ACADEMIC PROGRAM PROPOSAL FORM

(*Revised: October 2017*)

DIRECTIONS: *Use this form when proposing a new major or primary field of study, new emphasis (BAS only), or new degree or certificate (30+credits) program.* ***For more detail on the NSHE program approval process, see the last page of this form.***

DATE SUBMITTED: October 2019

INSTITUTION: University of Nevada, Las Vegas

Date of AAC Approval:

12-4-19

Date of Board Approval:

REQUEST TYPE:

□ New Degree
☒ New Major or Primary Field of Study
□ New Emphasis (BAS only)

DEGREE: Check applicable box

□ Certificate: 30+ Credits
□ Associate of Science (AS)
□ Associate of Applied Science (AAS)
□ Bachelor of Arts (BA)
☒ Master of Science (MS)
□ Doctor of Philosophy (Ph.D.)

□ Associate of Arts (AA)
□ AA/AS
□ Bachelor of Applied Science (BAS)
□ Bachelor of Science (BS)
□ Master of Arts (MA)
□ (Other or Named Degree)

MAJOR OR PRIMARY FIELD OF STUDY (i.e. Animal Science): Cybersecurity

INCLUDED IN LAST NSHE PLANNING REPORT: ☒ Yes □ No
(Website for NSHE Planning Reports: https://www.nevada.edu/ir/Page.php?p=planning)

TOTAL NUMBER OF CREDITS TO PROGRAM COMPLETION: 30

PROPOSED SEMESTER/TERM OF IMPLEMENTATION: Fall 2020

Action requested (specify full program title):
Approval of a new M.S. Cybersecurity degree, as an interdisciplinary program between the Lee Business School and the Howard R. Hughes College of Engineering is requested.

A. Brief description and purpose of proposed program. For proposed certificates (30+ credits), provide any existing degree or program under which the certificate falls.

The new program is an interdisciplinary master of science in cybersecurity. Resources will be shared between the Lee Business School and the Howard R. Hughes College of Engineering as students will be required to take courses in both schools. Currently, there is a demand at the local, state, regional, and national levels for individuals to be trained in the knowledge of computers, networks, and risk and security management. This has been identified by the Department of Labor and other sources as one of the most needed professions/skills, yet the traditional sources of such skills (i.e., higher education) are not producing graduates as fast as this field is growing (https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm).

Students will be trained in technical and managerial aspects of cybersecurity. This program would build upon the strengths within the Computer Science department in the College of Engineering, which can provide the technical expertise of dealing with data, computers and networks. This program also builds on the strengths of the management information systems group within the Management Entrepreneurship, and Technology (MET) department in the Lee Business School to provide the expertise in managerial aspects of security, compliance, and risk management.

The graduate program in cybersecurity will also enable those already in the field to hone their managerial skills and enter into the management of cybersecurity, or provide those with other related skill sets to move from a related/technical field into cybersecurity. This M.S. in Cybersecurity will:
1) prepare cybersecurity specialists for management positions,
2) broaden skill sets from the undergraduate level, and
3) provide a broader view of cybersecurity within an organization.

B. Provide a list and description of institutionally approved expected student learning outcomes

1. Evaluate the computer network and information security needs of an organization
2. Assess cybersecurity risk management policies in order to adequately protect critical resources and assets
3. Demonstrate a mastery of in-depth knowledge of cybersecurity
4. Formulate, update and communicate regarding organizational cyber-related strategies and policies

C. Provide an institutionally approved plan for assessing student learning outcomes

The program will evaluate the achievement of its objectives through the assessment of the student learning outcomes. See Appendix A for additional details on the assessment process for the proposed program.

This assessment plan has been submitted to the Office of Assessment and was approved on November 30th, 2017.

D. Contribution and relationship of program objectives to

i. NSHE Master Plan

This program will impact the following goals of the current NSHE Master Plan:

1. Increase Student Success
This program is focused on a career pathway that is largely untouched by regional academic programs, despite a large need within the employment sector. There will be a strong demand for the M.S. in Cybersecurity because it will prepare graduates for high demand jobs paying competitive salaries. It will contribute to more M.S. degrees being awarded, which impacts this goal.

2. Workforce. There is a large workforce demand for cybersecurity that NSHE institutions are not currently meeting. Cybersecurity is one of the largest growing fields without a current supply line from academic institutions. The latest estimates for the demand of cybersecurity professionals is maintained at cyberseek.org, supported in part by a grant from the National Initiative for Cybersecurity Education (NICE), which is part of a cooperation between the Department of Homeland Security (DHS), National Institute of Science and Technology (NIST)

and the National Security Agency (NSA). These work force demands are summarized in Section E, subsection i.

ii. Institutional mission and core themes

As part of the Top Tier initiative, the goals for research, scholarship and creative activity metrics will be positively impacted by this program.

1. UNLV Core Theme: Research, Scholarship and Creative Activity, "Objective 5: The number of master's and professional degrees granted per year, as appropriate for individual academic units" (https://www.unlv.edu/toptier/progress/rsc-info). This program will increase the number of graduate degrees conferred, thus directly impacting this metric.

2. UNLV Core Theme: Community Partnerships, "Objective 1: Create community connections." This degree will provide direct outreach between UNLV and specific community entities in the form of partnerships. These partnerships will allow students access to internships, resources for cyberlabs, competitions and speakers from local security organizations. The following community collaborations are detailed more specifically:

Collaborations with CCSD: CyberPatriots is a cyber program which aims to encourage high school students to engage and participate in cyber competitions. These programs are run by local cyber groups within Nevada, and in the future will include UNLV students in the new degree serving as mentors and coaches for the teams. This will result in more collaborations for UNLV with the entity CyberPatriots and CCSD.

Collaborations with local cybersecurity professional organizations (e.g., Southern Nevada Security Alliance, ISC2, Cloud Computing, etc.). These collaborations will provide access to the local cybersecurity professional network, which will help with job and internship placement, course projects, guest speakers, and potential for resources to help fund/build a cyberlab. This may have impacts on CMP M3A & B by involving local business leaders with UNLV students and events.

3. UNLV Core Theme: Research, Scholarship and Creative Activity, "Objective 6: Increase supervised research and research internships and undergraduate research" (https://www.unlv.edu/toptier/progress/rsc-info).

It is anticipated, that since the program is aligned with the NICE curriculum framework, it will be able to receive accreditation as an Academic Center of Excellence, and also with the Department of Homeland Security and thus be eligible for federal grant funds to create a cyberlab. If this occurs, the number of students working in a lab will also increase. This will have a spillover impact on students engaging in research and presenting in conferences through their involvement with faculty research within this laboratory setting. These interactions would directly result in more students engaging in research with faculty.

iii. Campus strategic plan and/or academic master plan

The proposed degree supports several pathway goals of the Top Tier Strategic Plan, as stated in the previous section, and it was included in the most recent academic master plan for UNLV. It contributes to the strategic plan of both the Lee Business School and the Howard R. Hughes College of Engineering as follows:

LEE Business School (LBS) Strategic Plan Highlights:
Section 1. Cultivate Student Success

- Action step, bulleted item 4: Identify relevant and market-driven knowledge areas

- Action step, bulleted item 7: Enhance curricula and develop programs that help students gain contemporary, market-driven professional skills.

Section 2. Nurture Excellence and Achievement

- Action step, bulleted item 3: Identify and enhance each department's distinctive capabilities in teaching, research and service.

Section 4. Process-Related Strategies - Continuous Improvement & Innovation, and Data-Driven Decision-Making

- Action step, bulleted item 1: Prioritize and enhance programs that add value and allocate resources accordingly.

Howard R. Hughes College of Engineering Strategic Plan Highlights:
Scholarship: Strategy 3:

- Identify nationally competitive new research themes, clusters, and Centers of Excellence. Potential for gaining external funding.

Education Measures, 2: Graduate Students. Increase the number of graduate students for the college.

iv. Other programs in the institution

This program will build upon the strengths within the Computer Science department in the College of Engineering, which can provide the technical expertise of dealing with data, computers and networks. This program also builds on the strengths of the management information systems group within the Management, Entrepreneurship, and Technology (MET) department in the Lee Business School to provide the expertise in managerial aspects of security, compliance and risk management.

v. Other related programs in the System

A Master of Science Cybersecurity was approved in September 2019 for the University of Nevada, Reno. It will be a completely online degree program and will begin in summer 2020.

The College of Southern Nevada offers an associate level degree that is focused on technical aspects of securing computer systems.

The University of Nevada, Reno offers a minor in cybersecurity at the undergraduate level, and a certificate at the graduate level.

There is a certificate in Emergency Crisis Management Cybersecurity in the Department of Criminal Justice at UNLV and its focus is different than the M.S. The certificate was offered for the first time in 2018, and has matriculated five students. The program includes 12 credits, and takes two semesters to complete. The nature of this program is planning for and responding to cyber-terrorism events, primarily for government employees. It is not meant to train in the management and development of a protective, operational cybersecurity plan or portfolio.

E. Evaluation of need for the program

i. The need for the program and the data that provides evidence of that need

Cybersecurity is an emerging field that didn't exist as an academic discipline two decades ago. It is touted as one of the most important fields in the current digital age, wherein cyber defense and cyber offense are needed to combat cyber terrorism, cyber warfare, industrial espionage, data breaches, etc. In order to train students to enter these careers, a degree in this area needs to be created. At UNLV, technical expertise can be provided by the Howard R. Hughes College of Engineering and organizational skills by the Lee Business School.

The federal government is also highly interested in cybersecurity educational efforts, having created the National Initiative for Cybersecurity Education (NICE), which will be providing grants to promote programs and educational ventures. This initiative will become a significant resource for potential research grants in cybersecurity. Funding has been on the rise both with the National Science Foundation and Department of Defense/Department of Energy grant programs. UNLV recently received this NICE Center of Academic Excellence designation in the summer of 2019.

In Las Vegas, the second highest attendance rate at conferences are cyberhacking related, i.e., BlackHat and DefCON, held annually.

The southern Nevada region has no pipeline for cybersecurity talent and prospective employees have to be recruited from existing professionals in the valley or from out-of-state. This is a costly venture as many organizations find it difficult to recruit from out of state, and then to retain such individuals. The degree program will help fill this employment gap.

The existence of local, regional and national demand for cybersecurity professionals is reviewed below.

Locally:

Based on a review of local jobs that list the focus of the position as cybersecurity, there are roughly 1,500 local jobs that are unfilled (per cyberseek.org) in the Las Vegas metro area. Further, discussions with local companies, such as Caesars, CapitalOne, Sands, Bally's, IGT, Southwest Gas, NV Energy, NSTec, etc. have shown that there is a concern with the inability to hire local talent in this area. The College of Engineering created a task force from industry representatives from over 40 companies that support this viewpoint, and obtained several letters of support showing this demand from local industry, which are attached.

Regionally:

Based on available data from the U.S. Bureau of Labor Statistics, there is a high and increasing demand for individuals with cybersecurity training for the western region (Last updated May 2018: https://www.bls.gov/oes/current/oes151122.htm#st). Currently, there are about 37,000 cybersecurity unfilled positions in California, and 79,000 filled positions; in Arizona, 8,000 unfilled positions and 15,000 filled positions. Although no data on cybersecurity jobs was collected from the state of Nevada, the U.S. Bureau of Labor Statistics predicts the information security job growth rate of 13.4% from 2014 to 2024 in Nevada. This prediction is supported by the NSHE in the Statewide Workforce Supply and Demand Report (https://ir.nevada.edu/strategic_plan.php?metric=spm4&mid=workforce_demand) that analyzed the job growth of the computing occupations, which is the general field of this degree. According to the Nevada Department of Employment, Training and Rehabilitation's employment projection data (http://nevadaworkforce.com), the total employment is projected to grow by 24.5% between 2014 and 2024. Computer related jobs have a stronger growth projection as following:

- Computer and Mathematical Occupations: 26.5%
- Computer Science and Systems Analysts: 26.1%
- Computer systems Analysts: 33.7%
- Software developers Applications: 37.9%
- Web developers: 42.6%

This shows that there are about 1,087 annual openings in the area of Computer and Information

Sciences and Support Services, with an annual growth rate of 17.1%

Based on the graduation rates of computer science and management information sciences students (the nearest degrees available to cybersecurity), the supply in this area at the associate level is 356; bachelor level, 302; and MS/PhD 87 which leaves a shortfall of 342 each year. This information is based on very high-level job descriptors of those who have a background in computer science only. The CIP code designation for cybersecurity does not yet exist at the national level. Based on the growing needs, it is predicted that the cybersecurity job shortage will exceed the data above.

National data places employment in this field as the top job, in terms of pay and growth for the coming years (https://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/).

According to the U.S. Bureau of Labor Statistics, the expected job growth rate from 2014 to 2024 for the Information Security field is 18%. This is far higher than the growth rate of 12% in the overall computer occupation.

ii. Student population to be served

Based on student interest, it is predicted that some of the current undergraduate students in computer sciences and information management will chose to stay at UNLV and obtain this master's degree. There are a large number of employees in UNLV's Office of Information Technology who will be attracted to this degree to enhance their career opportunities. Externally, the program will recruit current professionals in cybersecurity and improve their career trajectories through completion of this graduate program.

iii. Procedures used in arriving at the decision to offer the program

The U.S. government has recognized the need for more cybersecurity training at its institutions of higher learning and created the National Initiative for Cybersecurity Education (NICE). The Association for Computing Machinery (ACM; the oldest and largest group in regards to computing technology development and research in the world), established a model curriculum for cybersecurity, which became available in 2017. This proposed model curriculum highlights in detail the need and demand for cybersecurity in the world, nationally and for higher education. The report is available as Appendix C.

In 2016 the dean of the College of Engineering convened a taskforce for cybersecurity education. This had an impetus in numerous communications from industry leaders requesting a degree program. The task force began with heavy support from industry, as identified here at the May 2016 meeting:

Industry	Organizations
Casino/Gaming	IGT, Aristocrat, Bally technology, Konami, Boyd Gaming, Sands, MGM Mirage
Technology	JT3, Switch, Influential, Nevsys, NovaGeotech, Originate, ViaWest
Utilities	NV Energy, Southwest Gas, Southern NV Water Authority, Carollo
Transportation	Allegiant
Government	US DOE/NNSA, Remote Sensing Lab, Clark County, Clark Cty Schools District
Cybersecurity	Axiomcyber.com
Construction	Hill International, Las Vegas Paving, Penta Building, Tutor Perini Building
HR	MNCP Staffing, Roceteer

This first meeting focused on the desired outcomes and skillsets of the individuals. It was high-level only, as it was uncertain what current programs existed at UNLV. This was addressed at the taskforce's second meeting in September 2016 through a presentation of all the coursework, certificates and programs at UNLV that touched the cyber profession. The list was determined to be too small and unsatisfactory by the industry partners, who requested more skills, which requires formal degree programs.

The third meeting of the task force presented the plans for the M.S. degree, which followed the NICE curriculum framework. The industry members present ratified and agreed to the overall structure and nature of the program and offered support in the form of instructors, mentors, workshops, labs and equipment to help get the program started, once approved by the NSHE.

During this process, two surveys were conducted to gather degree requirements for learning and skills outcomes. These were completed in April 2016 and December 2016.

Members of approximately 13 local cybersecurity/information technology associations have promised support and opportunities for networking, job placement, and internships for students.

During the time that was taken to prepare and plan for this program, faculty also submitted the necessary paperwork to the federal government and has recently received a designation as an Academic Center of Excellence following the NICE framework.

iv. Organizational arrangements required within the institution to accommodate the program

The program will be officially housed in the Graduate College, based on the recently approved Graduate College interdisciplinary programs guidelines adopted in 2018. The program will be administered by an executive committee.

A program director will be needed for the program, which will involve a stipend and a course release, like any other Graduate Coordinator. This individual will run the program, including scheduling courses and instructors, plus advising students.

v. The timetable, with dates, for implementation steps

The Graduate College Program Committee approved this proposal in fall 2019.

Upon approval by NSHE, engaged faculty in the Computer Science and management, Entrepreneurship and Technology Departments will work with industry partners in order to help create content, review curriculum, and establish labs, by means of a newly created Cybersecurity Advisory Board. These faculty will be assigned to teach courses in the newly created program Some part-time instructors, identified through the assistance of this Advisory Board, will be used while the program is beginning and growing.

It is anticipated that by the fourth year one full-time faculty line will have been hired to teach exclusively in this program.

vi. If this or a similar program already exists within the System, what is the justification for this addition

A Master of Science Cybersecurity was approved in September 2019 for the University of Nevada, Reno. It will be a completely online degree program and will begin in summer 2020.

UNLV’s M.S. Cybersecurity will be a face-to-face program. There appears to be a large enough market in southern Nevada to support the UNLV program without encroaching on UNR’s market. Students who enroll in the face-to-face program are more likely to be local residents and to be already employed in southern Nevada and to stay here when their degree is completed. The overall need for graduates in this program is large enough to sustain both programs as noted earlier in section E.

vii. Evidence of employment opportunities for graduates (state and national). Include information on institutional review of the need for the program based on data from the Nevada P-20 Workforce Research Data System (https://www.nevada.edu/ir/Page.php?p=workforce), including the supply/demand reports at http://npwr.nv.gov/reports/student-completion-and-workforce-part-ii/.

Locally, the entire Southern Nevada region has no pipeline for cybersecurity graduates and employees have to be recruited from existing professionals in the valley or from out-of-state. This is a costly venture as many organizations find it difficult to recruit from out of state, and then to retain individuals. The degree program will help fill this employment gap.

The existence of local, regional and national employment opportunities for cybersecurity professionals is reviewed below.

Local:

Based on a review of local jobs that list the focus of the position as cybersecurity, there are over 1,500 local jobs that are unfilled (per cyberseek.org) in the Las Vegas metro area. Further, discussions with local companies, such as Caesars, CapitalOne, Sands, Bally's, IGT, Southwest Gas, NV Energy, NSTec, etc. have shown that there is a concern with the inability to hire local talent in this area. We have created a task force from industry representatives from over 40 companies that support this viewpoint, and obtained several letters of support showing this demand from local industry.

Regional:

Based on available data from the U.S. Bureau of Labor Statistics, there is a high and increasing demand for individuals with cybersecurity training for the western region (https://www.bls.gov/oes/current/oes151122.htm#st). Currently, there are about 45,000 cybersecurity jobs in California and 8,500 in Arizona, where half of the positions cannot be filled due to worker shortage, Cyberseek.org. Although no data on cybersecurity jobs was collected from the state of Nevada, the U.S. BLS predicts the information security job growth rate of 13.4% from 2014 to 2024 in Nevada. This prediction is supported by the NSHE in the Statewide Workforce Supply and Demand Report (https://www.nevada.edu/ir/page.php?p=workforce_tableau) that analyzed the job growth of the computing occupations, which is the general field of this degree. According to NV DETR Employment projection data (http://nevadaworkforce.com), the total employment is projected to grow by 24.5% between 2014 and 2024. Computer related jobs have a stronger growth projection as following:

- Computer and Mathematical Occupations: 26.5%
- Computer Science and Systems Analysts: 26.1%
- Computer systems Analysts: 33.7%
- Software developers Applications: 37.9%
- Web developers: 42.6%

This shows that there are about 1,087 annual openings in the area of Computer and Information Sciences and Support Services, with an annual growth rate of 17.1%

Based on the graduation rates of computer science and management information sciences students (the nearest degrees available to cybersecurity), the supply in this area at the associate level is 356; bachelor level, 302; and MS/PhD 87 which leaves a shortfall of 342 each year. This information is based on very high-level job descriptors of those who have a background in computer science only. The CIP code designation for cybersecurity does not yet exist at the national level. Based on the growing needs, it is predicted that the cybersecurity job shortage will exceed the data above.

National:
National data places employment in this field as the top job, in terms of pay and growth for the coming years (https://www.forbes.com/forbes/welcome/?toURL=https://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/&refURL=https://www.google.com/&referrer=https://www.google.com/).

According to the U.S. Bureau of Labor Statistics, the expected job growth rate from 2014 to 2024 in the Information Security field is 18%. This is far higher than the growth rate of 12% in the overall computer occupation.

F. Detailed curriculum proposal

i. Representative course of study by year (options, courses to be used with/without modification; new courses to be developed)

The M.S. program has 30 total credits. 24 are required credits and 6 are elective credits.

All courses in the program are new and to be developed.

Required Courses. (24 Credit hours)

- CSEC 700: Security Operations (3 Credits)
- CSEC 701: Secure Communication Protocols (3 Credits)
- CSEC 702: Security Data Analytics (3 Credits)
- CSEC 703: Cyber Physical Systems Security (3 Credits)
- CSEC 704: Human Factors in Cybersecurity (3 Credits)
- CSEC 705: Enterprise Security Administration (3 Credits)
- CSEC 790: Capstone (6 credits)

Electives. (6 Credit hours)

- CSEC 721: Modern Cryptography (3 Credits)
- CSEC 722: Trusted Software Systems (3 Credits)
- CSEC 723: Cybercrime and Cyberterrorism (3 Credits)
- CSEC 724: Forensics & Incident Response (3 Credits)
- CSEC 731: Cybersecurity in the Hospitality Industry (3 Credits)
- CSEC 732: Cybersecurity in the Healthcare Industry (3 Credits)
- CSEC 733: Cybersecurity in the Financial Industry (3 Credits)
- CSEC 734: Information Warfare (3 Credits)
- CSEC 750: Special Topics (1-6 Credits, depending on topic, can be repeated for up to 6 credits)
- CSEC 755: independent Study (1-3 Credits, depending on topic, can be repeated for up to 3 credits)
- CSEC 780: Internship (1-6 Credits, depending on position, can be repeated for up to 6 credits)
- Other CSEC, CS, IS, or related field, with advisor approval at the 600/700 level (Max of 3 credits)

ii. Program entrance requirements

Admission requirements:

- Undergraduate degree in a technology program (i.e., CS, IS, Security, Engineering, etc.)
- GRE test scores placing the student in the top 50% of test-takers (i.e., 309 or higher) will be given preference
- Overall undergraduate GPA of 2.75, or 3.0 during the final 2 years of the program
- Official transcript of all university-level education
- International students from a country where English is not the native language and who did not receive a degree from a university where English is the language of the institution must submit a TOEFL score (minimum score of 550 for the paper-based test, 213 for the computerized test, or 80 for the Internet-based test)
- Two letters of recommendation concerning the potential for success in the graduate program
- Statement of purposes explaining interest in the program

iii. Program completion requirements (credit hours, grade point average; subject matter distribution, preprogram requirements)

Students must complete the following to graduate with a M.S. in Cybersecurity

- Overall GPA of 3.00
- Successful completion of culminating experience (i.e., CSEC 790 Capstone course)
- Complete all required courses with a grade of B or higher

iv. **Accreditation consideration (organization (if any) which accredits program, requirements for accreditation, plan for attaining accreditation - include costs and time frame)**
NA

v. **<u>For certificates only:</u> Name of any state, national and/or industry recognized certification(s) or licensing examination(s) for which certificate prepares the student, if applicable**
NA

G. Institutional Review Process

i. **Date of Faculty Review (may include additional information, as needed)**
There have been four academic reviews of this proposal to date.

MET Faculty
This was reviewed at a meeting of the faculty, and a vote was obtained in unanimous support. April 1, 2019. 19 in favor; none opposed.

CS Faculty
This has been reviewed at several different meetings, in which final approval was given, after numerous revisions in October, 2018. 10 in favor; 3 opposed; 2 abstained.

LEE Graduate Committee
This was reviewed in April 2019 and received complete support from this committee. 5 in favor, none opposed.

Engeering Graduate Committee
This was reviewed in late November, 2018, and received complete support, after some minor revisions.

ii. **Describe the process for review and approval by the appropriate academic policy body of the institution**
Given pre-approval support from the departments, colleges, the Vice Provost for Academic Programs (VPAP), and then later support of this full proposal by the respective departments and colleges, it has been submitted for technical review by the Graduate College. It will go through final review and approval with the office of the VPAP and the Graduate College, prior to submission to the Board of Regents.
All institution level approvals have been completed.

H. Readiness to begin program

i. **List the educational and professional qualifications of the faculty relative to their individual teaching assignments**
To begin the program, there are several faculty members with the appropriate expertise to assist with implementation:
- The first is a business professor, specializing in behavioral security, with a Ph.D. in Information Systems. This professor was a Research Associate for the Information Systems Security Research Center, has published over 11 A publications, and over 50 peer-reviewed

publications in the last 8 years, and has expertise to teach risk-based management, controls, security administration and human-factors in cybersecurity.

- The second faculty member, in computer science, has published over 90 papers in peer-reviewed journals and conferences, and has six patents granted or pending. This individual's research has been sponsored by Microsoft Research, U.S. Air Force, Naval Air Warfare Center, Oak Ridge National Laboratory, National Security Technologies, and National Science Foundation. The individual's research on Distributed Denial of Service attacks has established a foundation for Rate-Based Intrusion Prevention Systems, which has been cited over 400 times.

- The third faculty member is an associate professor in engineering with over 50 peer-reviewed publications. This individual's specialty is in cyber security, computer networks, big data analytics and security log data.

The second and third faculty members are qualified to teach in the more technical adminstration and oversight of security, encryption, and security protocols.

- The fourth faculty member is an associate professor in business with over 20 peer-reviewed publications. This individual's specialty is in technical aspects of design and previous experience as a software development manager. This individual will be able to teach several of the business focused and technical courses.

- The fifth faculty member is an assistant professor in business with over 20 years as a data scientist and consultant. This individual will specialize in cyberanalytics, which is an emerging area in the field.

ii. List the anticipated sources or plans to secure qualified faculty and staff

Each faculty member mentioned in the section above will teach courses in his/her area of expertise. Industry partners may assist in identifying potential educationally qualified instructors that can help start and build the program. In year three the hiring process will commence for a full-time teaching position to start in the fourth year of the program. Additional positions will be hired every two years after that, if enrollment warrants and funding allows.

Administrative support will come from existing administrative assistants. Future growth would determine whether additional, dedicated support is warranted and if funding allows.

iii. Contribution of new program to department's existing programs (both graduate and undergraduate) and contribution to existing programs throughout the college or university

This program is complementary to both the M.S. in Computer Science and the M.S. in Management Information Systems (MIS) currently offered. Cybersecurity is a related field, but is not as technical as computer science, nor is it as diverse as MIS. Cybersecurity is focused on one specific career pathway, which is not well served by either degree program.

iv. Recommendations from prior program review and/or accreditation review teams

NA

I. Resource Analysis

i. Proposed source of funds (enrollment-generated state funds, reallocation of existing funds, grants, other state funds)

Student tuition will support the program in addition to the two colleges.

A new faculty line will be needed to start in year four of the program and will be requested by one of the two colleges, depending on the area of expertise required. Partial salary is reflected in year three of the cost estimate but no increase in FTE. After the first five years, a permanent, full time administrative assistant and office space will be requested, assuming the program warrants it.

ii. Each new program approved must be reviewed for adequate full-time equivalent (FTE) to support the program in the fifth year. Indicate if enrollments represent 1) students formally admitted to the program, 2) declared majors in the program, or 3) course enrollments in the program.

a. (1) Full-time equivalent (FTE) enrollment in the Fall semester of the first, third, and fifth year.

1st Fall semester 7.5

3rd Fall semester 11.25

5th Fall semester 15.00

(2) Explain the methodology/assumptions used in determining projected FTE figures.
Full-time students will take 9 credit hours as per semester, multipled by the number of students, divided by 12.

b. (1) Unduplicated headcount in the Fall semester of the first, third, and fifth year.

1st Fall semester 10

3rd Fall semester 15

5th Fall semester 20

(2) Explain the methodology/assumptions used in determining projected headcount figures.
A current student club, with interest in cybersecurity, has 20 active students. If some of those students continued their education at the graduate level, about five students per year could be expected from current programs. There are also other students and alumni that have expressed interest and work in cybersecurity. In working with industry partners, many of them have expressed interest in completing the degree or having their employees complete the degree. These two areas should provide about five additional students. There will also be additional recruiting efforts in appropriately identified areas.

iii. Budget Projections – Complete and attach the Five-Year Program Cost Estimate and Resource Requirements Table.
See attached Cost Estimate.

J. Facilities and equipment required

i. Existing facilities: type of space required, number of assignable square feet, space utilization assumptions, special requirements, modifications, effect on present programs

Nothing additional required.

ii. **Additional facilities required: number of assignable square feet, description of space required, special requirements, time sequence assumed for securing required space**
The program will require one or two offices for part-time instructors to be able to meet with students outside of the classroom. The offices will be provided by the colleges involved, with the appropriate dean requesting any additional space approximately one year before it is needed.

iii. **Existing and additional equipment required**
Some existing equipment will be used and approximately every two to three years replacement equipment will be necessary. Leading security software and tools are available via Kali-Linux which is a free operating system.

K. Describe the adequacy and availability of library and information resources
Cybersecurity has developed from the management information and computer science fields and the available library matierals and resources contain the necessary resources for the new degree.

L. Student services

i. **Describe the capacity of student support services to accommodate the program. Include a description of admissions, financial aid, advising, library, tutoring, and others specific to the program proposal**
The program director will provide advising to the new M.S. students in addition to graduate coordinators in the Lee Business School and the Howard R. Hughes College of Engineering.

ii. **Describe the implications of the program for services to the rest of the student body**
No major implications are expected.

M. Consultant Reports – If a consultant was hired to assist in the development of the program, please complete subsections A through C. A copy of the consultant's final report must be on record at the requesting institution.

i. **Names, qualifications and affiliations of consultant(s) used**
N/A

ii. **Consultant's summary comments and recommendations**
N/A

iii. **Summary of proposer's response to consultants**
N/A

N. Articulation Agreements

i. **Articulation agreements were successfully completed with the following NSHE institutions. (Attach copies of agreements)**
N/A

ii. **Articulation agreements have not yet been established with the following NSHE institutions. (Indicate status)**
N/A

iii. **Articulation agreements are not applicable for the following institutions. (Indicate reasons)**

N/A

O. Summary Statement

The creation of the first 1.5 to 2 year graduate level cybersecurity degree in Nevada will position the university, the Howard R. Hughes College of Engineering and the Lee Business School as leaders in an extremely important area of study with documented industry demand and good starting salaries for graduates. The degree program will combine rigorous coursework and interaction with industry professionals, and national competitions to produce highly qualified, cybersecurity professionals.

The program will provide exceptional students with technical and organizational training in the area of cybersecurity, which will prepare them for positions in this high-demand field. There is a large demand which is not being met by the national educational system, and Nevada is currently unable to provide graduates in this field, yet there is local and regional industry demand as evidenced by the willing participants in the surveys conducted. The program will appeal to students who are interested in becoming the technical and cyber leaders of tomorrow.

NSHE Academic Program Proposal - Five-Year Program Cost Estimate and Resource Requirements

Enter N/A if the information is not applicable to the program proposal

Program Resource Requirements. Indicate all resources needed including the planned FTE enrollment, projected revenues, and estimated expenditures for the first, third and fifth fiscal years of the program. Include reallocation of existing personnel and resources and anticipated or requested new resources. Third and fifth year estimates should be in dollars adjusted for inflation. If the program is contract related, explain the fiscal sources and the year-to-year commitment from the contracting agency(ies) or party(ies). Note: This form reflects the NWCCU's Substantive Change Budget Worksheet as of 8/28/17.

College/University: University of Nevada, Las Vegas | **Program: M.S. Cybersecurity**

I. PLANNED STUDENT ENROLLMENT

***Note*: Enrollment numbers (A + B) for each fiscal year should match the FTE/Headcount numbers in the Academic Program Proposal Form (Sect. I.ii.).**

	FY 1:	**2021**	**FY 3:**	**2023**	**FY 5:**	**2025**
	FTE	Headcount	FTE	Headcount	FTE	Headcount
A. New enrollments to the Institution	7.50	10	11.25	15	15.00	20
B. Enrollments from Existing Programs						

II. REVENUE

	FY 1:	**2021**	**FY 3:**	**2023**	**FY 5:**	**2025**
	On-going	One-time	On-going	One-time	On-going	One-time
1. New Appropriated Funding Request						
2. Institution Funds		$13,673				$39,823
3. Federal (e.g. grant, appropriation)						
4. New Tuition Revenues (registaration fee) from Increased Enrollments*	$42,863		$64,294		$85,725	
5. Other Student Fees (associated with the program)* Differential fee	$45,000		$67,500		$90,000	
6. Other (i.e., Gifts)						
Total Revenue	$87,863	$13,673	$131,794	$0	$175,725	$39,823

***Note*: Total Revenue (Section I) should match Total Expenditures (Section III)**

NSHE Academic Program Proposal - Five-Year Program Cost Estimate and Resource Requirements

Enter N/A if the information is not applicable to the program proposal

III. EXPENDITURES

	FY 1:	FY 2021	FY 3:	FY 2023	FY 5:	FY 2025
	On-going	One-time	On-going	One-time	On-going	One-time
A. Personnel Costs						
1. FTE (**Total FTE for all personnel types**)	0.825	0	0.825	0	1.325	
Faculty	0.25		0.25		0.75	
Adjunct Faculty	0.2		0.2		0.2	
Grad Assts						
Research Personnel						
Directors/Administrators	0.25		0.25		0.25	
Administrative Support Personnel	0.125		0.125		0.125	
Other: ________________						
	Expenditures for personnel type below must reflect FTE levels in Section A.1.					
2. Faculty	$45,063		$69,496		$121,414	
3. Adjunct Faculty	$22,248		$22,915		$23,602	
4. Graduate Assistants						
5. Research Personnel						
6. Directors/Administrators	$8,000		$8,000		$8,000	
7. Administrative Support Personnel	$5,262		$5,420		$5,582	
8. Fringe Benefits	$13,463		$13,463		$34,450	
9. Other:						
Total Personnel Costs	$94,036	$0	$119,294	$0	$193,048	$0

NSHE Academic Program Proposal - Five-Year Program Cost Estimate and Resource Requirements

Enter N/A if the information is not applicable to the program proposal

	FY 1: FY 2021		FY 3: FY 2023		FY 5: FY 2025	
	On-going	One-time	On-going	One-time	On-going	One-time
B. Operating Expenditures						
1. Travel						
2. Professional Services						
3. Other Services						
4. Communications						
5. Materials and Supplies (upgrades to compters)		$5,000		$10,000		$20,000
6. Rentals						
7. Marketing materials and Advertising	$2,500		$2,500		$2,500	
8. Miscellaneous						
Total Operating Expenditures	$2,500	$5,000	$2,500	$10,000	$2,500	$20,000

NSHE Academic Program Proposal - Five-Year Program Cost Estimate and Resource Requirements

Enter N/A if the information is not applicable to the program proposal

	FY 1: FY 2021		FY 3: FY 2023		FY 5: FY 2025	
	On-going	One-time	On-going	One-time	On-going	One-time
C. Capital Outlay						
1. Library Resources						
2. Equipment						
Total Capital Outlay	$0	$0	$0	$0	$0	$0
TOTAL EXPENDITURES (IIIA + IIIB + IIIC):	$96,536	$5,000	$121,794	$10,000	$195,548	$20,000
Note : Total Expenditures (Section IIIA-C total) should match Total Revenue (Section I)						

Budget Notes (optional):

UNLV | Howard R. Hughes College of ENGINEERING

University of Nevada, Las Vegas

26 May 2017

From: Rama Venkat,

Dean, and Engineering

To: Diane Z. Chase

EVP & P

Re: College's full-fledged support for the Interdisciplinary degree and certificate programs in Cyber Security

The Howard Hughes College of Engineering and Lee Business School propose joint interdisciplinary BS and MS degree programs and a graduate certificate program in Cyber Security. These programs will also include courses from College of Urban Affairs and Law School. Curricula for these programs are conceived after a series of "listening meeting" with local industry partners and in consultation with CSN. These programs will address the growing need for Cyber Security workforce. The curricula will provide the needed skillsets, knowledge and training as indicated by our community and industry partners.

Addition of these degree programs is consistent with college's strategic plan which calls for interdisciplinary degree programs which address the need of the technology sector in the region. These proposed programs also are consistent with Governor Sandoval's establishment of a state wide Center for Cyber Security. College supports these programs with much enthusiasm and confidence that it will help with the local economy. If you have any questions, please do not hesitate to contact me.

UNLV | LEE BUSINESS SCHOOL

UNIVERSITY OF NEVADA, LAS VEGAS

Date: April 9, 2019

From: Brent Hathaway, Dean Lee Business School
To: Diane Z. Chase, Executive Vice President and Provost
RE: Letter of support for interdisciplinary degree and certificate program in Cyber Security

Dear Provost Chase,

The Howard Hughes College of Engineering and Lee Business School propose joint interdisciplinary BS MS, and PhD programs along with a graduate certificate program in Cyber Security. Such programs are in high demand at the local, regional, and national levels. These programs will also include courses from College of Urban Affairs and the Law School. Curricula for these programs were conceived after a series of listening meeting" with local industry partners and in consultation with CSN, to address the growing need for a Cyber Security workforce. The curricula will provide the needed skillsets, knowledge and training as indicated by our community and industry partners.

The addition of these degree programs is consistent with the Lee Business School strategic plan, which calls for the establishment of effective collaborations with the community and other units on campus. These proposed programs also are consistent with Governor Sandoval's establishment of a state wide Center for Cyber Security. The LBS supports these programs and believes that producing graduates in these areas will help the local economy.

The Lee Business School will provide the required staffing to offer two class sections per year. Subsequent growth of the program will necessitate the university provide additional faculty lines in order to offer additional sections of these courses. I will meet with Dean Rama Venkat of the College of Engineering to discuss how our colleges will split funding that comes from this program.

If you have any questions, please do not hesitate to contact me.

Sincerely,

Brent Hathaway

UNLV | GRADUATE COLLEGE

Graduate Programs Committee
Graduate College
FDH 352. P.O. Box 451017
University of Nevada, Las Vegas
4505 S. Maryland Parkway,
Las Vegas, NV 89154-1017

September 22, 2019

Dear VPAP Rodriguez and Graduate Programs Committee Chair and Members,

Hello! I am writing to express my full support for the establishment of the proposed interdisciplinary M.S. program in Cybersecurity at UNLV, to be implemented in the 2020-2021 academic year (FY 2021). Cybersecurity is an extremely fast-growing field as evidenced by a growing demand at the local and national levels for an experienced workforce possessing knowledge of computers, networks, programs and apps, risk assessment and management, and strategic data security skills. Cybersecurity is broadly viewed as an emergent but critical field in the digital era, in which cyber defence and cyber offenses are needed to counter cyber-terrorism, cyber-warfare, industrial espinonage, data breeches, and the like. Aligned with UNLV's top tier mission, the program will prepare graduates for a number of career paths including but not limited to doctoral programs and careers in academia, private companies, government, and non-profit organizations.

In summer 2019, UNLV was granted an institutional wide designation as the Center of Academic Excellence (CAE) in cybersecurity by the National Security Agency. This highly prestigious designation provides students with unique resources and opportunities for education and recruitment which include (a) opportunities for the Department of Defense scholarships in cybersecurity and (b) preferential application privileges for post-graduation employment for government or government-based positions.

As an interdisciplinary program, our Master's in Cybersecurity will involve faculty with tenure lines from units across campus, including but not limited to the School of Business and the College of Engineering. This program will allow participating faculty to recruit and mentor higher-quality Master's students, which will enhance their ability to accomplish high-impact research and attract new funding for their research and related initiatives (e.g., equipment grants, training grants).

The program will be housed in the Graduate College and adhere to the Interdisciplinary Graduate Programs guidelines (https://www.unlv.edu/sites/default/files/page_files/27/Provost_Interdisciplinary-Grad-Degrees.pdf. Individual faculty from the cooperating units (Business and Engineering) will chair and serve as additional committee members for students' culminating activities, and teach classes that satisfy program requirements. The Graduate College's Associate Dean Lin will provide program support in collaboration with the Program Director. Fiscally, the program will be supported by the participating units to support this program and participating deans have signed a memo to this effect.

Thank you for your time and consideration. Please let me know if you need any additional information.

Sincerely,

Kathryn Korgan

Kate Korgan, Ph.D.
Dean, UNLV Graduate College
kate.korgan@unlv.edu

cc: Professor Greg Moody, Cybersecruity Program Director
Dean Rama Venkat, Howard Hughes College of Engineering
Dean Brent Hathaway, Lied School of Business
Associate Dean Emily Lin, Graduate College
Dr. Janet Dufek, Graduate Faculty Fellow for Interdisciplinary Programs 2019-2020

National Security Technologies LLC
Vision • Service • Partnership

F800-JM-17-0007

March 28, 2017

Dr. Diane Chase
Executive Vice President and Provost
University of Nevada, Las Vegas (UNLV)
4505 South Maryland Parkway
Las Vegas, NV 89154

Subject: **Letter of Support for a Cybersecurity Program at UNLV**

Dear Dr. Chase,

The need for cybersecurity talent has never been greater in the United States and particularly in the area of critical infrastructure defense and national security. One of our nation's largest challenges is defending against advanced cyber adversaries and finding skilled individuals to perform this work is extremely difficult. Just doing a search for cybersecurity professionals on any career site will reveal thousands of vacant positions and employers have no effective talent pipeline for early career candidates. UNLV is perfectly positioned to become a center of excellence by producing a highly trained and skilled cybersecurity workforce not only for Nevada, but the entire country.

As a member of the UNLV Howard Hughes College of Engineering Advisory Board, an adjunct professor for the College of Southern Nevada, and the Chief Information Officer of the Nevada National Security Site (NNSS), I have firsthand knowledge of the challenges that industry has trying to recruit cyber talent as well as the opportunities that UNLV has before it to meet these ever-growing needs. National Security Technologies (NSTec), the management and operating contractor for the NNSS, is the largest employer of engineers and scientists in Nevada and we have hired multiple UNLV students and graduates, including within our IT and cybersecurity programs.

NSTec has been extremely dedicated to UNLV and especially the STEM programs due to our mission. We would welcome the opportunity to be involved in cybersecurity program development at UNLV and look forward to the future of this program.

Respectfully,

Joshua S. Moulin, MSISA
Chief Information Officer

JM

cc: Correspondence Control

Sands

LAS VEGAS SANDS CORP.

March 15, 2017

RE: Letter of Support for a Cyber Security Program at UNLV

Dear Provost Chase and NSHE Board of Regents,

On behalf of the Las Vegas Sands Corp (LVSC), I am writing this support letter for developing a Cybersecurity Program at UNLV, which would be performed by the collaborative team of the Engineering and Business Colleges at the University of Nevada, Las Vegas. As the LVSC Senior Vice President Global Cybersecurity, I have a unique appreciation for the importance that cybersecurity education can play in the economic development of the entire state of Nevada. In my cybersecurity role, I have first-hand experience with the shortage of cybersecurity talent and resources. Over the coming years, I am tripling the size of my cybersecurity team adding over 60 cybersecurity professionals. This proposal will help produce a trained workforce that industries and communities desperately require.

A brief summary of resources Las Vegas Sands Corp (LVSC) has committed to UNLV:

1. UNLV and LVSC have established cross-collaborative opportunities for PhD fellowships in the area of big data analysis as well as Certified Ethical Hacker (CEH) scholarships.
2. LVSC cybersecurity subject matter experts regularly provide guidance to UNLV faculty serving as advisory board members for industry driven curriculum and inter-disciplinary studies.
3. LVSC provides cross-collaborative opportunities for students from internships, facility tours, job shadow opportunities, and assistance on student run cybersecurity projects.
4. LVSC cybersecurity subject matter experts regularly engage students on cybersecurity careers

In summary, cybersecurity education is vitally important for the future of Las Vegas Sands Corp, Nevada and the United States of America. UNLV has assembled a dynamic team of educators in the state. These individuals know and understand how this STEM proposal will be an economic driver for Nevada's growth and the integrated resort industry. UNLV has a vision for cybersecurity education that is vital for building a better tomorrow. This letter is for private correspondence only and may not be reproduced or published without the expressed written consent of LVSC.

Sincerely,

Ken Haertling
Senior Vice President Global Cybersecurity

SIM | WHERE IT LEADERS CONNECT

LAS VEGAS

March 19, 2017

Dr. Diane Chase
Executive Vice President, Provost
University of Nevada at Las Vegas

Dear Dr. Chase,

The Las Vegas Chapter for the Society for Information Management (SIM) is comprised of leaders in information technology (IT) management throughout the Las Vegas Metropolitan area. In addition to providing an exchange of ideas among peers in Southern Nevada, we strive to provide advocacy for important issues in IT, especially those surrounding education.

All our members feel the impact of a lack of enough skilled technology workers, especially in cybersecurity. This shortage is critical as cybersecurity threats are growing exponentially and threaten business viability and sustainability. All indications are that this problem will only get worse unless a significant investment is made in increasing the number of skilled workers in this area. The demand for these skills far outpaces the local availability.

Currently, to fill this need, Las Vegas companies are looking outside our area and hiring cybersecurity professionals from other universities and regions of the country. Oftentimes these new residents have difficulty in adjusting to the local culture, and as a result, retention of these professionals is not guaranteed.

The opportunity to grow Las Vegas cybersecurity professionals at UNLV would provide a much stronger chance of retaining qualified workers for our employers.

As the chair of the SIM Las Vegas Cybersecurity Committee, I fully support the development of a cybersecurity curriculum and degree program in the Engineering College at UNLV. I am confident that Southern Nevada employers would benefit greatly from this local talent and the opportunity for internships and job placements would be significant.

Sincerely,

Mary G Siero

Mary G. Siero, CISSP, CISM, CRISC
SIM Las Vegas Cybersecurity Committee Chair

As the President of SIM, I represent the Board, Officers, and members of SIM as we support the development of a cybersecurity curriculum and degree program in the Engineering College at UNLV for the reasons Ms. Siero has listed above.

Laura L. Fucci
Laura L Fucci

SIM Las Vegas President

UNLV Office of THE VICE PROVOST FOR UNDERGRADUATE EDUCATION

3-Year Academic Assessment Plan Cover Sheet

Email to: assessment@unlv.edu

Program Information:

Program Assessed	M.S. Cybersecurity
Department	CS/MET
College	Engineering / Business
Department Chair	Laxmi Gewali / Monica Sheng
Assessment Coordinator	Greg Moody
Date Submitted	Dec 1, 2017
Contact Person for This Plan	
Name	Greg Moody
Phone	895-1365
Email	Greg.moody@unlv.edu

Please address the following items:

- What are the student learning outcomes? Please provide a numbered list.

1. Evaluate the computer network and information security needs of an organization
2. Assess cybersecurity risk management policies in order to adequately protect critical resources and assets
3. Demonstrate a mastery of in-depth knowledge of cybersecurity
4. Formulate, update and communicate regarding organizational cyber-related strategies and policies

- **Plans must include a curriculum map showing which courses will address which learning outcomes.** Examples can be found here: http://provost.unlv.edu/Assessment/map.html

Table 1. Curriculum Map of M.S. Cybersecurity Learning Objectives

Required Courses in Program	Evaluate the computer network and information security needs of an organization	Assess cybersecurity risk management policies in order to adequately protect critical resources and assets	Possess a mastery of in-depth knowledge of cybersecurity	Formulate, update and communicate regarding organizational cyber-related strategies and policies
CSEC 701	M	M	M	
CSEC 702			M	M
CSEC 703	M	M	M	
CSEC 704		M	M	M
CSEC 705	E	E	E	E
CSEC 790	E	E	E	E

KEY: B = Beginning, M = Middle, E = End

B = outcome introduced in beginning of development, such as in introductory course

M = outcome covered in middle stages of development

E = outcome fully developed at the end of career, such as in a capstone course

- Which learning outcomes will be assessed in each cycle year (i.e., assessment timeline)?

Table 2. Assessment Schedule by Objectives

	Evaluate the computer network and information security needs of an organization	Assess cybersecurity risk management policies in order to adequately protect critical resources and assets	Possess a mastery of in-depth knowledge of cybersecurity	Formulate, update and communicate regarding organizational cyber-related strategies and policies
Where assessed?	CSEC 702, 705	CSEC 705	CSEC 705, 790	CSEC 705, 790
When assessed?	Annually in fall	Annually in fall	Annually in fall	Annually in fall

- How will the learning outcomes be assessed? (Programs must use at least one direct assessment of student learning.)

Table 3. Assessment Methods by Objectives

Learning Objective	Assessment Method
Evaluate the computer network and information security needs of an organization	**CSEC 702 & 705.** Culminating project for the course will be evaluated by two instructors in the program, that did not teach this course, to assess the learning outcome. Specifically, the evaluators will be rating the following: 1. Did students demonstrate the technical capability to gather and describe evidence relative to the security posture of the organization? (Ranked from 0-10) 2. Did students perform an effective evaluation of the evidence relative to the security posture of the organization/ (Ranked from 0-10) 3. Were actionable recommendations provided with the final project? (Ranked from 0-10)
Assess cybersecurity risk management policies in order to adequately protect critical resources and assets	**CSEC 705.** Culminating project for the course will be evaluated by two instructors in the program, that did not teach this course, to assess the learning outcome. Specifically, the evaluators will be rating the following: 1. Did the students accurately define, describe and provide a list of the critical resources and assets. How well was this accomplished? (Ranked from 0-10) 2. Did the students accurately identify and describe the security policies that related to these assets and resources? (Ranked from 0-10) 3. Did the students perform an evaluation of these policies and their ability to provide reasonable protection to the identified resources and assets? (Ranked from 0-10) 4. Were recommendations from this analysis clearly defined and provided in the project? (Ranked from 0-10)
Possess a mastery of in-depth knowledge of cybersecurity	**CSEC 705.** Culminating project for the course will be evaluated by two instructors in the program, that did not teach this course, to assess the learning outcome. Specifically, the evaluators will be rating the following: 1. How well does the student demonstrate general knowledge and mastery of all major cybersecurity domain areas? (Ranked from 0-10) **CSEC 790.** Thesis committee will be charged to assess this for each student. The average rankings for the program will

	be obtained from these individual assessments. Specifically, the committee will determine the following: 1. How well has the student demonstrated their mastery of cybersecurity in this chosen domain area? (Ranked from 0-10) 2. How well does the student demonstrate general knowledge and mastery of all major cybersecurity domain areas? (Ranked from 0-10)
Formulate, update and communicate regarding organizational cyber-related strategies and policies	**CSEC 705 & 790.** Culminating project for the course will be evaluated by two instructors in the program, that did not teach this course, to assess the learning outcome. Specifically, the evaluators will be rating the following (All ranked from 0-10: 1. **Content.** The extent to which the student uses data to support analyses and arguments **2.** **Organization.** The extent to which the student organizes ideas and makes arguments flow 3. **Logic.** Ideas are evaluated fairly and completely in support of the premise of the communication 4. **Grammar and Mechanics.** The extent to which the student uses the language properly 5. **Professionalism.** The extent to which the student's tenor and tone are appropriate for communication in this field

- Graduate programs should assess at least one outcome related to one of the following graduate level requirements each year:
    - student engagement in research, scholarship, creative expression and/or appropriate high-level professional practice.
        - **Assessment**. Each year the program will gather:
            - How many students are currently working on a thesis
            - Number of submissions to a conference or journal that has a student listed as a co-author
            - Number of acceptance proceedings or articles that has a student listed as a co-author
    - activities requiring originality, critical analysis and expertise.
        - **Assessment**. Culminating project from CSEC 705 will be used, as described above, to demonstrate critical analysis capabilities of students in the program.
    - the development of extensive knowledge in the field under study.
        - **Assessment**. Although not required by the M.S. in Cybersecurity, the following statistics will be gathered, to serve as external validators of students' domain knowledge of cybersecurity:
            - Number of students holding CISSP, or equivalent certification
            - Number of certificates completed by students during the year
            - Nature of the certificates being earned by students

- What is your plan for sharing the assessment results and acting on them (i.e., closing the loop)?

Assessment results will be summarized and reported to the appropriate offices. Recommendations, generated through the assessment function and then reporting, will then be shared in a program meeting held at the end of every spring. Specifically, the assessment coordinator will call the meeting during the reading week of Spring and cover the following points as agenda items:

1. Follow-up on assignments made at last annual meeting
2. Overall assessment results, by objective
3. Identified weaknesses in the program
4. Discussion
    a. How to address weaknesses
    b. Action plan, by objective and course
5. Assignments made to faculty and courses