with terminal degrees as adjunct faculty or instructors for the program on a need basis.

The College of Business currently has a need for more online elective course offerings. The COB will offer the MBA Cybersecurity Management courses as electives and use the current instructional resource budget to fund the sections (either through current faculty [both on-load and over-loads]; or adjuncts). Resources for additional funding may also be procured through grants.

APPENDIX A. Estimated Enrollment and Degree Completions

For initial years, our aim is to enroll 10 students in year 1, followed by 15 students in year 2, 20 students in year 3, 25 students in year 4, and 30 students in year 5. The FTE calculations in the Table A.1 are based on the Colorado Commission on Higher Education Full-time Equivalent (FTE) Reporting Guidelines and Procedures (April 2019).

Table A.1 Estimated Enrollment and Degree Completions

	Year 1	Year 2	Year 3	Year 4	Year 5
Resident Headcount	6	14	18	22	26
Nonresident Headcount	4	11	17	23	29
Total Headcount	10	25	35	45	55
Resident FTE (credits)	4.5	10.5	13.5	16.5	17.25
Nonresident FTE (credits)	3	8.25	12.75	17.25	19.5
Total FTE (credits)	7.5	18.75	26.25	33.75	41.25
Degrees Awarded	0	10	15	20	25

APPENDIX B. Course Descriptions

INFS 6110 Fundamentals of Cybersecurity Technologies (3 credits)
This course will examine fundamental cyber security technologies that are needed to ensure protection of critical information systems. The focus will be on the technical aspects of cybersecurity. We will discuss cryptography, operating systems security, application security, and network security. The course content also includes topics of principles of computer security, user authentication, access control, malicious software, denial-of-service attacks, intrusion detection, firewalls and Intrusion Prevention Systems. *Prerequisites:* Graduate students only.

INFS 6120 Enterprise Information Security (3 credits)
This course will provide an understanding to effectively implement the information security vision and strategy set forth by the executive management. The emphasis will be on cybersecurity management including information security policy and development of security program. The course focuses on establishing security processes, information security standards, risk management (models), business continuity, contingency planning tools, and SETA (security education, training and awareness). *Prerequisites:* Graduate students only.

INFS 6130 Cybersecurity Governance
This course will investigate the challenges and opportunities of effectively governing an organization's information security requirements and resources. Cybersecurity governance lays out the vision for the cybersecurity program. This course will discuss what constitutes good cybersecurity governance, and development of an effective security strategy and policy. We will also focus on how to improve information security accountability and maturity. *Prerequisites:* INFS 6110, INFS 6120, Graduate students only.

INFS 6140 Cybersecurity Law and Cybercrime Investigation
This course examines the data security and privacy laws and regulations that govern the collection, use, storage, and destruction of sensitive information. An understanding of these laws can help a cybersecurity expert understand how organizations can implement a program that will minimize legal and business risks. Students enrolled in this course will also learn about the nature of cybercrime, methods of investigating cybercrime, securing the crime scene, and collecting evidence of cybercrime. Students will explore the challenges involved with international cooperation in pursuing cybercrime offenders, and problems of enforcement between different international legal systems. *Prerequisites:* Graduate students only.

Certificate Approval Form

PART I

1. **Name of Certificate**: Graduate Certificate in Cybersecurity Management

2. **Department(s):** Business Analysis

3. **College(s)/Institutions**: College of Business

4. **Faculty Director/Advisor**: Ying Fan, Ph.D. / Gurvirender Tejay, Ph.D.

5. **Type of Certificate**: Gainful Employment

6. **Expected start date** (semester and year): Fall 2020

7. **Number of required credit hours**: 12 credit hours

8. **Anticipated length of the program in semesters including summer**:
   8 months (2 semesters) – 18 months (4 semesters)

9. **Describe the certificate program**.
   a. **How the certificate program fits the unit's role and mission.**

      The mission of the College of Business includes offering "…select master's degrees and professional programs that emphasize principle-based ethical decision making…support innovation and impact in our teaching, research and service." The Graduate Certificate in Cybersecurity Management will provide professionals with comprehensive understanding of cybersecurity concepts and technologies.

      This Certificate requires the same series of four cybersecurity classes as the Cybersecurity Management Area of Emphasis in our Master of Business Administration program. The Certificate is intended for students that want to study Cybersecurity Management but do not want to pursue a full master's degree.

   b. Courses and requirements (e.g., minimum grades) to complete the certificate.

      The certificate will require completion of 12 credits. These courses include:
      1. INFS 6110 - Fundamentals of Cybersecurity Technologies (3 credits)
      2. INFS 6120 - Enterprise Information Security (3 credits)

3. INFS 6130 - Cybersecurity Governance (3 credits)
4. INFS 6140 - Cybersecurity Law and Cybercrime Investigation (3 credits)

c. Admission criteria (at a minimum must follow criteria delineated in policy but program may have higher standards)

Bachelor's degree from a regionally accredited university with a cumulative grade point average of 3.0 or better.

d. **The exit process.**

Students need to complete required courses with requisite grades as per UCCS policy. In order to graduate, the Graduate Certificate in Cybersecurity Management completion form has to be signed by the Director of Graduate Programs and Dean, Graduate School of Business Administration.

e. **Costs of offering the certificate program**.

The proposed certificate will be offered utilizing existing faculty and resources at the College of Business. Further, the required courses for the Certificate are the same series of four cybersecurity classes as the Cybersecurity Management Area of Emphasis in our Master of Business Administration program.

f. **Expected benefits, income, return on investment**.

Students successfully completing the program will be awarded UCCS Graduate Certificate in Cybersecurity Management. The certificate trains students for mid-level and advance-level cybersecurity roles of cybersecurity analyst, cybersecurity consultant, IT Auditor, and Cybersecurity Manager. Depending upon experience, skills and location, graduating students can expect to attain average salary of $85,000 to $115,000 (see Table 1). There are significant job openings in cybersecurity as listed in table 1.

Table 1. Cybersecurity Roles, Job Openings & Salary (Source: Cyberseek.org)

Skill-level	**Role**	**Job Openings**	**Average Salary**
Mid-level	Cybersecurity Analyst	26,013	$85,000
Mid-level	Cybersecurity Consultant	13,439	$100,00
Mid-level	IT Auditor	6,915	$86,000
Advance-level	Cybersecurity Manager	14,320	$115,000

g. **If applicable, describe any fees (e.g., program, course, application) that you will charge**. (Note: You will need to follow campus procedures for fees.)

The fees involved include the application processing fee of $60, and online fee of $100 per course.

h. **If you are proposing a non-notated certificate, please explain why this is the best type of certificate and why you are not using a CoS or PD certificate. Please submit a plan for how you will inform students that the certificate will not be notated on official university transcripts**.

Not applicable.

PART II (for GE Certificates)

1. **Program website URL for certificate program**:

https://www.uccs.edu/business/programs/masters/graduate-business-certificates

2. **Provide a narrative description of how the institution determined the need for the program**.

According to Burning Glass, the demand for cybersecurity skills has risen 255% since 2013, while demand for risk management rose by 133%. Employer demand for cybersecurity professionals across the United States continues to accelerate. According to CyberSeek, program of NIST, there are 313,735 cybersecurity jobs openings across U.S. The Bureau of Labor Statistics estimates that employment of Information Security Analysts is projected to grow by 32% from 2018 to 2028, much faster than the average for all occupations. Please refer to table 1 for current demand and average salary for cybersecurity jobs.

3. **Provide a narrative description of how the program was designed to meet local market needs, or for an online program, regional or national market needs**.

We used data from Bureau of Labor Statistics, Burning Glass and CyberSeek (program of NICE and NIST) to determine demand for cybersecurity management skills and roles. The graduate certificate program was designed to address these cybersecurity skills in demand. For the state of Colorado, there is high demand for cybersecurity skills and low supply of trained professionals. There are currently 10,207 cybersecurity job openings. For the industry certifications of CISM

(Security Manager) and CISA (IT Auditor), there is current shortage of 543 and 558 cybersecurity professionals. The program content was developed by faculty members with expertise in cybersecurity management and information systems.

4. **Provide a narrative description of any wage analysis the institution may have performed, including any consideration of Bureau of Labor Statistics wage data related to the new program.**

The wage analysis was performed based on data from Bureau of Labor Statistics, Burning Glass and CyberSeek (program of NIST, US Department of Commerce). Please see section 9.f of Part I.

5. **Was the program reviewed and approved by any external groups**?

Business that would likely employ graduates of the program

6. **Provide a narrative description of how the program was reviewed or approved by, or developed in conjunction with, the entities selected in #5**. **For example, describe the steps taken to develop the program, identify when and with whom discussions were held, provide relevant details of any proposals or correspondence generated, and/or describe any process used to evaluate the program. The institution must retain, for review and submission to the appropriate federal agencies upon request, copies of meeting minutes, correspondence, proposals, or other documentation to support the development, review, and/or approval of the program.**

The program content was developed by faculty members with expertise in cybersecurity management and information systems. The faculty member used past experience in cybersecurity program development along with information on required cybersecurity skills and competencies from 'Oversee and Govern' category of NICE framework (NIST SP 800-181) to develop the program and course content. The courses were also aligned with the subject matter covered in in-demand cybersecurity certifications of CISM, CRISC and CISA. The program was reviewed by two additional faculty members. Subsequently, the certificate program was reviewed and approved by the Department of Business Analysis.

7. **Describe how you will determine the on-time completion rate, job placement rate, and median loan debt in order to disclose the information on the departmental website**.

We will use an exit survey of graduating students and coordinate with the campus financial aid office and institutional research office to gather required data for reporting purposes. This certificate will typically be completed in 1 year.

8. **When do you intend to begin disbursing Title IV funds to students**: Fall 2020

9. **Estimate the cost of the program:**

	Per Term		Annual	
	Resident	**Non-resident (Online)**	**Resident**	**Non-resident (Online)**
Tuition and fees	$2588	$2753	$10,352	$11,012
Room and board	N/A	N/A	N/A	N/A
Books and supplies	$400	$400	$1,200	$1,200

Additional explanation of costs, if necessary (e.g., cost per credit hour):
There are three semester per year. To finish in one year, the student will need to take two courses during one of the terms, which is feasible to do.

10. **Using the Standard Occupational Classifications http://www.bls.gov/soc,**

a. **Select the primary occupational group for which the Gainful Employment Program will train the student:**

Information Technology

b. **List all six-digit codes that reflect occupations in which the graduates of the proposed program will be trained for employment:**
15-1122.00 - Information Security Analysts,
11-3021.00 - Computer and Information Systems Managers

CIP Code: 11.1003 Computer and Information Systems Security

11. Have you read the Gainful Employment regulations posted at http://www.ifap.ed.gov/GainfulEmploymentInfo/index.html and are you aware that failure to comply and failure to meet "gainfulness" could make your program ineligible for the Title IV financial aid on an annual basis?
Yes

Have you reviewed the regulations for any further requirements in the application?
Yes

Application fee waiver instructions in graduate school application

*

In order to submit your application the nonrefundable $60.00 application fee must be paid. Payment can be made by credit card or ACH electronic check. Please contact the Office of Admissions at 719-255-3084 or gradapp@uccs.edu if an alternate payment method is needed.

How would you like to pay your application fee?

- ○ I would like to pay now by credit card or ACH electronic check
- ○ Scholar Program Application Fee Waiver Options
- ○ Other Financial Need Based Application Fee Payment Options

<< Back | Save & Next >>

For Scholar Program:

*

In order to submit your application the nonrefundable $60.00 application fee must be paid. Payment can be made by credit card or ACH electronic check. Please contact the Office of Admissions at 719-255-3084 or gradapp@uccs.edu if an alternate payment method is needed.

How would you like to pay your application fee?

- ○ I would like to pay now by credit card or ACH electronic check
- ◉ Scholar Program Application Fee Waiver Options
- ○ Other Financial Need Based Application Fee Payment Options

*

If you were involved in one of the following scholar programs, you may be eligible for an application fee waiver. Please select the scholar program you are participating in.

- ○ Gates Millennium Scholars Program
- ○ GEM: National Consortium for Graduate Degrees for Minorities in Engineering and Science Program
- ◉ Maximizing Access to Research Careers (MARC) Program
- ○ PREP: Postbaccalaureate Research Education Program
- ○ Research Initiative for Scientific Enhancement (RISE) Program
- ○ The McNair Scholars Program: Ronald E. McNair Postbaccalaureate Achievement Program
- ○ TRIO Student Support Services (SSS) Program
- ○ Undergraduate Student Training in Academic Research (U-STAR) Program
- ○ Extended studies agreement EdAssist

*

The application fee waiver is only for the Scholar Program you selected above. You must upload a letter from the program coordinator at your undergraduate institution for verification. You may be contacted by the graduate admissions office if more information is needed for verification. Please select another payment option if you are not one of these Scholar Program participants.

Choose File | No file chosen

For Need Based Waiver or departmental waiver:

*

In order to submit your application the nonrefundable $60.00 application fee must be paid. Payment can be made by credit card or ACH electronic check. Please contact the Office of Admissions at 719-255-3084 or gradapp@uccs.edu if an alternate payment method is needed.

How would you like to pay your application fee?

- ○ I would like to pay now by credit card or ACH electronic check
- ○ Scholar Program Application Fee Waiver Options
- ◉ Other Financial Need Based Application Fee Payment Options

To qualify for a financial need application fee waiver, you must fall in to one of the following categories:
College seniors:
1. A dependent, who has Student Aid Report (SAR) that shows a parental contribution of not more than $2,500 for the senior year (submit a copy of the 1st page of your Student Aid Report) **or**
2. Self-supporting and have a Student Aid Report (SAR) that shows a contribution of not more than $3,000 for the senior year (submit a copy of the 1st page of your Student Aid Report) **or**
3. If you received a fee reduction voucher from ETS to take the GRE test, you qualify for an application fee waiver. Please send us a copy of the fee reduction voucher you received from ETS for the GRE test.

Unenrolled college graduates:
1. Have applied for financial aid, **and**
2. Have a Student Aid Report (SAR) that indicates self-supporting status and a contribution of not more than $3,000 (submit a copy of the 1st page of your SAR) **or**
3. If you received a fee reduction voucher from ETS to take the GRE test, you qualify for an application fee waiver. Please send us a copy of the fee reduction voucher you received from ETS for the GRE test.

If you believe you might be eligible for a financial need based application fee waiver based on the criteria above, please contact the Financial Aid office at finaidse@uccs.edu. If approved for a fee waiver, you will be provided a code to submit your application without payment.

If you do not meet any of the criteria listed above but would still like to pursue other application fee waiver options, please email the Office of Admissions at gradapp@uccs.edu to explain your circumstances. A graduate admissions staff member will contact you to discuss any other options and provide you with your next steps.

Alternate Payment Password
* (the Graduate School Office will provide this for you)