EXECUTIVE SUMMARY

Item Name: **Request for New Academic Programs for Northern Arizona University**

☒ Action Item

Requested Action: Northern Arizona University asks the board to approve the new program requests effective in the 2020-2021 academic year.

Background/History of Previous Board Action

- As provided in board policy, Academic Strategic Plans may be modified during the year with the approval of the Academic Affairs and Educational Attainment Committee.

- The demand for cybersecurity related careers in Arizona is particularly acute. According to CyberSeek, a workforce and career resource which tracks the supply and demand in the Cybersecurity job market, there are more than 7,000 open cybersecurity positions in Arizona with 15,000 individuals currently employed in this sector. The Greater Phoenix Chamber of Commerce has identified four priority workforce sectors in their Phoenix Forward initiative and Cybersecurity is included as a priority area of workforce need in the Phoenix metropolitan area as identified by business leaders, The Phoenix Chamber states, "Unfortunately for businesses, there is a jobs gap in the cybersecurity industry. Arizona's supply of cybersecurity professionals is low and the demand for these experts is high."

- Demand for cybersecurity education is similarly high. In a study conducted by Engine Insight, 1,004 adults across the United States were surveyed about cybersecurity education and 41% said they would consider returning to college for a degree in this field, and 91% of respondents agreed that in order to help reduce cyber threats and improve information security, colleges and universities should create more cybersecurity education programs.

- NAU established the School of Informatics, Computing, and Cyber Systems (SICCS) in 2015 for the purpose of cultivating critical research and academic programs in computing and cybersecurity to serve state and national needs. With existing strengths in cybersecurity research activities that are rooted in computer science and electrical engineering and a secure-by-design professional engineering and computer science curriculum, development of additional academic programs

Contact Information:
Diane Stearns, Provost diane.stearns@nau.edu 928-523-4340
Chad Sampson, ABOR chad.sampson@azregents.edu 602-229-2512

focused on cybersecurity is the next progression. Our faculty already include noted experts in cybersecurity with strong research portfolios in this area such that the proposed programs build on a strong foundation of existing PhD-credentialed expertise by our tenure track and instructional faculty. These programs will also build on existing successful programs and faculty expertise in the area of informatics, computer science, electrical engineering, and computer engineering. Our double-digit percentage enrollment growth in these areas is evidence of our ability to successfully implement the following two new program proposals: a Cybersecurity, Bachelor of Science and a Cybersecurity, Master of Science.

Discussion

Northern Arizona University seeks to amend its Academic Strategic Plan for implementation in the 2020-2021 academic year. This request is for the following:

- **Cybersecurity, Bachelor of Science**
- **Cybersecurity, Master of Science**

Committee Review and Recommendation

The Academic Affairs and Educational Attainment Committee reviewed this item at its September 5, 2019 meeting, and recommended forwarding the item to the full board for approval.

Statutory/Policy Requirements

ABOR Policy 2-223.A – the Academic Strategic Plan

EXECUTIVE SUMMARY

ACADEMIC DEVELOPMENT PLAN

UNIVERSITY: Northern Arizona University

ARIZONA BOARD OF REGENTS
ASU ◆ NAU ◆ UA

PROPOSED NEW ACADEMIC PROGRAM

NAME OF PROPOSED DEGREE:

Cybersecurity, BS (BSCYB; online)
Cybersecurity, MS (MSCYB; online)
College of Engineering, Informatics, and Applied Sciences (CEIAS)
School of Informatics, Computing, and Cyber Systems (SICCS)
Flagstaff, Arizona
Catalog year 2020-2021

PROGRAM FEE REQUIRED? YES X NO

A program fee for both BSCYB and MSCYB students will help support the cost of delivering these programs by supporting teaching assistants, lab aides, graders, specialized computational and engineering equipment, specialized software licensing and consumable supplies. Through cutting edge cybersecurity software, hardware, and instructional personnel, students will have access to all of the infrastructure, materials and support they need in order to have a meaningful educational experience to ensure their career success. A portion of the fee will be used for financial aid and scholarships for those students who demonstrate merit and financial need.

BRIEF DESCRIPTION:

The BSCYB and MSCYB are completely online cybersecurity programs designed to support a totally new student population that builds on faculty expertise and research in SICCS, strongly supports University goals and priorities, supports a critical workforce need in Arizona, and provides a unique program for NAU. The Cybersecurity (BS & MS) programs are strategically crafted to complement SICCS' research activities in cybersecurity, support important University strategic goals, and address the institutional performance measures and goals for expanding student success and access. The programs are designed to be wholly online in an information-infrastructure-critical area with high employability and significant future growth potential. The programs will reach students who might not otherwise pursue a degree in SICCS; and provides an online delivery option to support diverse student groups. The programs use cutting-edge interdisciplinary research in cybersecurity to provide research-based training and learning opportunities for undergraduate and graduate students creating a research talent pipeline for NAU faculty that supports ongoing internationally recognized research, scholarship and creative endeavors.

These programs supports the goal of engagement by providing a workforce critical to defending Arizona's information infrastructure and through engagement with industrial partners and cybersecurity partnerships with the public and private sector in Arizona. Allied Market Research states:

> *[The] Cyber Security Market is expected to garner $198 billion by 2022, registering a compound annual growth rate of 15.5% during the forecast period 2016-2022. […] Increase in adoption of mobile devices, and growing reliability on Internet services*

in industries such as retail, healthcare, BFSI, and energy and Utility supplements the market growth.

The U.S. Bureau of Labor Statistics forecasts annual growth at up to 28% in cybersecurity-related careers. The need in Arizona is particularly acute. According to CyberSeek, there are more than 7,000 open cybersecurity positions in Arizona with 15,000 individuals currently employed in this sector.

LEARNING OUTCOMES AND ASSESSMENT PLAN:

The undergraduate program will be supported through the ABET-accrediting process and the student learning outcomes, evaluation criteria, and core topics described below will mirror the Cybersecurity standard set by the Computing Accreditation Commission.

Learning Outcome 1 (LO1): Apply security principles and practices to maintain operations in the presence of risks and threats.

- Concepts: a) Data Security: protection of data at rest, during processing, and in transit; b) Human Security: the study of human behavior in the context of data protection, privacy, and threat mitigation; and c) Organizational Security: protecting organizations from cybersecurity threats and managing risk to support successful accomplishment of organizations' missions.
- Competencies: a) Ability to use cryptographic methods to protect data and communication channels; b) Ability to protect human, software, and hardware systems by identifying risks and threats and planning mitigation strategies.
- Measures and Assessment: Direct measure of mastery using performance indicators and rubrics associated with classes in cryptography and secure design.

Learning Outcome 2 (LO2): Analyze a complex computing problem and apply principles of computing and other relevant disciplines to identify solutions.

- Concepts: a) Software Security: development and use of software that reliably preserves the security properties of the protected information and systems; and b) Hardware Security: development and use of hardware that provides cryptographic primitives and secure computational architectures.
- Competencies: a) Ability to develop secure-by-design software and hardware for computational problems; b) Ability to apply mathematics, statistics, and cryptography to develop new security algorithms, software, and hardware.
- Measures and Assessment: Direct measure of mastery using performance indicators and rubrics associated with classes in software design, math, and statistics.

Learning Outcome 3 (LO3): Design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of the program's discipline.

- Concepts: a) Component Security: the security aspects of the design, procurement, testing, analysis, and maintenance of components integrated into larger systems.

EXECUTIVE SUMMARY

- Competencies: a) Ability to develop new systems composed of hardware, software, and organizational systems; b) Ability to analyze and evaluate security risks inherent to a system.
- Measures and Assessment: Direct measure of mastery using performance indicators and rubrics associated with classes in senior design (CYB486C).

Learning Outcome 4 (LO4): Communicate effectively in a variety of professional contexts.

- Concepts: a) Oral communication: communication in teams, delivering presentations, and communication security risks; b) Written communication: use written communications to report on security issues.
- Competencies: a) Ability to understand and appropriately communicate security issues appropriately to an audience.
- Measures and Assessment: Direct measure of mastery using performance indicators and rubrics associated with the junior level writing class and senior design.

Learning Outcome 5 (LO5): Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles.

- Concepts: a) Societal Security: aspects of cybersecurity that broadly impact society; b) Professional responsibilities: the legal and ethical principles and professional obligations of cybersecurity practitioners.
- Competencies: a) Ability to identify ethical concerns in cybersecurity practice and take appropriate remedial action; b) Ability to engage within the discipline and nurture lifelong learning.
- Measures and Assessment: Direct measure of mastery using performance indicators and rubrics associated with classes in ethics.

Learning Outcome 6 (LO6): Function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline.

- Concepts: a) Teamwork: Working with diverse colleagues and clients to develop secure-by-design systems; b) Project Management: The use of project management and engineering principles to design and implement security sensitive software and hardware.
- Competencies: a) Ability to solve problems in a team setting; b) Ability to work in software engineering and computer engineering development teams.
- Measures and Assessment: Direct measure of mastery using performance indicators and rubrics associated with classes where teamwork is used like senior design CYB486C.

The graduate program includes student learning outcomes that build on the undergraduate learning outcomes but are designed to emphasize the necessary preparation for doctoral study or advanced professional practice in cybersecurity.

Learning Outcome 1 (LO1): Investigate and develop advanced security theory and practice for maintaining operations in the presence of risks and threats.

EXECUTIVE SUMMARY

- Concepts: a) Advanced Data Security: protection of data at rest, during processing, and in transit through the application of advanced research and analysis; b) Human Security: the study of human behavior in the context of data protection, privacy, and threat mitigation; and c) Advanced Organizational Security: protecting organizations from cybersecurity threats and managing risk to support successful accomplishment of an organizations' missions.
- Competencies: a) Ability to research and develop cryptographic methods to protect data and communication channels; b) Ability to protect human, software, and hardware systems by identifying risks and threats and developing novel new mitigation strategies and advanced cybersecurity practices.
- Measures and Assessment: Direct measure of mastery using performance indicators and rubrics associated with classes in advanced cryptography and secure design research.

Learning Outcome 2 (LO2): Study advanced problems and concerns in cybersecurity and apply principles of computing and other relevant disciplines to research and deploy novel solutions.

- Concepts: a) Software Architecture Security: development and use of software architectures and paradigms that provably preserve the security properties of the information and systems; and b) Hardware Architecture Security: design and development of electronics that provide cryptographic primitives and provably secure computational architectures.
- Competencies: a) Ability to develop provably secure-by-design software and hardware for computational problems; b) Ability to use mathematics, statistics, and cryptography to develop advanced security algorithms, software, and hardware.
- Measures and Assessment: Direct measure of mastery using performance indicators and rubrics associated with classes in software and hardware design.

Learning Outcome 3 (LO3): Design, implement, and rigorously test computing-based solutions for advanced cybersecurity problems.

- Concepts: a) System Security: the security aspects of the design, procurement, testing, analysis, and maintenance of large and distributed systems.
- Competencies: a) Ability to develop parallel and distributed systems composed of hardware, software, and organizational components and sub-systems; b) Ability to analyze and evaluate advanced security faults inherent to a system.
- Measures and Assessment: Direct measure of mastery using performance indicators and rubrics associated with classes in advanced design coursework.

Learning Outcome 4 (LO4): Communicate effectively in professional and academic research contexts.

- Concepts: a) Oral communication in a research context: communication in research teams, delivering presentations, and communicating security risks to diverse

EXECUTIVE SUMMARY

audiences; b) Written communication in a research context: writing research reports and communicating complicated security issues.
- Competencies: a) Ability to communicate security issues to diverse academic, research, and professional audiences through reports, proposals, and presentations;
- Measures and Assessment: Direct measure of mastery using performance indicators and rubrics associated with research project coursework.

Learning Outcome 5 (LO5): Recognize professional and research responsibilities and make informed judgments in cybersecurity practice based on legal and ethical principles.

- Concepts: a) Societal Security: aspects of cybersecurity that broadly impact society; b) Professional responsibilities: the legal and ethical principles and professional obligations of cybersecurity practitioners.
- Competencies: a) Ability to identify ethical concerns in cybersecurity practice and take appropriate remedial action; b) Ability to engage with the cybersecurity research community and nurture lifelong learning and professional development.
- Measures and Assessment: Direct measure of mastery using performance indicators and rubrics associated with coursework in ethics.

Learning Outcome 6 (LO6): Provide team and organizational leadership in cybersecurity.

- Concepts: a) Leadership and Teamwork: Working with diverse colleagues and clients to develop secure-by-design systems and providing leadership in these areas to organizations and research groups; b) Project Management: The use of project management and engineering principles to design and implement security sensitive software and hardware in both professional and research contexts.
- Competencies: a) Ability to solve problems in a team setting and provide leadership in problem solving and analysis; b) Ability to lead software engineering and computer engineering development teams in cybersecurity focused analysis and development.
- Measures and Assessment: Direct measure of mastery using performance indicators and rubrics associated with coursework in leadership and teamwork.

MEASURES AND ASSESSMENT

Measurement and assessment of LO1-LO6 in both the undergraduate and graduate programs will use a continuous improvement model. Classes where mastery is demonstrated for an outcome are collectively assessed using performance indicators, rubrics, metrics, and targeted levels of attainment.

Direct measures for each learning outcome will be deployed in key classes where mastery experiences take place for that outcome (e.g., Capstone Senior Design class CYB486C). Indirect measures include Senior Exit Surveys, Industry Surveys, and Faculty surveys.

This assessment then drives future improvement to the program. This mirrors the assessment and continuous improvement model used in our existing Computer Science and Engineering programs at NAU.

PROJECTED 3RD YEAR ENROLLMENT: Undergraduate = 180; Graduate = 38

This page intentionally left blank