



ACADEMIC PROGRAM PROPOSAL FORM

(Revised: January 2021)

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: April 18, 2024

Date of AAC Approval:
06-05-24

INSTITUTION: University of Nevada, Las Vegas

REQUEST TYPE: New Degree
 New Major or Primary Field of Study
 New Emphasis (BAS only)

Date of Board Approval:

DEGREE: Check applicable box

- | | |
|---|--|
| <input type="checkbox"/> Certificate: 30+ Credits | <input type="checkbox"/> Associate of Arts (AA) |
| <input type="checkbox"/> Associate of Science (AS) | <input type="checkbox"/> AA/AS |
| <input type="checkbox"/> Associate of Applied Science (AAS) | <input type="checkbox"/> Bachelor of Applied Science (BAS) |
| <input type="checkbox"/> Bachelor of Arts (BA) | <input checked="" type="checkbox"/> Bachelor of Science (BS) |
| <input type="checkbox"/> Master of Science (MS) | <input type="checkbox"/> Master of Arts (MA) |
| <input type="checkbox"/> Doctor of Philosophy (Ph.D.) | <input type="checkbox"/> Other or Named Degree: _____ |

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

INCLUDED IN THE NSHE PLANNING REPORT: Yes No

(Website for NSHE Planning Reports: <https://nshe.nevada.edu/administration/academic-student-affairs/reporting/planning/>

TOTAL NUMBER OF CREDITS TO PROGRAM COMPLETION: 121

PROPOSED SEMESTER/TERM OF IMPLEMENTATION: Fall 2025

Action requested (specify full program title):

The University of Nevada, Las Vegas requests approval of a new interdisciplinary B.S. Cybersecurity degree offered jointly by the Lee Business School and the Howard R. Hughes College of Engineering.

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 undergraduate bachelor of science in cybersecurity. This program would train students to enter into the cybersecurity field, and also serve as a feeder program for the recently launched M.S. Cybersecurity program, offered jointly by the Lee Business School and the Howard R. Hughes College of Engineering. 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>). These skills lie outside of any currently existing program in the state of Nevada. Students will be trained in technical and managerial aspects of cybersecurity.

This program 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 both the technical and managerial aspects of security and risk management that are needed for those entering into the cybersecurity field.

The program also builds on the strengths of the faculty in the department of computer science, who can provide the technical view and training for the foundations of technology and technological components of cybersecurity.

It is also positioned to accept CSN applied associate graduates from the cybersecurity program to transfer over into this program and earn their bachelor degree. This program is also adequately designed so that those from other fields that desire to enter into cybersecurity would be well served by this program.

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

1. Evaluate basic computer network and information security needs of an organization
2. An ability to understand risk governance and its application to cybersecurity in an organizational setting
3. Demonstrate a knowledge of foundational cybersecurity concepts and skills
4. Formulate, update, and communicate regarding cybersecurity to non-technologists

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 was submitted to the Office of Assessment and approved in September, 2022.

D. Contribution and relationship of program objectives to

i. NSHE Master Plan / Strategic Goals

a. Access – *Increase participation in postsecondary education*

This program will impact the following goals and metrics of the current NSHE Master Plan in regards to student access:

1. Many students are looking for college degrees that have clear goals and career pathways with well paying salaries and placement rates. This is one such program that aligns with these goals, as evidenced by statistics from the U.S. Department of Labor and Cyberseek.org
2. Further, we have already aligned the program with the existing 2-year program at CSN which focuses on cybersecurity. In that, following the correct pathways laid out with the Transfer officers, students can then transfer to UNLV into this program and in two years graduate with their B.S. in Cybersecurity, which further expands upon the knowledge obtained in the associate degree in cybersecurity obtained with CSN.
3. Several high schools and magnet schools in CCSD have Cyber Patriot clubs, which are national groups that train high school students in cybersecurity. Having an undergraduate opportunity at the local university affords such students a clear pathway to not only continue into postsecondary education, but to also stay in Nevada, as such a program is lacking at the university level in NSHE.

b. Success – *Increase student success*

This program will impact the following goals and metrics of the current NSHE Master Plan in regards to student success:

1. This program is focused on a career pathway that is completely untouched by regional academic programs, despite a large need within the employment sector. It will be a very attractive program for students because there are open jobs and they pay good salaries, which is likely to increase their completion of the program.
2. There is a large workforce demand for cybersecurity that NSHE institutions are not currently meeting. Cybersecurity is one of the largest growing fields, with no supply line from academic institutions. The latest estimates for the demand of cybersecurity professionals are maintained at cyberseek.org - which is 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.i.

c. Close the Achievement Gap – *Close the achievement gap among underserved populations*

This program will impact the following goals and metrics of the current NSHE Master Plan in regards to the student achievement gap:

1. Students of lower economic status are often most challenged to advance to the middle class. One of the surest ways to the middle class is through higher education, with placement in a career that pays prevailing wages. The annual average salary of an individual with a bachelor in cybersecurity in Nevada is around \$75,000 for the entry level position¹ (i.e., those requiring an associates or bachelor degree, or equivalent professional certification or experience). Such a salary is above the national average, and with a low cost of obtaining the degree, the ROI on such a degree is an impactful way to provide upward class mobility.

¹ <https://www.salary.com/research/salary/posting/entry-level-cyber-security-analyst-salary/las-vegas-nv>

d. Workforce – Collaboratively address the challenges of the workforce and industry education needs of Nevada

This program will impact the following goals and metrics of the current NSHE Master Plan in regards to student workforce:

1. One of the largest skill gaps in the valley is technical skills, with most local companies and executives having to recruit from outside of the valley to obtain crucial technical skills. By providing more pathways for technical postsecondary education, the workforce of Nevada, especially Southern Nevada, will be better able to diversify, but also importantly and critically for this career pathway, it is needed in all industries as cybersecurity is fundamental and critical resource needed in all industries due to the rise and reliance of technology.

e. Research – Co-develop solutions to the critical issues facing 21st century Nevada and raise the overall research profile

Starting with several initiatives at the federal and state level (e.g., AB 471), cybersecurity has been identified as a critical area for national security and for workforce development. To help aid in this development, the NSF, DOE, and DOD are all heavily invested in the growth of these technologies through basic research. Thus, millions of dollars in grant funds are available to aid in research and development in these areas. Currently, faculty associated with this program and the CAE for Cybersecurity Defense at UNLV are attempting to secure such funds to aid in the continued research in this domain.

ii. Institutional mission and core themes

As part of the Top Tier initiative, the goals for research, scholarship and creative activity metrics will be directly impacted by this program. These metrics are taking directly from UNLV's Top Tier initiative.

1. UNLV Metric: Increase breadth and depth of economic and cultural impact of the university's activities on the community, as measured by impact of campus/community cultural events, increased engagement with K-12 education, partnerships with non-profits and public institutions to address social issues, invention disclosures, patents applied for and granted, licensing deals (both exclusive and nonexclusive), number of startups, other intellectual property, revenues, and jobs created from innovations initiated at UNLV.

Partnerships with our local community will be impacted, as this program has partnerships with local community and cybersecurity organizations. 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, which will be helped with volunteers from our students to serve as mentors and coaches for these teams.

Collaboration with CSN: CSN has started a two-year applied associates degree in cybersecurity, which will allow students that complete that degree to then transfer to UNLV and complete their B.S. and M.S. in cybersecurity. The B.S. and M.S. programs are being constructed in a way to will allow such a pathway from our local community college program to higher degree programs at UNLV.

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.

2. UNLV Metric: Increase breadth and depth of graduate and undergraduate student participation in research.

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. Thus, the number of students working in a lab will also increase. This would then have spillover impacts on students engaging in research and presenting in conference through their involvement with faculty research within this laboratory setting. These interactions would directly result in more students engaging in research with faculty.

3. UNLV Metric: Workforce development and diversification derived from UNLV's highly qualified graduates who readily gain employment in their preferred careers, particularly in STEAM fields (Science, Technology, Engineering, Arts and Mathematics).

This is a STEM designated degree and will directly impact this metric by 1) providing the first degree pipeline in Nevada for students in cybersecurity, which has a large workforce demand in the local economy, regionally, and nationally. It is part of the Governor's plan for economic diversification. Cybersecurity has been identified by the Governor of Nevada as one area of economic diversification, supported by the recent development of a Cyber Defense Office for the State of Nevada.

4. UNLV Metric: Inclusion of the community to advance development and fundraising.

This degree proposal was in large part due to the demand from over 40 industry partners who requested it and serve as industry advisors. Please refer to the attached letters of support from various industry partners.

iii. Campus strategic plan and/or academic master plan

As referenced in section ii above, the proposed degree supports several pathway goals of the Top Tier 2.0 Strategic Plan and it was included in the most recent academic master plan for UNLV. It contributes to the strategic plan of the Lee Business School 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

iv. Other programs in the institution

There are two relevant cybersecurity programs at UNLV.

1. Existing graduate certificate program in emergency crisis management cybersecurity (<https://www.unlv.edu/certificate/emergency-crisis-management-cybersecurity>) under the department of Criminal Justice. This program takes the specific angle of how to train government officials placed in an emergency management position how to respond to a cybersecurity related emergency at the local, county or state level.
2. Existing graduate program in cybersecurity. The proposed program would serve as a feeder for this program and would be complementary.

v. Other related programs in the System

There are three relevant cybersecurity programs within NSHE.

1. The previously mentioned applied associate degree program in cybersecurity with CSN, which allows students to transfer and immediately start working on the upper undergraduate level courses for this program.
2. UNR offers an interdisciplinary minor in cybersecurity, and a regular minor in cybersecurity. Each is modeled off of the same approach. These degrees are essentially non-overlapping in skillsets outside of the fundamental concepts of cybersecurity and technology.
3. UNR offers an online graduate degree and certificate in cybersecurity. Both of these would be well served as potential outcomes for future education for students in this proposed B.S. Cybersecurity program.

vi. If the program was not included in the NSHE Planning Report, please explain why.

This program is listed in the Planning Report.

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 discipline in this area needs to be created.

The federal government is also highly interested in cybersecurity educational efforts, having created the National Initiative for Cybersecurity Education (NICE), which will be providing millions of dollars in 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.

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 established pipeline for entry-level cybersecurity talent and it has 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 would eliminate these issues, filling 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 over 5,664 local jobs that are unfilled (per cyberseek.org) in the state of Nevada. Further, discussions with local companies, such as Caesars, CapitalOne, Sands, Bally's, IGT, Southwest Gas, NV Energy, NSTec, etc. all have expressed a large concern with the inability to hire local, talent in this area. We have an existing advisory board for cybersecurity which actively supports the creation of this program and members of this board, from various industries have written letters of support for this proposal.

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 (<https://www.bls.gov/oes/current/oes151212.htm>). Currently, there are about 77,000 cybersecurity jobs in California and nearly 20,000 in Arizona, where half of the positions cannot be filled due to worker shortage, [Cyberseek.org](http://cyberseek.org).

This regional shortage also puts great pressure on the cybersecurity job market in Nevada. 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://ir.nevada.edu/page.php?p=completion_and_workforce) 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 11% in the long-term for security analysts and for more general computer occupations, it is projected to grow by 24%. Overall, each of the subdisciplines that could be employed by individuals with this degree range from 11-24% projected growth rates.

This shows that there are roughly 25,000 annual openings in the area of Computer Occupations, with an annual growth rate of 6%.

Based on the graduation rates of computer science and management information sciences students (the nearest degrees available to cybersecurity), the supply in this area does not reach the current shortfalls in these domains. This information is based on very high-level job descriptors of those who have a background in computer science only. 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/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 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

Any student at UNLV is available to join this program. It is focused on the strengths of UNLV and will be offered as an in-person degree offering.

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

The initial launch of cybersecurity education at UNLV began with a taskforce created under the direction of the dean of the Howard R. Hughes College of Engineering. It consisted of faculty from business, engineering, law, and urban development and industry partners.

The first meeting focused on the desired outcomes and skillsets of the individuals. But it was high-level only, as it was uncertain as to what current programs existed at UNLV. This was addressed at the taskforce's second meeting. This presented 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, which requested more skills, which would require 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. Further plans for the development of this undergrad degree were placed on hold until the successful creation and launch of the graduate program, which began in Spring 2020.

Members of approximately 13 local cybersecurity/information technology associations have promised support and opportunities for networking, job placement, and internships for students. Working with this continued group, which has since formally adapted into an advisory board for the cybersecurity education at UNLV, this program was developed and refined.

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

The program will reside in the Office of Undergraduate Studies, as an interdisciplinary degree program. The hosting of the program will be jointly shared and rotated between faculty members in the departments of Computer Science (Engineering) and Management, Entrepreneurship and Technology (Business).

v. The timetable, with dates, for implementation steps

Faculty voted to approve the proposal of the new degree on 2/2/2024. The provost's office approved the proposal on 3/20/24. The faculty senate voted to approve the program on 4/18/2024. If approved by the Board of Regents, the program will begin enrolling students in Fall 2025.

vi. If this or a similar program already exists within the System, what is the justification for this addition? Please describe the nature and extent of the consultation with other institutions that have similar programs.

See section D subsections iv and v above.

This program is offered at a less technical level of expertise than the other existing programs. It is anticipated that graduates of this program occupy other career pathways within cybersecurity outside of the more technical roles being focused on by the other existing programs from UNLV and UNR.

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 and/or any other applicable sources.

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 over 5,664 local jobs that are unfilled (per cyberseek.org) in the state of Nevada. Further, discussions with local companies, such as Caesars, CapitalOne, Sands, Bally's, IGT, Southwest Gas, NV Energy, NSTec, etc. all have expressed a large concern with the inability to hire local, talent in this area. We have an existing advisory board for cybersecurity which actively supports the creation of this program and members of this board, from various industries have written letters of support for this proposal.

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 (<https://www.bls.gov/oes/current/oes151212.htm>). Currently, there are about 77,000 cybersecurity jobs in California and nearly 20,000 in Arizona, where half of the positions cannot be filled due to worker shortage, Cyberseek.org.

This regional shortage also puts great pressure on the cybersecurity job market in Nevada. 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://ir.nevada.edu/page.php?p=completion_and_workforce) 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 11% in the long-term for security analysts and for more general computer occupations,

it is projected to grow by 24%. Overall, each of the subdisciplines that could be employed by individuals with this degree range from 11-24% projected growth rates.

This shows that there are roughly 25,000 annual openings in the area of Computer Occupations, with an annual growth rate of 6%.

Based on the graduation rates of computer science and management information sciences students (the nearest degrees available to cybersecurity), the supply in this area does not reach the current shortfalls in these domains. This information is based on very high-level job descriptors of those who have a background in computer science only. 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/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 for 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)

Specific program requirements:

Foundations in Business (18 credit hours)

- COM 101: Oral Communication
- MGT 301: Principles in Management and Organizational Behavior
- BLW 302: Legal and Ethical Environment of Business
- BUS 321: Business Communications
- IS 330: Strategic Management of Technology and Innovation
- ENG 407B: Fundamentals of Technical Writing

Foundations in Computer Science (9 credit hours)

- CS 138: Programming for Data Science I
- CS 238: Programming for Data Science II
- **CSEC 210: Computer Science Fundamentals

Foundations in Technology (6 credit hours)

- **CSEC 112: Network+
- **CSEC 174: Linux System Administration

Foundations in Cybersecurity (9 credit hours)

- **CSEC 100: Introduction to the World of Cybersecurity
- CS 251: Security Concepts
- **CSEC 220: Network Security

Cybersecurity Core Requirements (18 credit hours) – taken in a cohort approach

- **CSEC 300: Cybersecurity Data Analytics (FALL)
- **CSEC 301: Operating Systems Security (FALL)
- **CSEC 302: Audit and Compliance (FALL)
- **CSEC 303: Website Administration and Security (FALL)
- **CSEC 310: Cyberlaw, Privacy and Ethics (SPRING)
- **CSEC 311: Vulnerability Assessment and Practice (SPRING)
- **CSEC 312: Security Management (SPRING)
- **CSEC 313: Cyber Clinic Methods (SPRING)

Cybersecurity Culminating Requirements (21 credit hours)

- **CSEC 400: Cloud and Data Center Security
- **CSEC 401: Perimeter Security
- **CSEC 402: Wireless Network Security
- **CSEC 403: Digital Forensics
- **CSEC 404: Secure Systems Analysis and Design
- **CSEC 405: Cybercrimes, Law and International Issues
- **CSEC 450: Cyber Clinic Practicum (Culminating Experience)

Typical Four-Year Plan

First year:

First Semester

- CSEC 100
- ENG 101
- MATH 126
- BUS 103 or EGG 101
- COM 101
- CS 138

Second Semester

- CS 238
- ENG 102
- MATH 127
- US & NV Constitution
- Fine Arts

Second Year

First Semester

- CSEC 112
- CSEC 110
- CSEC 210
- Humanities/International
- Second-year seminar

Second Semester

- IS 101
- CSEC 220
- CS 251
- BUS 321
- CSEC 174

Third Year

First Semester

- CSEC 300
- CSEC 301
- CSEC 302
- CSEC 303
- IS 330

Second Semester

- CSEC 310
- CSEC 311
- CSEC 312
- CSEC 313
- BLW 302

Fourth Year

First Semester

- CSEC 400
- CSEC 401
- CSEC 402
- MGT 301
- ENG 407B

Second Semester

- CSEC 403
- CSEC 404
- CSEC 405
- CSEC Elective
- CSEC 450

ii. Program entrance requirements

- Complete 55 credits (earned or in progress)
- Currently have a 2.75 UNLV GPA or, a 2.75 transfer GPA if this is your first semester at UNLV and you meet all of the other entrance requirement
- All pre-major grades are recorded in the MyUNLV system and/or attach unofficial transcripts showing grades for pre-major

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

All courses in the major requirements section must be completed with a grade of C or better.

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

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

G. Method of Delivery (for the purpose of state authorization [NC-SARA])

- i. **How will this academic program be delivered when the program begins?
(mark all that apply)**

- 100% face-to-face courses
 Hybrid (some online courses, some face-to-face courses)
 100% online courses

- ii. **Learning Placements**

Does the academic program have learning placements (e.g. internships, externships, clinical placements, student teaching, etc.) that *may take place outside the state of Nevada?*

- Yes
 No.

H. Institutional Review Process

- i. **Date of Faculty Review (may include additional information, as needed)**

The UNLV Faculty Senate Curriculum Committee approved the program on 4/18/2024.

- ii. **Describe the process for review and approval by the appropriate academic policy body of the institution**

The provost's office reviewed the proposal and approved it before submission in to the Curriculog platform, which allowed review and approval by various stakeholders in the university, culminating with the Faculty Senate approval.

I. Readiness to begin program

- i. **List the educational and professional qualifications of the faculty relative to their individual teaching assignments**

There are currently several faculty associated with this program, and the expertise to help its initiation.

- The first is a Lee 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 15 A+ publications, and over 50 peer-reviewed publications

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

- The second is an assistant professor of information systems that has a specialty of behavioral cybersecurity, and has previous professional certification experience, both in terms of having earned them and having instructed courses towards professional certification. This tenure-track faculty member has published in premier academic journals for his discipline.
- The third faculty member was recently hired by the university and is an expert in analytics, which is one of the main foci of the program. This faculty member has a Ph.D. and a few publications in the analytics area.
- The fourth faculty member is a full professor with a background in computer science. He has obtained numerous grants in relation to cybersecurity and has published extensively in this area. He also assists in the graduate program and has a specialty in encryption and other cyber-related areas.
- The fifth faculty member is a full professor with a background in computer science. She has also obtained numerous grants in relation to cybersecurity and has published extensively in this area. She also assists in the graduate program.
- The sixth faculty member is a faculty in residence in the area of computer science who has an extensive background in teaching the technological foundations and other related material that would be of use for this program.

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 their area of expertise. Industry partners will provide qualified, certified instructors that can help start and build the program. Administrative support would come from existing administrative assistant. Additional faculty resources will be requested by deans through established request processes.

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 the B.S. in both Information Systems and Computer Science offered by the parent departments. Cybersecurity is a related field, but is not as diverse as Information Systems nor is Cybersecurity as focused as Computer Science. Cybersecurity is focused on one specific career pathway, which is not well served by the IS or CS programs alone.

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

N/A

J. Resource Analysis

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

Student tuition (differential fees) will support the program in addition to regular support offered by the department and college. A differential fee proposal will be submitted to the Board of Regents for approval.

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 24

3rd Fall semester 72

5th Fall semester 120

(2) Explain the methodology/assumptions used in determining projected FTE figures.

The projected FTE was determined using the formula documented in the NSHE Procedures and Guidelines Manual, Chapter 6, Section 2. FTE is computed by multiplying the number of students times the average number of credits they will be taking (12) and then dividing that number by 15.

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

1st Fall semester 30

3rd Fall semester 90

5th Fall semester 150

(2) Explain the methodology/assumptions used in determining projected headcount figures.

These numbers are believed to be as accurate as possible based on interest in the degree from a current student club interested in cybersecurity, current students and alumni who have expressed interest, and the interest expressed by industry partners in having their employees complete the degree. CSN has an associate degree in cybersecurity and some of them are anticipated to matriculate to UNLV to complete the bachelor degree.

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

See attached cost estimate.

K. 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

No additional facilities are 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 college involved, with the appropriate dean requesting any additional space approximately one year before it is needed.

iii. Existing and additional equipment required

Following the path of the M.S. Cybersecurity program, a cyberrange will be required in order to provide the tools necessary to train students on the architecture, at scale, and in a realistic setting. Fortunately, we can adjust the contract that is already in effect for the M.S. program to include more licenses for the undergraduate students to also be serviced by the same platform. As the cost per license is roughly \$3,500-\$4,000 per student, depending on the number of total licenses the program will request a differential fee structure, mainly to cover this large expense.

L. Describe the adequacy and availability of library and information resources

Existing resources are adequate.

M. 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 existing advisors in the participating colleges will be able to advise students regarding the program requirements and courses.

ii. Describe the implications of the program for services to the rest of the student body

No major implications are expected.

N. 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

O. Articulation Agreements

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

CSN transfer articulation is completed.

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

P. Summary Statement

The creation of the first bachelor degree in cybersecurity in Nevada will position the university as a leader 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: <u>B.S. Cybersecurity</u>			
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: FY _25__		FY 3: FY _27__		FY 5: FY _29__		
	FTE	Headcount	FTE	Headcount	FTE	Headcount	
A. New enrollments to the Institution	24	30	72	90	120	150	
B. Enrollments from Existing Programs							
II. REVENUE							
	FY 1: FY ____		FY 3: FY ____		FY 5: FY ____		
	On-going	One-time	On-going	One-time	On-going	One-time	
1. New Appropriated Funding Request							
2. Institution Funds		\$205,837					
3. Federal (e.g. grant, appropriation)							
4. New Tuition Revenues (registraration fee) from Increased Enrollments*	\$126,450		\$409,725		\$568,350		
5. Other Student Fees (diff fees)*	\$0		\$157,500		\$258,750		
6. Other (i.e., Gifts)							
Total Revenue	\$126,450	\$205,837	\$567,225	\$0	\$827,100	\$0	
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 ____		FY 3: FY ____		FY 5: FY ____	
		On-going	One-time	On-going	One-time	On-going	One-time
A. Personnel Costs							
1. FTE (Total FTE for all personnel types)		2.8	0	4.425	0	5.175	0
	Faculty	2		2		2	
	Adjunct Faculty			1.5		2.25	
	Grad Assts						
	Research Personnel						
	Directors/Administrators	0.05		0.05		0.05	
	Administrative Support Personnel	0		0.125		0.125	
	Other: _hourly_____	0.75		0.75		0.75	
		Expenditures for personnel type below must reflect FTE levels in Section A.1.					
2. Faculty		\$214,000		\$235,935		\$286,780	
3. Adjunct Faculty				\$45,000		\$67,500	
4. Graduate Assistants							
5. Research Personnel							
6. Directors/Administrators		\$15,000		\$15,000		\$15,000	
7. Administrative Support Personnel				\$6,369		\$7,022	
8. Fringe Benefits		\$71,007		\$90,681		\$111,711	
9. Other: Hourly		\$20,280		\$21,840		\$23,400	
	Total Personnel Costs	\$320,287	\$0	\$414,825	\$0	\$511,413	\$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 ____		FY 3: FY ____		FY 5: FY ____		
	On-going	One-time	On-going	One-time	On-going	One-time	
B. Operating Expenditures							
1. Travel			\$5,400		\$5,400		
2. Professional Services					\$67,500		\$450 per st
3. Other Services							
4. Communications							
5. Materials and Supplies			\$135,000		\$225,000		
6. Rentals							
7. Marketing materials and Advertising	\$12,000		\$12,000		\$17,787		
8. Miscellaneous							
Total Operating Expenditures	\$12,000	\$0	\$152,400	\$0	\$315,687	\$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 ____		FY 3: FY ____		FY 5: FY ____	
		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):		\$332,287	\$0	\$567,225	\$0	\$827,100	\$0
Note: Total Expenditures (Section IIIA-C total) should match Total Revenue (Section I)							

Budget Notes (optional):

Professional services: \$450 per student in year 5 (DEFCON - Senior year), Field Trip, Competitions, Awards, Harvard Business Review(Cases)

Materials and Supplies: Cyberbit \$1,500 per student per year

3-Year Academic Assessment Plan Cover Sheet

Email to: assessment@unlv.edu

Program Information:

Program Assessed	B.S. B.A. Cybersecurity
Department	MET
College	Business
Department Chair	Rajiv Kishore
Assessment Coordinator	Greg Moody
Date Submitted	Sept 1, 2022
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 basic computer network and information security needs of an organization
 2. An ability to understand risk governance and its application to cybersecurity in an organizational setting
 3. Demonstrate a knowledge of foundational cybersecurity concepts and skills
 4. Formulate, update and communicate regarding cybersecurity to non-technologists

- **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 B.S. B.A. Cybersecurity Learning Objectives

Required Courses in Program	Evaluate basic computer network and information security needs of an organization	An ability to understand risk governance and its application to cybersecurity in an organizational setting	Demonstrate a knowledge of foundational cybersecurity concepts and skills	Formulate, update and communicate regarding cybersecurity to non-technologists
CSEC 401	B		B	
CSEC 402			B	B
CSEC 403		B		B
CSEC 410	M		M	
CSEC 411	M	M	M	M
CSEC 412	M	M	M	M
CSEC 480	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, review and application focus

E = outcome fully developed at the end of program, 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 basic computer network and information security needs of an organization	An ability to understand risk governance and its application to cybersecurity in an organizational setting	Demonstrate a knowledge of foundational cybersecurity concepts and skills	Formulate, update and communicate regarding cybersecurity to non-technologists
Where assessed?	CSEC 480	CSEC 480	CSEC 480	CSEC 480
When assessed?	Annually	Annually	Annually	Annually

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

Table 3. Assessment Methods by Objectives

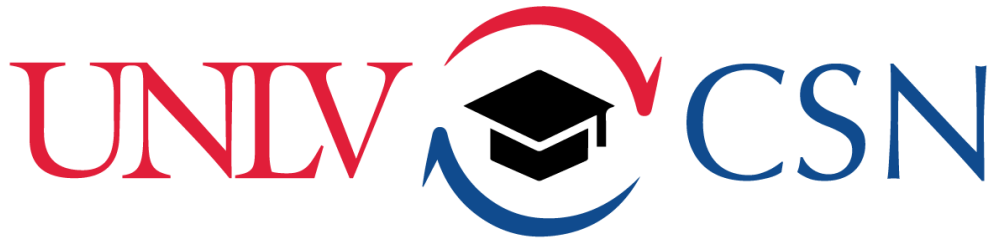
Learning Objective	Assessment Method
Evaluate basic computer network and information security needs of an organization	Culminating project for the program will be evaluated by two external evaluators to assess the learning outcome. Specifically, the evaluators will be rating the following: <ol style="list-style-type: none"> 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)
An ability to understand risk governance and its application to cybersecurity in an organizational setting	Culminating project for the program will be evaluated by two external evaluators to assess the learning outcome. Specifically, the evaluators will be rating the following: <ol style="list-style-type: none"> 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)
Demonstrate a knowledge of foundational cybersecurity concepts and skills	Culminating project for the program will be evaluated by two external evaluators to assess the learning outcome. Specifically, the evaluators will be rating the following: <ol style="list-style-type: none"> 1. How well does the student demonstrate general knowledge of relevant cybersecurity domain areas to this project? (Ranked from 0-10)

<p>Formulate, update and communicate regarding cybersecurity to non-technologists</p>	<p>Culminating project for the program will be evaluated by two external evaluators to assess the learning outcome. Specifically, the evaluators will be rating the following:</p> <ol style="list-style-type: none"> 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
---	--

- 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



TRANSFER PROGRAM

TRANSFER AGREEMENT: 2025-2026

University of Nevada Las Vegas Bachelor’s Degree Program:

Bachelor of Science – Cybersecurity

College of Southern Nevada Associate’s Degree Program:

AS in Computer Science

CSN	Fall – 1st year	Total Credits: 15
------------	------------------------	--------------------------

Course	Prerequisite	Credits
ENG 100 OR 101 OR 110 OR 113 (C or better)	English Placement Test; or completion of ENG 098 with a grade of C- or better; or ESL 139 with a grade of C- or better	3
MATH 127 or Above		3
EGG 101		3
FINE ARTS		3
COM 101		3

CSN	Spring – 1st year	Total Credits: 16
------------	--------------------------	--------------------------

Course	Prerequisite	Credits
ENG 102 OR 114 (C or better)	ENG 100/101/101H/113 with a grade of C- or higher	3
EGG 131		3
CIT 112		3
PHIL 242		3
CIT 114		4

CSN		Fall – 2nd year	Total Credits: 14
Course	Prerequisite		Credits
PSC101			4
CIT 173			3
CS 138			4
Special Program Electives	Recommended: BUS 101; MGT 201, CSEC 110, CSEC 131, CSEC 226		3

CSN		Spring – 2nd year	Total Credits: 16
Course	Prerequisite		Credits
ENG 231 OR 232 (Values & Diversity)	ENG 100 or 101 or 101H or 113 with a grade of C- or higher		3
CIT 217			3
CS 238			3
Special Program Electives	Recommended: BUS 101; MGT 201, CSEC 110, CSEC 131, CSEC 226		4
Special Program Electives	Recommended: BUS 101; MGT 201, CSEC 110, CSEC 131, CSEC 226		3

Total Credits at CSN: 61

Multicultural and International requirements waived if CSN AA, AS, or AB is completed.

UNLV		Fall – 3rd year	Total Credits: 15
Course	Prerequisite		Credits
CSEC 300			3
CSEC 301			3
CSEC 302			3
CSEC 303			3

UNLV		Spring –3rd year	Total Credits: 15
Course	Prerequisite		Credits
CSEC 310			3
CSEC 311			3

Course	Prerequisite	Credits
CSEC 312		3
CSEC 313		3
CSEC Elective		3

UNLV	Fall – 4th year	Total Credits:15
-------------	------------------------	-------------------------

Course	Prerequisite	Credits
CSEC 400		3
CSEC 401		3
CSEC 402		3
ENG 407B		3
CSEC Elective		3

UNLV	Spring – 4th year	Total Credits:15
-------------	--------------------------	-------------------------

Course	Prerequisite	Credits
CSEC 403		3
CSEC 404		3
CSEC 450		3
CSEC 405		3
CSEC Elective		3

Total Credits at UNLV:60

Degree Total: 121

Program Specific Information: Grades of a C or higher must be earned in any English, Mathematics, Science, and Engineering courses. For more information on this program refer to <http://engineering.unlv.edu/>.

The Howard R. Hughes College of Engineering and the Lee Business School have policies on the maximum number of attempts that are allowed to successfully complete a course in the undergraduate curriculum. Students are allowed a maximum of three attempts in an engineering, computer science, construction management, or business course. Under this policy, the attempts

include all attempts that result in a course grade of “A-F”, “AD”, “S/U”, “I” or “W”. The only exceptions to the repeat rule could include withdrawals for medical or military duties.

Transfer Policies:

REVISED 50/50 RULE

- The policy stating that UNLV will only accept up to 60 credits to be transferred and applied to any specific program/major is no longer in place. Unless a college/major has a specific requirement on credit limitations i.e., Lee Business School, College of Education, transfer credits from 2-year institutions should no longer be limited to 60 credits. At least 30 credits of upper division from UNLV are now required to obtain a Bachelor's.

REPEAT POLICY

- Students may retake a CSN course as often as needed to gain a better grade and, thereby, a higher grade point average. Only the highest grade received will count as part of the total CSN grade point average. All repeated courses taken at CSN will remain as part of a student's permanent academic record.
*PLEASE NOTE: While CSN accepts the BEST grade, UNLV accepts the LAST grade.
- To improve GPA and change the original grade the course must be repeated at the institution that it was completed. For example, if a student takes MATH 124 at CSN and receives an F the course must be repeated at CSN to replace the grade and improve the GPA.

REVERSE TRANSFER

- Students who have earned 15 or more credits at CSN and have transferred to a four-year institution without an associate's degree may “reverse transfer” the earned credits from the four-year institution to complete an associate's degree. This process makes it possible for students to earn an associate's degree as they continue to work toward completing their bachelor's degree.

NOTE: Some courses that fulfill specific general education requirements at CSN may fulfill different general education requirements at UNLV. Please see a UNLV/CSN Transfer Program Advisor to confirm your choices.

Revised on: 5/6/24

March 9, 2023

From: Rama Venkat, Dean, HRH College of Engineering

To: Chris Heavey, Executive Vice President and Provost

Re: Dean's Memo from the College of Engineering in support of the proposed new Bs degree in Cyber Security...



I am delighted to support the creation of a new BS degree program in Cyber Security. This is an important area of global significance right now and will stay that way as long as we have technologies which interact with one another through communication, which will have to be secure. The research, development and workforce demand this for area of technology is enormous and is expected to grow exponentially in the coming decades. Thus, there is a need for degree programs from associate degrees to Ph.D. degrees. UNLV has already successfully developed an interdisciplinary MS degree in Cyber Security. This program has a healthy enrollment in the first year of its offering. A BS degree is needed to

- (1) satisfy the enormous need for a BS degree work force in this technology area locally and regionally
- (2) develop a pipeline for the MS degree .

If the program gets initial funding to hire the needed faculty lines, both tenure track and non-tenure track, with the charging of differential fees, the program can be sustained. The differential fees will also be necessary to buy the necessary hardware and software. For the program. These faculty lines may be able to help with the existing MS degrees and also pave way for a future PhD degree.

The program can be offered using existing classrooms and the laboratory space that is already allocated for the MS in Cyber Security Program.

In summary, I am very enthusiastic about the new degree program and the college of engineering supports it whole heartedly and will work to provide the personnel and intellectual resources necessary to stand up a successful degree program and sustain it. If you have any questions, please do not hesitate to contact me.

September 9, 2022

Office of the Provost
University of Nevada, Las Vegas
4505 S. Maryland Parkway
Las Vegas, NV 89154

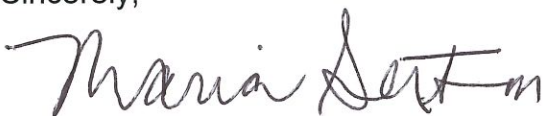
Greetings –

I write this letter to declare my wholehearted and emphatic endorsement of a BS Cybersecurity program at UNLV. The need for educated and skilled cybersecurity professionals is at an all-time high, with no foreseeable end in sight. As our adversaries grow in number and sophistication, we too must advance our practice and our defenses. The limited pool of candidates and the fierce competition among employers is making for a perfect storm. This is the single biggest risk we face as Cybersecurity leaders, a concern echoed in every roundtable, conference and event I attend.

Establishment of a BS Cybersecurity program will serve to not only increase the number of professionals entering the industry and supply a larger candidate pipeline for hiring managers like myself, it clearly demonstrates UNLV's strong and continued commitment to providing education opportunities in highly desirable fields.

I am a proud graduate of the UNLV MIS Program Class of 2004, and am privileged to submit this letter of endorsement. Please let me know how I can help make this important endeavor a reality for our industry and our community.

Sincerely,



Maria Sexton
Chief Information Officer
University Medical Center of Southern Nevada



September 7, 2022

University of Nevada, Las Vegas
4505 S. Maryland Parkway
Las Vegas, NV 89154

Dear Office of the Provost,

I am writing in support of the proposal to develop a new bachelor's degree program in cybersecurity at UNLV. I have reviewed the planned coursework and believe that this would be a great addition to the current program offerings.

As an information security executive at one of Nevada's largest employers, I see the continued demand for cybersecurity talent on a regular basis. I believe that this demand will continue to increase in Nevada as gaming companies continue to expand their digital ecosystems to better serve customers. The proposed cybersecurity program would adequately prepare UNLV students to start careers in cybersecurity and help address the current shortage of talent in the industry.

Sincerely,

A handwritten signature in black ink, appearing to be "BN" with a long, sweeping underline.

BRANDEN NEWMAN
SVP, CHIEF INFORMATION SECURITY OFFICER
MGM RESORTS INTERNATIONAL