UTAH SYSTEM OF HIGHER EDUCATION
Building a Stronger State of Minds

State Board of Regents
Board of Regents Building, The Gateway
60 South 400 West
Salt Lake City, Utah 84101-1284

Phone 801.321.7101
Fax 801.321.7199
TDD 801.321.7130
www.higheredutah.org

July 6, 2016

MEMORANDUM

TO: State Board of Regents

FROM: David L. Buhler

SUBJECT: Utah Valley University – Master of Science in Cybersecurity

Issue

Utah Valley University (UVU) requests approval to offer a Master of Science in Cybersecurity effective Fall Semester, 2017. This proposal was approved by the institutional Board of Trustees March 30, 2016.

Background

Utah Valley University resides in a service area that is experiencing strong economic growth. The computer industry is a main economic driver within Utah County. As the computer industry evolves, the need for professionals prepared in cybersecurity is becoming increasingly apparent. Over the last few years, UVU has become a regional leader in preparing people for work within the cybersecurity sector. In 2012, UVU was awarded a three million dollar grant from the United States Department of Labor to train displaced workers in computer security issues. Today, UVU offers three bachelor's degrees with cybersecurity emphases and two certificates in cybersecurity including a certificate designed for individuals who currently possess a baccalaureate degree. The proposed master's degree program is the institution's next step in meeting the growing labor market demand for cybersecurity professionals.

The Master of Science in Cybersecurity is intended for individuals who desire to acquire additional cybersecurity knowledge, skills, and abilities in order to pursue new careers or to advance within an existing career. The program focuses on the managerial and technical perspectives of cybersecurity through extensive use of case-studies and hands-on lab exercises.

Cybersecurity jobs are available at a number of organizations from a wide variety of sectors. An October 2015 job search on the Indeed.com job aggregator showed over 150 cybersecurity/information security positions currently posted in Utah.

Cybersecurity is integral to most information technology occupations (e.g., network administration, database administration, information systems management, etc.). A worker who is qualified in cybersecurity could obtain employment within any of these occupational groups.

The Department of Workforce Services projects that Information Security Analysts, an occupational category that relates to UVU's proposed program, will experience a 5.1% growth rate in Utah with employees earning an annual median income of $78,590.

Policy Issues

The proposed program has been developed through established institutional procedures and Board of Regents policy. Chief academic officers as well as faculty in related departments from the Utah System of Higher Education institutions have reviewed the proposal and have provided input. There are no additional policy issues that need to be addressed relative to approval of the program.

Commissioner's Recommendation

The Commissioner recommends the Board of Regents approve the request from Utah Valley University to offer a Master of Science in Cybersecurity.

_____
David L. Buhler
Commissioner of Higher Education

DLB/BKC
Attachment

Utah Valley University
Master of Science in Cybersecurity

Section I: The Request

The Department of Information Systems and Technology in the College of Technology and Computing at Utah Valley University requests approval to offer a Master of Science in Cybersecurity effective Fall Semester, 2017. The UVU Board of Trustees approved this program March 30, 2016.

Section II: Program Description

Complete Program Description

The Master of Science in Cybersecurity is intended for individuals who desire to acquire additional cybersecurity knowledge, skills, and abilities in order to pursue new employment or to advance within existing careers in cybersecurity. The program is also designed for individuals who plan to pursue doctorate degrees in cybersecurity or related fields. The program focuses on the managerial and technical perspectives of cybersecurity through extensive use of case-studies and hands-on lab exercises.

Purpose of Degree

The federal government has made information security a national security and public safety issue. This is evident in the creation of the Cyber Threat Intelligence Integration Center;[1] a government center tasked with coordinating the response to cybersecurity threats and combating hackers. However, and despite the heightened realization of the importance of cybersecurity, industry reports continue to show that there is a severe shortage of skilled cybersecurity professionals.[2]

UVU is a regional leader in cybersecurity teaching and training. In 2012 the university was awarded a three million dollar grant from Department of Labor (DOL) to train displaced TAACCCT workers with the support of the Utah State Workforce Development Board. Today, UVU offers three bachelor's degrees and two certificates with cybersecurity emphases, including a one-year post-baccalaureate certificate.

The proposed program will provide students with a comprehensive education in cybersecurity, which will enhance their cybersecurity knowledge and skills and prepare them to address cybersecurity challenges in private and public sectors. The new program is designed to address a shortage of cybersecurity professionals and scholars at the National Security Agency's (NSA) Cybersecurity Data Center (CDC), the largest security data center in the world, and other employment deficits relevant to cybersecurity throughout Utah and the western United States.

Institutional Readiness

The proposed program will be administered by the Department of Information Systems & Technology (IST) within the College of Technology and Computing at Utah Valley University. A full-time faculty member will serve as the Director of Cybersecurity. The director will report to the IS&T Department Chair, who reports to the Dean of the College of Technology and Computing.

The Department of IST has three full-time faculty who are already qualified to support the proposed program. Two of these faculty were exclusively hired under the cybersecurity grant to develop curriculum for the various cybersecurity-related offerings, including a post-baccalaureate certificate in cybersecurity. The proposed master's degree is a natural expansion. The cybersecurity grant covered the salaries of these two faculty members through the 2014-2015 academic year with the university funding the positions thereafter. The IST

[1] https://www.whitehouse.gov/the-press-office/2015/02/25/presidential-memorandum-establishment-cyber-threat-intelligence-integrat
[2] http://www.isaca.org/Pages/Cybersecurity-Global-Status-Report.aspx

Department Chair and the College of Technology and Computing Dean are both qualified to teach some classes in this program.

None of these full-time faculty will be reassigned as they already teach cybersecurity courses at the undergraduate and graduate levels as part of the post-baccalaureate certificate in cybersecurity. However, as the program grows, it is projected that one full-time faculty position will be added. With an additional tenure-track position, there should not be any adverse impact on the undergraduate programs within the department.

The proposed graduate program may affect enrollments only in the IST Department. Specifically, the program may increase enrollments in lower-division IT courses for incoming graduate students who do not have bachelor's degrees in information technology or related fields. Such students will be required to complete some lower-division IT courses to be prepared for the graduate cybersecurity courses.

Courses will be delivered through face-to-face, hybrid, and online delivery methods. The particular delivery methods may vary based on the course content to achieve the best delivery for each specific course.

Departmental Faculty

Faculty Category	Faculty Headcount – Prior to Program Implementation	Faculty Additions to Support Program	Faculty Headcount at Full Program Implementation
With Doctoral Degrees (Including MFA and other terminal degrees, as specified by the institution)			
Full-time Tenured	2	1	3
Full-time Non-Tenured	4		4
Part-time Tenured			
Part-time Non-Tenured			
With Master's Degrees			
Full-time Tenured	6		6
Full-time Non-Tenured	4		4
Part-time Tenured			
Part-time Non-Tenured	2		2
With Bachelor's Degrees			
Full-time Tenured			
Full-time Non-Tenured			
Part-time Tenured			
Part-time Non-Tenured	6		6
Other			
Full-time Tenured			
Full-time Non-Tenured			
Part-time Tenured			
Part-time Non-Tenured	1		1
Total Headcount Faculty			

Full-time Tenured	8	1	9
Full-time Non-Tenured	8	0	8
Part-time Tenured	0		0
Part-time Non-Tenured	9	0	9
Total Department Faculty FTE (As reported in the most recent A-1/S-11 Institutional Cost Study for "prior to program implementation" and using the A-1/S-11 Cost Study Definition for the projected "at full program implementation.")	25	1.00	26.00

Staff

The Department of Information Systems and Technology currently employs one full-time and one part-time administrative assistant. Administrative support for the proposed program will be shared between these assistants. The part-time administrative assistant could develop into a full-time position as the program grows.

Students in the proposed program will be advised by the 1.5 full-time advisors in the Department of Information Systems and Technology. One advisor is assigned 100% to the IST majors. Another full-time advisor is assigned 50% to the IST majors. The department may need an additional academic advisor as the program grows.

Library and Information Resources

Under the TAACCCT grant, the library acquired adequate books and resources to start the cybersecurity program. Additional cybersecurity journals have been identified with the assistance of library personnel.

Admission Requirements

Potential students must apply for admission into the program. In order to qualify for admission into the program, the following are required:

1. Bachelor's degree with a GPA of at least 3.2 on a 4.0 scale from a regionally accredited institution in one of the following fields*
    - Information Systems
    - Information Security
    - Information Technology
    - Computer Science
2. Admissions Essay
3. Application
4. Official transcripts from all attended institutions of higher education
5. Two letters of recommendations

*Applicants who have bachelor's degrees in other fields may be admitted to the program if they have at least two years of IT or cybersecurity industry experience and have completed undergraduate courses in data communication, programming, and servers with a grade of C+ or better. Students may also take a comprehensive exam on these topics to satisfy this admission requirement. These applications will be handled on a case-by-case basis.

Student Advisement

Students in the proposed program will be advised by the current full-time advisors in the IST Department. As the program grows, the department may need an additional academic advisor to support the program.

Justification for Graduation Standards and Number of Credits

The proposed program requires ten cybersecurity courses (seven core courses including a capstone course and three electives) for a total of 30 credit hours. By requiring students to complete ten courses, all in cybersecurity, the proposed program will provide students with a quality and comprehensive education that will prepare them for senior positions in cybersecurity. In addition, the proposed 30-credits requirement is in line with the range of credits for similar cybersecurity master's degrees, which would allow it to compete nationally.

External Review and Accreditation

The Cybersecurity program has an advisory board that reviews and advises on program and course content, provides insight on industry trends, and provides opportunities for student placement as interns and employees. The program manager communicates with advisory board members regularly through scheduled group meetings, individual meetings, email, and conference calls. Ongoing additional review is being conducted by associates of the advisory board as well.

Additionally, UVU is reviewing the recently updated National Security Agency and the Department of Homeland Security Center of Academic Excellence program and will be aligning to the knowledge units specified under this program.

Projected Program Enrollment and Graduates; Projected Departmental Faculty/Students

Data Category	Current – Prior to New Program Implementation	Projected				
		Year 1 (16-17)	Year 2 (17-18)	Year 3 (18-19)	Year 4 (19-20)	Year 5 (20-21)
Data for Proposed Program						
Number of Graduates in Proposed Program	0	0	0	15	18	20
Total # of Declared Majors in Proposed Program	0	15	33	38	40	40
Departmental Data – For All Programs Within the Department						
Total Department Faculty FTE (as reported in Faculty table above)	25.00	25.50	26.00	26.00	26.00	26.00
Total Department Student FTE (Based on Fall Third Week)	510	519	532	538	540	540
Student FTE per Faculty FTE (ratio of Total Department Faculty FTE and Total Department Student FTE above)	20.40	20.35	20.46	20.70	20.77	20.77

Program accreditation-required ratio of Student FTE/Faculty FTE, if applicable: (Provide ratio here:_____)						

Expansion of Existing Program

This program will expand UVU's cybersecurity graduate education by building on the existing cybersecurity graduate certificate.

Additionally, this program will provide graduate education options for IST Department's growing enrollment. From 2013-2014 to 2014-2015, student credit hours in IST courses went from 4,185 to 7,059.

Section III: Need

Program Need

The evolving landscape of information security and the increasing pace at which cyber attacks continue to grow in scale and complexity, coupled with a gap of qualified cybersecurity professionals and scholars, provide rationale for the proposed program.

Data breaches across the country have impacted millions of businesses, agencies, and individuals. The Idenity Theft Resource Center reported that in 2014, there were 783 data breaches: 42.5% in medical/healthcare industry, 33% in business, 7.3% education, 5.5% banks/credit unions/financial institutions, and 11.7% government/military.[3] In 2014 it was reported that hackers believed to be working for the Russian government breached the unclassified White House computer networks.[4] Hackers believed to be based in China breached the computer systems of the Office of Personnel Management and stole the personal information of four million federal employees.[5] These incidents demonstrate he need to educate and train a workforce of cybersecurity-savvy professionals who are able to handle complex cybersecurity threats and capable of securing information, computer networks, and IT infrastructure.

A Master of Science in Cybersecurity is needed to provide undergraduate students in information technology, computer science, and other related fields, with the advanced cybersecurity knowledge and skills needed to address the complexity of cybersecurity threats and challenges. This rationale is echoed in the recommendations of several workshops on cybersecurity education and training. For example, a 2013 Association for Computing Machinery workshop[6] supported by the National Science Foundation (NSA) recommended that "Educational institutions should be encouraged to support master's and doctoral degree programs in fields requiring cybersecurity knowledge and skills." The group noted that "A master's degree in cybersecurity in a two-year timeframe would allow suitably prepared graduates to master the knowledge, skills, and abilities (KSAs) specific to advanced topics in cybersecurity".

Labor Market Demand

A 2015 Global information Security Workforce Study[7] by (ISC)[2], a global leader in educating and certifying information security professionals, reported a widening shortfall in the information security workforce with 62% of the survey respondents stating that their organizations have too few information security professionals

[3] Identity Theft Resource Center, http://www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html
[4] http://www.washingtonpost.com/world/national-security/hackers-breach-some-white-house-computers/2014/10/28/2ddf2fa0-5ef7-11e4-91f7-5d89b5e8c251_story.html
[5] http://www.wsj.com/articles/u-s-suspects-hackers-in-china-behind-government-data-breach-sources-say-1433451888
[6] https://www.acm.org/education/TowardCurricularGuidelinesCybersec.pdf
[7] https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC)%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf

compared to 56% in the 2013 survey. The study projects that the demand for cybersecurity professionals in the Americas would reach 2.5 million in 2019 with a compound annual growth rate (CAGR) of 11.2% over the five year period 2014-2019. This is compared to a supply of 1.9 million security professionals in 2019 with a CAGR of 6.0% over the same period. As noted in the study, the reasons for this hiring shortfall are due to an insufficient pool of suitable candidates.

The (ISC)^2 study further found that the largest increase in cybersecurity professional roles in the future are in those roles that are mostly managerial. The study goes on to note that "as security professionals advance in organizational roles, their educational investments also need to evolve to ensure professional success." This lends further support to the rationale for the need of a master program in cybersecurity.

Utah County is now the home of, or a key venue for, some of the world leaders in information technology and cybersecurity. Taking advantage of the unique corporate and human resources that Utah County has to offer, the National Security Agency (NSA) chose the area for the construction and implementation of a new Cybersecurity Data Center (CDC), the largest security data center in the world.

The NSA facility, however, is only part of the target for the proposed program. Some of the world leaders in information technology and cybersecurity are headquartered or have facilities in Utah County. Examples of potential employers include:

> Symantec: A Fortune 500 company and global leader in IT Security Management and technology; employs more than 1,000 IT Security professionals at its Lindon, Utah, facility. At the time this proposal was written, the company had 32 job openings in Utah.
>
> SecurityMetrics, Inc.: A leading provider of Data Security Standard (DSS) security solutions based in Orem, Utah; employs more than 400 security professionals and support staff. The company plans to expand operations and has expressed a need for more qualified penetration testers.
>
> NetIQ/Novell: NetIQ was acquired by Novell/Attachmate in an acquisition in which Novell's secure data center technology will merge with NetIQ technology in data security and secure virtualization. The Provo facility employs about 1,300 technology & data systems professionals & support staff.
>
> Additional cybersecurity jobs are available from a number of organizations from a wide variety of sectors. An October 2015 job search on the Indeed.com job aggregator shows over 150 current posted cybersecurity/information security positions in Utah. Here is a selection of titles and companies listed:
>
> Information Security Manager – State of Utah
> Security Analyst – SecurityMetrics
> Information Security Support Engineer – ConsultNet
> Director, Information Security Operations – D+H
> Security Risk Analyst – The Church of Jesus Christ of Latter-day Saints
> Information Systems Security Staff – Intermountain Healthcare
> US IT Security Rish Management Manager – PwC

The Department of Workforce Services projects that Information Security Analysts, an occupational category that relates to UVU's proposed program, will experience a 5.1% growth rate in Utah with employees earning an annual median income of $78,590.

Student Demand

The IST Department conducted a survey of students enrolled in IST undergraduate programs during Fall Semester, 2015. The survey received 145 responses. Of those, 50 are planning to attend graduate school and 81 are unsure. When asked their interest in a master's degree in cybersecurity at Utah Valley University, 91 were very interested and 42 were interested. The respondents were asked when they would consider starting a program. Forty-three respondents indicated either "as soon as possible" or the 2016-2017 school year. Fifty-one respondents indicated the 2017-2018 school year.

Similar Programs

Aside from UVU, which offers a post-baccalaureate certificate in cybersecurity, three other Utah System of Higher Education institutions offer cybersecurity graduate courses. Southern Utah University recenlty received approval to offer an on-line cybersecurity master's degree. In addition, the University of Utah and Utah State University offer graduate-level cybersecurity courses.

Western Governors University (WGU) offers a distance-only Master of Science in Information Security and Assurance degree. While this program covers similar topics, WGU's competency based approach is a different model and difficult to compare directly. Western Governors University offers courses nationwide, serving a different market than UVU's regional role.

Collaboration with and Impact on Other USHE Institutions

The proposed program is a natural expansion of UVU's current offerings in cybersecurity. Specifically, the new program would augment UVU's post-baccalaureate certificate in cybersecurity, thereby providing an alternative pathway for students. As the program develops, UVU has indicated an intent to collaborate with other institutions to provide the best outcomes for all students within the Utah System of Higher Education. Chief academic officers as well as faculty in related departments from the Utah System of Higher Education institutions have reviewed the proposal and have provided input.

Benefits

The proposed Master of Science in Cybersecurity holds the promise of providing undergraduate students and others who are in the workforce with the opportunity to be trained in a high-demand area and to find mid and high-level employment in a promising and growing field.

Consistency with Institutional Mission

Utah Valley University's Mission states that: "Utah Valley University is a teaching institution which provides opportunity, promotes student success, and meets regional educational needs." As a regional state university, UVU places high value on "preparing intellectually resilient graduates for a future of continuous and cross-disciplinary learning." One of UVU's key roles is to provide "quality academic learning opportunities for students through programs at the certificate, associate, baccalaureate, and graduate levels." Further, the College of Technology & Computing Mission Statement is "to prepare students for successful careers or advanced study in a dynamic, technology-based, global environment."

The proposed Master of Science in Cybersecurity fits within the mission of Utah Valley University in that it aims to meet the educational needs for cybersecurity skilled workforce in Utah and throughout the Western United States. The new program supports the university role in that it complements the current cybersecurity offerings at UVU by creating a new opportunity for comprehensive and quality cybersecurity education at the graduate level. Finally, the proposed program supports the College of Technology & Computing Mission in that it will prepare the student for advanced careers or doctoral studies in the dynamic and technology-based field of cybersecurity.

Section IV: Program and Student Assessment

Program Assessment

The program has two main program goals. Each goal has specific measurements.
Program Goal 1: Provide students with a comprehensive education in cybersecurity

> Measurement 1.1: Use the capstone course to determine whether or not the students have gained the knowledge and skills that were introduced and developed in the core courses.
>
> Measurement 1.2: Evaluate and update the curriculum through Advisory Board and industry-partnerships.
>
> Measurement 1.3: Evaluate the curriculum against the current standards of the National Security Agency and Department of Homeland Security for the designation of Centers of Academic Excellence in Information Assurance.

Program Goal 2: Produce cybersecurity graduates with the knowledge and skills needed to fill advanced technical and management positions in cybersecurity.

> Measurement 2.1: Monitor graduation numbers with 15 students expected to graduate annually; starting with year three of the program.
>
> Measurement 2.2: Monitor post-graduation employment trends with 80% of graduates expected to be placed within three months of graduation.

Expected Standards of Performance

Students graduating with a Master of Science in Cybersecurity will have achieved the following learning outcomes:

1. Demonstrate an understanding of the technical and managerial aspects of cybersecurity.
2. Demonstrate the ability to solve cybersecurity related problems and to make effective cybersecurity decisions in a dynamic and constantly changing environment.
3. Demonstrate proficiency in using the tools, techniques, and technologies related to the identification and mitigation of cybersecurity threats.
4. Develop an understanding of risk management methods as they relate to cybersecurity.
5. Develop an understanding of the legal, regulatory, and ethical issues surrounding cybersecurity.

The aforementioned learning outcomes will be introduced and reinforced across various courses throughout the program. A variety of methods will be conducted to assess the learning outcomes of students. Specifically, faculty members teaching the courses will design and administer several learning activities to assess the learning outcomes. These activities include, but are not limited to, tests, projects, lab exercises, case studies, debates, research papers, and oral presentations. Whenever appropriate, scoring rubrics will be developed to examine the degree to which students learning outcomes are fulfilled.

In addition, UVU institutional effectiveness officials will be consulted in the ongoing evaluation of methods and processes appropriate to these activities. This will include the following: Content/Learning, Post-Graduation Outcomes, and Measures of Student Satisfaction.

Faculty, students, and advisors will be active participants in ongoing learning outcomes assessment and program evaluation processes. Goals and objectives will be reviewed, data collected and analyzed, evaluation processes implemented, and feedback utilized in an effort to generate continuous improvement in all these activities.

Section V: Finance

Department Budget

9/11/2015 Note: Waiting from the Budget Office to update the Library and Travel data.

Three-Year Budget Projection							
Departmental Data	Current Departmental Budget - Prior to New Program Implementation	Departmental Budget					
		Year 1 (2016-17)		Year 2 (2017-18)		Year 3 (2018-19)	
		Addition to Budget	Total Budget	Addition to Budget	Total Budget	Addition to Budget	Total Budget
Personnel Expense							
Salaries & Wages	$968,122	$52,500	$1,020,622	$52,500	$1,073,122	$0	$1,073,122
Benefits	$412,694	$21,030	$433,724	$21,030	$454,754	$0	$454,754
Total Personnel Expense	$1,380,816	$73,530	$1,454,346	$73,530	$1,527,876	$0	$1,527,876
Non-personnel Expense							
Travel	$0	$3,000	$3,000	$0	$3,000	$0	$3,000
Capital	$0	$0	$0	$0	$0	$0	$0
Library	$0	$2,000	$2,000	$0	$2,000	$0	$2,000
Current Expense	$20,101	$10,000	$30,101	$0	$30,101	$0	$30,101
Total Non-personnel Expense	$20,101	$15,000	$35,101	$0	$35,101	$0	$35,101
Total Expense (Personnel + Current)	$1,400,917	$88,530	$1,489,447	$73,530	$1,562,977	$0	$1,562,977
Departmental Funding		Year 1 (2016-17)		Year 2 (2017-18)		Year 3 (2018-19)	

Appropriated Fund	$1,400,917	$68,870	$1,464,787	-$37,773	$1,502,560	-$16,851	$1,485,709
Other:							
Special Legislative Appropriation							
Grants and Contracts							
Special Fees/Differential Tuition	$0	$24,660	$24,660	$35,757	$60,417	$16,851	$77,268
Total Revenue	$1,400,917	$88,530	$1,489,447	$73,530	$1,562,977	$0	$1,562,977
Difference							
Revenue - Expense	$0	$0	$0	$0	$0	$0	$0
Departmental Instructional Cost/Student Credit Hour* (as reported in institutional Cost Study for "current" and using the same Cost Study Definition for "projected")	$137		$143		$147		$145

** Projected Instructional Cost/Student Credit Hour data contained in this chart are to be used in the Third-Year Follow-Up Report and Cyclical Reviews required by R411.*

Funding Sources

This program requires the addition of several new courses within the Information Systems and Technology Department. Utah Valley University's three-year grant through the Department of Labor to develop and implement cybersecurity programs has already funded almost half the course development for the master's program. The institution continues to seek private and grant funding to support the program. Additionally, UVU will request support through mission-based funding.

Reallocation

No internal reallocation is planned.

Impact on Existing Budgets

It is not anticipated that other existing budgets will be impacted by this program.

Section VI: Program Curriculum

All Program Courses (with New Courses in Bold)

Course Prefix and Number	Title	Credit Hours
Required Courses		
IT 6300	Principles of Cybersecurity	3
IT 6330	Cybersecurity Operations	3
IT 6350	Law, Ethics, and Privacy in Cybersecurity	3
IT 6370	Penetration Testing and Vulnerability Assessment	3
IT 6740	Advanced Network Defense and Countermeasures	3
IT 6770	Cybersecurity Management	3
IT 6900	Cybersecurity Capstone	3
	Sub-Total	21
Elective Courses (Choose 3)		
IT 6660	Advanced Network Forensics	3
IT 6750	Reverse Engineering & Malware Analysis	3
IT 6780	Secure Coding	3
INFO 6420	Web and Mobile Application Security	3
Or other departmental approved electives		
	Sub-Total	9
	Total Number of Credits	30

Program Schedule

Fall of First Year (Course Prefix and Number)	Course Title	Credit Hours
IT 6300	Principles of Cybersecurity	3
IT 6330	Cybersecurity Operations	3
	Semester total:	6
Spring of First Year (Course Prefix and Number)	**Course Title**	**Credit Hours**
IT 6740	Advanced Network Defense and Countermeasures	3
IT 6350	Law, Ethics, and Privacy in Cybersecurity	3
	Semester total:	6
Summer of First Year (Course Prefix and Number)	**Course Title**	**Credit Hours**
IT 6370	Penetration Testing and Vulnerability Assessment	3
	Semester total:	3
Fall of Second Year (Course Prefix and Number)	**Course Title**	**Credit Hours**
IT 6770	Cybersecurity Management	3

Elective		3
	Semester total:	6
Spring of Second Year (Course Prefix and Number)	Course Title	Credit Hours
Elective		3
Elective		3
	Semester total:	6
Summer of Second Year (Course Prefix and Number)	Course Title	Credit Hours
IT 6900	Cybersecurity Capstone	3
	Semester total:	3

Section VII: Faculty

Basil Hamdan

- Assistant Professor, Cybersecurity
- Education: Ph.D. in Information Systems
- Professional Certifications: GIAC Web Application Penetration Tester

Keith R. Mulbery

- Department Chair and Professor, Information Systems
- Education: Ph.D. in Business Information Systems

C. Paul Morrey

- Assistant Professor, Information Technology
- Education: Ph.D. in Computer Science

Michael Savoie

- Dean, College of Technology & Computing
- Education: Ph.D. in Operations Management

Additional full-time faculty will need to be hired as the program grows (see Institutional Readiness section).