BOARD OF HIGHER EDUCATION
REQUEST FOR BOARD ACTION

NO.: BHE 24-18

BOARD DATE: December 12, 2023

APPROVAL OF LETTER OF INTENT OF BRIDGEWATER STATE UNIVERSITY TO AWARD THE MASTER OF SCIENCE IN CYBERSECURITY AND JUSTICE AND AUTHORIZATION FOR FAST TRACK REVIEW

MOVED: The Board of Higher Education (BHE) has evaluated the Letter of Intent of **Bridgewater State University** to award the **Master of Science in Cybersecurity and Justice** and has determined that the proposal aligns with BHE criteria. Accordingly, the BHE authorizes the Commissioner to review the program and to make a final determination on degree granting authority pursuant to the Fast-Track review protocol.

VOTED: Motion approved and advanced to the full BHE by the Executive Committee on 12/4/2023; and adopted by the BHE on 12/12/2023.

Authority: Massachusetts General Laws Chapter 15A, Section 9(b); AAC 18-40

Contact: Winifred M. Hagan, Ed.D., Senior Associate Commissioner for Strategic Planning and Public Program Approval

BOARD OF HIGHER EDUCATION
December 12, 2023
Bridgewater State University
Letter of Intent
Master of Science in Cybersecurity and Justice

DEGREE TITLE ABSTRACT ON INTENT AND MISSION OF PROGRAM

The Bridgewater State University (BSU) proposed Master of Science in Cybersecurity and Justice (MS/CJ) program is designed to focus on the technical elements of cybersecurity, and to frame the technical management of incoming cybersecurity threats within the local, regional, national, and global context of cybercrime. Graduate students will learn how to stop an attack, construct incident documentation, and communicate effectively with others inside and outside of the organization. It is expected that students will graduate from the program ready for employment in various contexts in the private and public sectors. BSU plans that the MS/CJ will exceed the content knowledge and skill set that non-credit bearing professional trainings and certifications typically provide.

BSU plans that the MS/CJ will be interdisciplinary in nature. It reports that higher education cybersecurity programs fall into two basic categories: one with a computer science focus and the other rooted in the criminal justice discipline. Computer science and criminal justice disciplines differ in teaching approaches, including each lens on a world view, examples used in classes, and contexts provided for learning. Computer science security operations are understood technically within the complex computer systems of an institution and network. Criminal justice security operations are understood through criminal acts to be thwarted and communicated to others within an organization and in law enforcement. The BSU MS/CJ is designed to integrate both computer science and criminal justice approaches to teaching and learning, as well as content knowledge from both fields of study.

The proposed Bachelor of Science in Cybersecurity and Digital Forensics was approved by the Bridgewater State University Board of Trustees on June 8, 2023. The LOI was circulated on September 18, 2023.

One comment was received from the University of Massachusetts Presidents office by University of Massachusetts Dartmouth (UMD). The commentary suggested the proposed Bridgewater State University program develop content for the relationship between cybersecurity techniques and real-world justice systems. It cited four similar programs in Florida, Massachusetts, and New York. UMD also referenced regulatory aspects of monitoring and enforcement in the field and offered UMD's collaboration with Bridgewater regarding its Cybersecurity Certificate technical courses. Bridgewater State welcomed these insights as helpful to consider as the program develops.

A. **ALIGNMENT WITH MASSACHUSETTS GOALS FOR HIGHER EDUCATION**

Address Gaps in Opportunity and Achievement in Alignment with Campus-Wide Goals

BSU reports that the proposed graduate degree program will promotes the system-level strategic goal to "*…make college more accessible and affordable to all residents. …*" No other comparable cybersecurity graduate degree programs exist in the area. The proposed program is designed to offer paid graduate assistantships as well as opportunities to work as a professional apprentice within BSU's Security Operations Center[1] (SOC). The proposed master's degree program would be one of few cybersecurity graduate degree programs in Massachusetts focused on both the technical elements of the field and its interdisciplinary components, including the legal, investigative, ethical, and management dimensions. The proposed program would be the only cybersecurity master's degree option within the state university system. Candidates will not be required to have an undergraduate major in cybersecurity or computer science, nor will the Graduate Record Examination (GRE) be required. This wider admissions funnel is distinctive as is BSU's state-of-the-art Cyber Range[2] and

[1] SOC is designed to be an on-campus facility offering real world, hands-on experience; staffed 24/7 by cybersecurity experts with assistance from BSU students. Through a partnership with CyberTrust Massachusetts, a consortium of statewide cybersecurity experts transforming cyber education and training through experiential learning environments, the SOC will provide much needed technical support to local businesses and municipalities, which often lack the staffing and funding to protect themselves against cyberattacks. *Retrieved 10/26/23 https://www.bridgew.edu/about us/news events/Press Release 03/02/23*

[2] The Cyber Range is a cybersecurity training space, designed to develop hands-on training through simulated cyberattacks, data breaches, and other cybercrimes. The 1,900 square foot facility will feature 24 "seats," a large video

SOC, all of which are expected to attract students. The 30-credit program is expected to cost students $14,655 at the current credit-hour rate for tuition and fees of $488.50. The use of the cyber range for the proposed program will allow students to experience the pressure and complexity of real-world cyber-attacks and prepare students for cybersecurity careers. Cybersecurity experts indicate that students and technology professionals should experience regular hands-on and collaborative learning in the field. BSU is working collaboratively with Cyber Trust Massachusetts (CTM), the MassCyberCenter, and Mass Tech Collaborative and has received federal grant dollars to expand development in cybersecurity learning. BSU reports that, as noted by Microsoft[3] and others, cybersecurity education has centered around the technical aspects of cybersecurity while neglecting to make overt connections to human behavior. This oversight is also identified within Massachusetts cybersecurity educational programs[4]. BSU advisory board members indicate that employers seek employees who can work collaboratively, who understand the wider impact of cybersecurity in our society, who can write about cybersecurity incidents, and who can communicate orally about such incidents. BSU further holds that cybersecurity requires an understanding of technology, human behaviors, and organizational cultures. Certification doesn't necessarily teach how to apply knowledge and skills and there are missing pieces in the existing training. Good cybersecurity training teaches the knowledge and skills required to perform the work itself; it doesn't merely impart knowledge about discrete topics, concepts or tools.[5]

Frameworks like the one developed by the National Initiative for Cybersecurity Education (NICE) establish standards and explicitly address the work roles that the learner will eventually hold. The NICE framework establishes the building blocks of a sound academic program that supports the use of a standard lexicon and promotes

wall, and command center. Through simulated "stress-tests," participants will navigate scripted cyberbreaches in real-time, dealing with demanding situations that mirror efforts required to mitigate a cyberattack. The Cyber Range will additionally serve as a resource to the community for municipalities, government agencies, or outside organizations hoping to renew certifications and qualifications. *Retrieved 10/26/23* *https://www.bridgew.edu/about us/news events/Press Release 03/02/23.*

[3] https://news.microsoft.com/europe/features/why-we-need-more-diversity-in-cybersecurity. May 2020

[4] ACT/NRCUA, *"Master's Degree in Cybersecurity,"* March 2021.

[5] Leslie Overmyer-Day, "Cracking the Code to Training Cybersecurity Workers," *Talent Development*, 2021, p. 54-59.

workforce development. NICE notes that those performing cybersecurity work must be lifelong learners. Since cybersecurity threats are constantly changing[6], the BSU cybersecurity graduate degree program will seek recognition via the NSA’s Cyber Defense, Centers of Academic Excellence in Cyber Defense Education (CAE-CD) designation. Core values of the designation include ethical behavior and collaboration. The dean of the College of Graduate Studies attended the training for applying for the CAE-CD recognition in January 2022. Once the program is established, BSU will seek to offer continuing education graduate courses to those who complete the program and others interested in honing their skills. In each graduate cybersecurity classroom, students will be required to discuss the differing views of colleagues and collaborate to write comprehensive reports targeting multiple readers, including business supervisors, courts, and legal counsel. As explained above, the teamwork practice provided by completing class exercises in BSU's cyber range is planned to equip graduates with hands-on experience in both technical and human interaction. The SOC will offer valuable on- campus internships and leadership opportunities for supervision of others.

The proposed program aligns with several goals of the Bridgewater State University Strategic Plan, and particularly the goals of Fostering Student Success, the Teaching and Learning Environment, serving as a Regional Catalyst for Economic, Cultural, and Intellectual Engagement and Advancing Higher Education Diversity and Social Justice. The proposed degree program also aligns with the goals of the Academic Affairs Divisional Strategic Plan which include, Providing Dynamic Learning Environments, Empowering Faculty to Excel within their Disciplines, Investing in High Impact Practices, making a Positive Impact on Massachusetts and Beyond, and serving as a Beacon for Social Justice.

BSU’s strategic goal of focusing resources and decisions on the overarching priority of student success is reflected in the proposed program. BSU reports that the Department of Criminal Justice has a strong undergraduate program and a robust master’s degree program in criminal justice. In the fall of 2020, there were 727 students enrolled in the department’s two undergraduate programs, criminal justice and victimology, and 32

[6] Workforce Framework for Cybersecurity (NICE Framework) (nist.gov)

students enrolled in the graduate program. It is planned that the MS in Cybersecurity and Justice will not be limited to students with CJ undergraduate experience as each course will provide the fundamental underpinnings of the field suitable for students with little or no background. The composition of the students in the Cybercriminology and Cybersecurity Graduate Certificate have provided BSU with useful insights into what to expect of the population of this proposed graduate degree program. The first students to enroll in the program did not come straight from undergraduate work. More than half of the prospective students making inquiries about the certificate program expressed interest in changing careers to the field of cybersecurity but worried about their lack of computing knowledge. It is further reported that undergraduate students in criminal justice and as well as other undergraduate students from other programs will also have the chance to apply for the Early Admissions Pathway (4 + 1) into the new graduate degree program. This pathway is designed to reduce the time and cost of completing the master's degree program. The Early Admissions Pathway (4 + 1) also serves as a recruitment tool for BSU's prospective undergraduates.

BSU's strategic goal to provide a teaching and learning environment with exceptional educational opportunities for intellectual, creative, and professional growth is reflected in the proposed program. A culture of success with undergraduate students has been developed through a structured approach to advising and mentoring. This begins with all majors taking a 1-credit course, an introduction to the major, where students learn about the opportunities and resources that are available (e.g., departmental honors, undergraduate research, internship opportunities, the criminal justice honor society, university-wide skill support, and graduate education). The College of Graduate Studies (CoGS) offers support for all graduate students including travel for conferences, research and creative work. CoGS' support includes a free-of-charge option skills course, *Maximizing the Graduate School Experience,* offered every semester and a peer-writing support group. The Department of Criminal Justice offers a student computer lounge with five new computers equipped with digital forensic investigative tools and other statistical software that students need to practice and explore what they learned in class. The lounge is open to students from 8 a.m. to 5 p.m. Monday through

Friday. If students need to use the lounge other than regular business hours, they can arrange time via a faculty member.

BSU's strategic goal to serve as a regional catalyst for economic, cultural, and intellectual engagement is reflected in the proposed program. BSU reports that cybersecurity teams are struggling to keep enterprise networks secure at a time when the rise in remote working is providing additional security challenges - stressing not only the networks but the people responsible for keeping them running and that there is a serious shortage of cybersecurity workers around the globe[7]. BSU further reports that a global study of cybersecurity professionals by Information Systems Security Association (ISSA) and the industry analysis firm Enterprise Strategy Group (ESG) warns of a lack of business investment in cybersecurity training. This, combined with the challenges of additional workloads, is resulting in a skills shortage resulting in unfilled jobs and a high burnout rate among information security staff. The proposed program is expected to mitigate these challenges with innovation that serves as a catalyst for growth. Many of the assignments in the courses will involve collaborative work on BSU's state-of-the-art cyber range. This hands-on learning opportunity will build the student's confidence and raise their marketability to potential employers. Employers have found that new graduates who have learned through hands-on experiences are ready and qualified, effective employees.

BSU's strategic goal to advance diversity and social justice with impact in the region and beyond is reflected in the proposed program. In fall 2020, BSU had 20 percent racially diverse students throughout its graduate population. The proposed program goal is to meet or exceed these percentages in all cybersecurity programs. BSU noted that 88 percent of workers in the cybersecurity sector are white[8]. BSU also reports that the field of cybersecurity is well-known as a male-dominated field with a predominantly white employee base[9]. BSU cited a report on how cyber-attacks are experienced and

[7] Architecture Technology Corporation, "The World has a Shortage of Cybersecurity Workers, Part Two," *Cyrin Newsletter*, August 2022, https://www.atcorp.com/products/cyrin/newsletter/the-world-has-a-shortage-of-cybersecurity-workers-two/, retreived August 15, 2022.)

[8] Commonwealth of Massachusetts' Executive Office of Labor and Workforce Development (2019)

[9] (ISC Cybersecurity Workforce, "Women in Cybersecurity: Young, Educated, and Ready to Take Charge," ISC2.org, retrieved January 11, 2021).

that gender shapes both how they are carried out and experienced, which significantly underscores the need for more women in cybersecurity[10]. BSU expects that by marketing and recruiting to a wide range of racial and gender diverse students, the proposed program will begin to address these well-documented inequities in the field. Noting that most graduate programs are not designed for career-changers, and that anyone who did not major in computer science as an undergraduate is typically excluded by candidacy requirements, the proposed program is designed to emphasize diverse perspectives. BSU underscores the current research in business which demonstrates that, the greater the diversity of a workplace, the better the decision making and results. Inclusive working groups are shown to make better decisions as much as 87 percent of the time[11].

Program or Department Supports to Ensure Student Retention and Completion

Divisional goals within the Academic Affairs division of BSU include, providing dynamic learning environments focused on students' futures, empowering faculty and librarians to excel within their disciplines, investing in high-impact practices and the people advancing them, encouraging people to develop their lives and careers, making a positive impact on Massachusetts and beyond, and serving as a beacon for diversity and social justice. Each of these goals were carefully explicated in the body of the Letter of Intent (LOI) and all program and departmental supports are nested within them.

The proposed MS/CSJ program will reside within the Department of Criminal Justice, which is home to the existing BS in Criminal Justice, MS in Criminal Justice, an undergraduate concentration in victimology, graduate concentrations in administration of justice and crime and corrections, and a Cybersecurity and Cybercriminology Graduate Certificate. The existing MS in Criminal Justice graduated 114 students from fall 2012 to spring 2022.

[10] https:// reachingcriticalwill.org/ Association for Progressive Communication and Women's International League (Women's International League for Peace and Freedom and the Association for Progressive Communications, "Why Gender Matters in International Cyber Security," April 2020, retrieved January 11, 2022

[11] Larson, Eric. *Hacking Diversity with Inclusive Decision-Making* and *New Research: Diversity and Inclusion + Better Decision Making at Work. Forbes*, September 21, 2017.

In addition to cybersecurity, faculty in the department represent a range of specialties to support students in their educational and career goals. These include criminal justice policy, policing, restorative justice, public opinion, immigration, human trafficking, juvenile delinquency, mental health, race, and gender. Faculty in the department have and will continue to mentor student research in the form of honors thesis projects, master's thesis projects, independent research, published research, and research presented at local, national, and international academic conferences. This resource will be brought to bear on the proposed program students and is expected to result in their similar successes.

Examples include the following: from 2015 through 2021, criminal justice students chose to undertake independent research to complete twenty-five master's thesis projects. Of these projects, four won Outstanding Thesis of the Year from the CoGS (2021, 2019, 2018, 2016). Additionally, five students were mentored in projects involving cybercrime or cybervictimization over this time. Each of these five students went on to doctoral programs with full financial funding; two have completed their programs and hold tenure track positions at four-year institutions with the specialty areas of cybercrime and cybersecurity. In addition to thesis work, CoGS has supported approximately twenty students per year in presenting research at national conferences around the country, including the American Society of Criminology and the Academy of Criminal Justice Sciences. CoGS makes approximately sixteen awards of $750 each to graduate students for travel to academic conferences annually. President Fred Clark has recently established the David B. Jenkins fund to further support graduate research. Further, the Department of Criminal Justice is home to the Cullen Scholarship Research Award (an endowed scholarship named for Francis Cullen, internationally renowned criminologist, and alumnus of BSU, and established through his desire to assist criminal justice students at BSU). Annually, one student that is engaged in independent research and presents at a conference is awarded $1,000, in addition to other paid graduate assistantships. Other examples include when the Cybercriminology and Cybersecurity Graduate Certificate was launched in fall 2019 the student group known as

CyberBears[12]was created; as well, a current graduate certificate student interned with CTR Cyber, which is part of the Office of the Comptroller in MA. The student's work involved the promotion of cybersecurity awareness to protect the Commonwealth against increasing cyber-attacks. Based on her summer intern experience, she is currently working on promoting cybersecurity awareness among graduate students.

As mentioned previously, students in the Department of Criminal Justice have access to a student lounge that is a flexible meeting and study space with computers. Students use this space to do research, group projects, and study with each other while having access to faculty.

Alliances and Partnerships with PK-12, Other IHE's, Community Employers

While there are no plans for the proposed program to have any direct relationship with PK-12 education BSU expects to establish an Early College program in cyber security that will encourage interest in cyber security careers.

BSU has developed two boards and one cross-divisional committee that will work with the Department of Criminal Justice, the CoGS, and the College of Humanities and Social Sciences in managing, assessing, and improving the cyber security degrees on campus (at all levels) and their resources, the cyber range and the SOC. The Computer Science and Cybersecurity Board (CSCB) is already in existence, supporting BSU's move toward the proposed MS/CSJ. The board meets regularly and reports on changes in the industry. The board members, mid-level to high-level leaders in the industry, regularly review curriculum and suggest changes. Further details regarding the two boards and cross divisional committee are detailed below.

[12] The BSU CyberBears is a group of students who are enrolled in the certificate program and compete in national/international level cyber-related events. The group's debut competition was Utica College's 2021 Student Cyber Forensic Competition. This competition was the preliminary competition for the second White Hat conference, sponsored by the Bureau of Justice Assistance (BJA) and Boston University. Even though it was their first attempt, the BSU CyberBears won second place in the competition and plans are underway to compete in subsequent events of this type. Since then, students in the program have actively engaged in various Capture the Flag competitions, free knowledge-based competitions that help hone students' technical skillset. One of the BSU CyberBears won second place in the student paper competition at the third White Hat conference in June 2022 and presented her work during the conference. In addition, the faculty in the program provide various opportunities for students to apply for internships and jobs in the field.

Computer Science and Cybersecurity Board (CSCB)

The College of Graduate Studies formed a Computer Science and Cybersecurity Board to support the Graduate Assistance in Areas of National Need (GAANN) Award and Supplement from the US Department of Education. After its founding, the scope of the board increased. The board seeks to assist students in obtaining internships, assess the curriculum and suggest updates that will assist the students in their search for employment upon graduation, and apprise faculty, staff, and students of changes in the cybersecurity industry.

Cybersecurity Advisory Board (CAB)

Two advisory boards will work collaboratively on the assessment of the full gamut of BSU's cyber security project – one taking the lead on education and learning outcomes (the Computer Science and Cybersecurity Board [CSCB]), and one overseeing business and technology outreach and engagement (the Cybersecurity Advisory Board [CAB]). The IT Division, along with the College of Graduate Studies, the College of Continuing Studies, and the Bartlett College of Science and Mathematics, are forming a new Cybersecurity Advisory Board. The board seeks to assess the yearly Cyber Range Performance Report presented by the cyber range director and IT vice president; assist BSU leadership with the strategic planning related to the cyber range; assist BSU cyber leadership with the marketing of our cyber range and related entity, the Security Operations Center (SOC); and apprise BSU cyber leadership of changes in the cybersecurity industry.

Cyber Range Steering Committee

Facilitation of communication between the two boards will be connected via an internal group, the Cyber Range Steering Committee (CRSC). This committee is an off-shoot of the original cross-divisional team, known as the Steering Committee, that brought the plan for the cyber range to fruition. The vice president of the Division of Information Technology (IT) or their designee will chair the committee. It will be composed of representatives from IT, the Department of Criminal Justice, the Department of Computer Science, the College of Continuing Studies, the Bartlett College of Science and Mathematics, and the College of Graduate Studies. The CRSC will meet regularly to assure all the internal stakeholders are being heard and will connect the academic assessment cyber range assessment groups. The CRSC also reviews and makes recommendations on the yearly Cyber Range Performance Report, written by the cyber range director.

Relationship to MassHire Regional Blueprints

The *Eduventures Report* of March 2021 is based on data collected on the occupations coded as Computer and Information Systems Security/Information Assurance, Cyber/Counter Forensics and Counterterrorism, and Cyber Electronic Operations and Warfare. Entry-level job titles include Computer and Information Systems Managers, Information Security Analysts, Computer Network Support Specialists, Computer Network Architects, Database Administrators, and Database Architects. Projected growth is well beyond the 6 percent growth anticipated within all US occupational categories between 2021 and 2030. Computer and Information Systems Managers will likely see a 12 percent change in that time, 100 percent more than that of the average. Information Security Analysts are anticipated to grow by 27 percent during the same period.

Eduventures concluded in the study commissioned by BSU that the master's degree market in cybersecurity is "much stronger and [more] consistent than the bachelor's degree market" and "the market does not look to be at risk for saturation." Eduventures concluded that there are more undergraduate programs in the field than graduate programs and that a master's degree will be a "stand out differentiator" in the marketplace. BSU expects this to be especially true for a graduate program open to undergraduates from a variety of disciplines.

BSU reports that according to the *2020 Regional Blueprint Update for Southeast MA and the Massachusetts Industry-Occupation Employment Projection Matrix,* between 2018 – 2028 there will be approximately 2,690 regional cybersecurity vacancies at any given time. Massachusetts seeks to become the nation's leader in the preparation of well-qualified employees. When the Baker-Polito administration announced the creation of the Cybersecurity Center (now called the MassCyberCenter) at Mass Tech

Collaborative, Governor Baker stated, “Massachusetts is home to many of the world’s leading innovative companies, accelerators, and educational institutions, as well as an economically competitive climate prepared to host the world’s emerging cybersecurity industry.” The governor also said that “[c]reating the Cybersecurity Growth and Development Center at the Massachusetts Technology Collaborative and the Cybersecurity Strategy Council will ensure the state serves as a committed partner with businesses, colleges, and universities, and the public sector to continue developing a talented workforce and to expand our cybersecurity ecosystem[13].”) According to the *Blueprint* and other lists of cybersecurity jobs, the BSU graduate degree program will ready students for a wide range of employment opportunities, including digital forensic analysts, penetration testers, computer system analysts, information security analysts, computer network support specialists, and network and computer systems administrators. Jobs can be found in many areas: government agency cybercrime units such as federal and state-level government agencies are seeking employees with knowledge and background in cybercrime and digital forensics; private company cybercrime units such as banking/finance, engineering, medical, insurance, manufacturing, transporting, and many other private entities that use computers and networks are seeking experts in cybercrime and cyber-investigation to recover and prevent losses; government agency cybersecurity unit such as government agencies at all levels that are seeking people with knowledge and background in cybersecurity. BSU also noted that students may choose to complete a PhD degree program or a second master’s degree in criminology/criminal justice, information technology, computer science, business, public administration, and many other fields to augment the study of cybersecurity.

The LOI cites that in 2019, the U.S. government announced that we “must enhance the workforce mobility of America’s cybersecurity practitioners to improve America’s national cybersecurity.” Within Executive Order 13870, America’s Cybersecurity Workforce, the president urged the government to issue awards to acknowledge the achievements of the nation’s cybersecurity operatives and encourage them to

[13] *Baker-Polito Administration Announces New Cybersecurity Center at Mass Tech Collaborative*, September 13, 2017. Retrieved January 5, 2022, at www.masstech.org.

participate in competitions. The directive launched a nationwide Call to Action to address private and public workforce needs and to “grow a dynamic and diverse cybersecurity workforce” in partnership with states, the private sector, academia, and tribal governments. (Executive Order 13870, America’s Cybersecurity Workforce, 1-7.) BSU further cites that cybersecurity grows even more complex when more workers are laboring remotely. (“One Year Later: Overcoming the Cybersecurity Challenges of a Remote Workforce,” *Eweek*, 3/29/21.) Note also the pressing need to enroll more US citizens in cybersecurity degrees so that they can keep the federal, state, and municipal governments and elections safe. (Maurice Dawson, “National Cybersecurity Education: Bridging Defense to Offense,” *Technical Services*, vol. 25, Issue 1, 2020: 72.)

Duplication

BSU finds that no publicly funded master’s degree program in the commonwealth has tied a cyber range to in-class work for training their students. Northeastern University currently offers a cybersecurity graduate program heavily reliant on a computer science background. Northeastern University is increasingly reaching a national and global student market and is becoming highly selective. Their 32-credit program is offered in both Boston and Seattle and in online and on-campus modalities. The Northeastern program is offered by Northeastern University’s Khory College. Northeastern University’s degree focuses on information technology but does bring in social science, law, criminology, and management issues. The degree focuses on those seeking employment in government and business, with an eye toward research. Northeastern students may earn a Graduate Certificate in Engineering Leadership along with their Master of Science in Cybersecurity. The degree costs $1,532 per credit hour at the present time, or $49,024 in total.

The University of Massachusetts Lowell offers graduate courses in cybersecurity or a Master of Science in Computer Science with a Cybersecurity option. This 30-credit degree allows students to take some courses in cybersecurity. Students must have an undergraduate degree in computer science or a closely related area. Applicants must have taken courses in four primary computer science fields and submit a GRE score. The cost per credit, at the time of the LOI submission, was $844.99, with a total degree cost of $25,349.70. Note that UMass Lowell has a cyber range, but it is research-based and primarily accessed by the student club and researchers.

Boston University offers a master's degree in criminal justice with a concentration in cybercrime investigation and cybersecurity via its Metropolitan CollegeThis 32-credit program is offered online and on campus. Courses are $955 per credit for part-time students (part-time students may take up to 11.5 credits) or $30,560 per semester, plus additional fees.

The BSU proposed program would be the only cybersecurity master's degree option within the state university system. BSU targets job changers (among others) and will not require an undergraduate major in cybersecurity or computer science for admission. This wider admissions funnel makes the degree program distinctive, and the proposed 30-credit program will cost students $14,655 in total, calculated at the current credit-hour rate for tuition and fees of $488.50. BSU will not require the Graduate Record Examination (GRE) and will rely on a range of multiple assessment measures for admission. This will be further addressed in the Phase II application materials.

Innovative Approaches to Teaching and Learning

BSU reports that cybersecurity experts indicate that graduating students and IT professionals within a wide range of industries, including government, non-profit, and for-profit concerns, should engage in regular, hands-on experiences in the field. Elochukwu Ukwanda et al. write that "refreshing established practices and the scope of the training to support the decision making of [cybersecurity] users and operators" is key and that "the foundation of the training provision is the use of Cyber-Ranges (CRs) and Test-Beds (TBs), platforms/tools that help inculcate a deeper understanding of the evolution of an attack and the methodology to deploy the most impactful countermeasures to arrest breaches[14]." In 2015, the Marine Corp brought in specialized cyber range training to keep Marines up to speed with current developments and to learn to react to challenges that they might confront in a variety of roles. Col. Gregory Breazile, Marine Corps, commented that the cyber range allowed the Marines to "test

[14] (Elochukwu Ukwanda, et al., "A Review of Cyber-Ranges and Test-Beds: Current and Future Trends," *Sensors,* 2020, 20: 1-35.)

things out, they can try different techniques, they can use different tools without breaking anything on real, live networks[15].” BSU reports that according to *Security Intelligence* author Mark Stone, cyber ranges “may be one of the most effective ways to train IT professionals in defending against cyber-attacks.” The training is successful as the real-world exercises improve memory retention and foster the adaptability to solve problems and confront new situations[16].

The MS in Cybersecurity and Justice offers students the opportunity to be engaged in multiple innovative learning experiences:

- Work as a team by participating in CyberBears: students compete in national/international level cyber-related events as the CyberBears as well as in a local, state, national, or international level competitions.
- Employ a highly utilized digital forensic tool, beginning with Magnet Axiom: students will experience real-life-based cybercrime scenarios through hands-on lab activities using Magnet Axiom software, which is user-friendly. Municipal, state, and federal government agencies are switching to Magnet Axiom and BSU anticipates widespread adoption of Magnet Axiom, employing it within the existing graduate certificate in cybersecurity.
- Role-play by employing the state-of-the-art BSU cyber range: the BSU cyber range is planned to add significant, hands-on learning experiences to the proposed MS/CSJ program. Employers actively seek employees with team-based training. With cyber range and interactive lab training, it is expected that graduates will be attractive candidates for open positions.
- Engage in an internship: BSU’s state-wide network indicates that the demand for interns and full-time workers with cybersecurity knowledge is robust. Fall 2021 meetings with municipalities underscored a dire need of properly trained cybersecurity experts more than with over three thousand unfilled cybersecurity positions in MA alone. MassCyberCenter offers a mentorship program and graduate program faculty assist students with internship placement. Most of the

[15] Daniel P. Taylor, “Cyber Warriors,” Special Report, U.S. Marine Corp, *Seapower* [September 2015]: 1-3.
[16] Mark Stone, “Why Cyber Ranges Are Effective to Train Your Teams,” *Security Intelligence*, July 20, 2020. https://securityintelligence.com/articles/cyber-range-training-effectiveness/)

opportunities in the proposed MS/CSJ program will consist of paid, formal apprenticeships. Some of the positions will be within the campus' SOC. BSU expects to work with their Computer Science and Cybersecurity Advisory Council and Mass Tech Collaborative to continue developing contacts and placements.

- Focus on real-life scenarios: In addition to the BSU cyber range and internships, a partnership with Massachusetts Maritime Academy is under development. This collaboration allows students to practice confronting a cyber emergency situated within a broader emergency. It is expected that scenarios will be run out of the BSU cyber range and the Emergency Operations Training Center (EOTC) at Mass Maritime Academy. More detailed information regarding EOTC is provided in the next section.

B. ALIGNMENT WITH CAMPUS STRATEGIC PLAN AND MISSION

BSU holds that Cybersecurity is a priority for the world, the nation, the state, and the region. As BSU seeks to serve the region in workforce development, and because there are thousands of open positions in the region, BSU finds itself committed to create academic programs at all levels to fill the needs. Significantly the proposed degree is designed to contribute to the social mobility of students, as jobs in the field are high paying.

As noted previously, the proposed program aligns with several goals of the institutional strategic plan, in particular: Fostering Student Success, Teaching and Learning Environment, Serving as a Regional Catalyst for Economic, Cultural, and Intellectual Engagement, and Advancing Higher Education Diversity and Social Justice. As well it is aligned with the BSU Academic Affairs Divisional Strategic Plan, which includes Providing Dynamic Learning Environments, Empowering Faculty to Excel within their Disciplines, Investing in High Impact Practices, Making a Positive Impact on Massachusetts and Beyond, and Serving as a Beacon for Social Justice. The proposed MS/CSJ aims to create a more diverse and responsive workforce in the field by using program structure and alignment to the aforementioned goals.

LOI Program Goals and Objectives (Form B)

The program strives to accomplish the following goals: Serve the region, the state, and the nation by preparing graduates in a program aligned to the NICE[17] framework (Tasks, Knowledge, and Skills) for critical positions related to cybersecurity; become the 9th National Center for Academic Excellence in Cybersecurity[18] (NCAE-C) institution in Massachusetts[19]; prepare graduates to work independently to halt cybersecurity threats via lab exercises and other assignments; prepare graduates to work collaboratively in NICE-defined work roles to halt cybersecurity threats via training on the BSU cyber range; and increase the number of women and diverse candidates for the cybersecurity job market.

C. ALIGNMENT WITH OPERATIONAL AND FINANCIAL OBJECTIVES OF INSTITUTION

Enrollment Projections (Form C)

BSU does not anticipate any negative impact on other programs. Some positive impact is expected on other programs as students enrolled in existing cybersecurity certificate programs have joined a range of other master's degree programs, and the same trend is expected once the MS/CJ is approved.

Resources and Financial Statement of Estimated Net Impact on Institution (Form D, Appendices)

Costs

The primary costs associated with the MS, Cybersecurity and Justice program are faculty stipends and pay. Graduate programming at BSU is run under the Division of Graduate and Continuing Education (DGCE) contract between the BHE and the MSCA. DGCE graduate programs are designed to be highly cost-effective. Most graduate

[17] The Nice Framework for Cybersecurity provides a set of building blocks for describing the tasks, knowledge, and skills that are needed to perform cybersecurity work performed by individuals and teams. www.nist.gov/cybersecurity/nice/niceframework. Retrieved 10/29/23

[18] https//:www.nsa.gov/Academic/Centers-of-Academic-Excellence retrieved 10/29/23

[19] e.g., Bay Path University, Boston University, and Northeastern University. The full list can be accessed using the following URL: CAE Institution Map.

courses are taught as overloads by BSU full-time faculty. The sum of the off-load instructors (4) average $5,500 for a total of $22,000 for each of the first three academic years; BSU assumes costs to increase in year four to an estimated $24,000 for the four instructors. The Form D budget chart is based on conservative enrollment estimates on Form C. One faculty member will serve in the role of the DGCE graduate chair and will run the department's graduate committee, working with both the College of Humanities and Social Sciences and the College of Graduate Studies, to strategically lead the graduate program. The anticipated annual cost of the graduate coordinator is included in the budget on Form D.

Revenue Calculations

Full-time graduate students at BSU take three courses a semester, or nine credits per semester and 18 credits per year. Part-time graduate students typically take two courses each semester, or six credits per semester and 12 credits per year. The gross revenue is calculated based on the total number of credits for the expected number of full-time and part-time students multiplied by the per credit cost of attendance. The price per credit hour was $488.50 in 2022-2023. This model includes an assumption of a 3 percent increase in tuition each year and starts the calculations at 3 percent higher than the current tuition. The estimated tuition is $503.16 in year one, $518.25 in year two, $533.80 in year three, and $549.81 in year four. The MS /CJ is expected to be run as an Early Admissions Pathway (4 + 1), allowing undergraduate students to complete up to three courses during their undergraduate degree programs. BSU offers a host of Early Admissions programs and anticipates steady Early Admissions Pathway enrollment in this degree program. This program will be taught in the evening and BSU anticipates little problem with space concerns. As noted on Form D, it is anticipated that this program will be profitable from year one.

STAFF REVIEW AND VALIDATION

Staff thoroughly reviewed the **LOI** proposing full degree granting authority for the **Master of Science in Cybersecurity and Justice** submitted by **Bridgewater State University.** Staff validate that the **LOI** includes all data required by the Massachusetts

Board of Higher Education.   Staff recommendation is for BHE authorization for the Commissioner to review the program pursuant to the Fast-Track review protocol.

Form A2: LOI Graduate Program Curriculum Outline

Major Required (Core) Courses (Total of 6 courses required plus the exit requirement=21 Credits)		
Course Number	Course Title	Credit Hours
CYGR 500	Introduction to Cybersecurity	3
CYGR 502	Cybersecurity Scripting/Programing (New)	3
CYGR 503	Ethics in Cybersecurity (New)	3
CYGR 510	Application and Digital Security Strategy	3
CYGR 520	Windows Forensics	3
CRJU 555	Cybercriminology	3
CYGR 598 Or CYGR 599	(Exit requirement) Internship in Cybersecurity and Justice (New) Or Project Research in Cybersecurity and Justice (New)	 3 or 4
	Sub-total # Core Credits Required	21 - 22
Elective Course Choices (Total of 3 courses required =9 credits) *(attach list of choices if needed)*		
CYGR 501	Foundation of Cybersecurity (New)	1
CYGR 541	Cyber Law (New)	3
CYGR 551	Organization and Governance in Cybersecurity (New)	3
CYGR 569	Special Topics in Cybersecurity and Justice (New)	3
CYGR 579	Special Topics in Cybersecurity and Digital Forensics (New)	3
CYGR 589	Advanced Seminar in Cybersecurity and Digital Forensics (New)	3
CRJU 510	Research Methods	3
CRJU 511	Applied Data Analysis	3
CRJU 551	Law and Society	3
MGMT 560	Management of People and Organization	3
MGMT 562	Strategic Management of Technological Innovation	3

MGMT 598	Leadership, Ethics, and Corporate Accountability	3
	Sub-total # Elective Credits Required	9

Curriculum Summary	
Total number of courses required for the degree	10
Total credit hours required for degree	30-32* and **

Prerequisite, Concentration or Other Requirements:

CYGR 501 Foundation of Cybersecurity – Online 1 credit module is optional for students who feel they need additional technical preparation for the program upon acceptance.

CYGR 500 –Introduction to Cybersecurity and **CYGR 502 – Introduction to Cybersecurity Scripting are <u>prerequisites for all upper-level technical courses</u>**.

- CYGR 510 – Application and Digital Security Strategy
- CYGR 520 – Windows Forensics
- CYGR 579 – Special Topics in Cybersecurity and Digital Forensics (e.g., Ethical Hacking)
- CYGR 589 – Advanced Seminar in Cybersecurity and Digital Forensics (e.g., CYGR 530 Mobile Forensics will be considered as one of the advanced seminar courses).

Optional concentration in Digital Forensic Investigations: 6 credits (count toward electives)
CYGR 579 Special Topics in Cybersecurity and Digital Forensics
CYGR 589 Advanced Seminar in Cybersecurity and Digital Forensics

**The Cybersecurity project class is a 4-credit course, with the possibility of repeat up to 8 credits, due to the intense nature and laboratory component of the course. Students who choose to do a project would complete 31 to 32 credits.

Form B: LOI Goals and Objectives

Goal	Measurable Objective	Strategy for Achievement	Timetable
Work independently to defend a system during a cyber-attack.	Success on assigned laboratory assignment.	The course instructor will use formative assignments to prepare students for assigned laboratories.	This will be assessed yearly by the Graduate Assessment Subcommittee of the Criminal Justice (CJ) Graduate Committee.
Collaborate with a team taking on a variety of NICE-defined work roles to stop a cyber-attack in process.	Success on a cyber range attack exercise.	The course instructor will use formative assignments to prepared students for cyber range exercises.	This will be assessed yearly by the Graduate Assessment Subcommittee of the CJ Graduate Committee.
Critically analyze cybersecurity incidents within the broader context of local, regional, national and international cybercrime to best structure their institutional policies and reconfigure systems to defend against future attacks.	Attack analyzation assignment.	The course instructor will introduce students to overlapping and interrelated local, regional, national, and international laws and policies.	This will be assessed bi-annually by the Graduate Assessment Subcommittee of the CJ Graduate Committee.

Facilitate communication regarding a cybersecurity incident with colleagues within a broad range of cybersecurity roles as well as those outside the field.	Written and oral communications assignments. .	The course instructor will discuss program models for such communication and work with the departmental Graduate Committee to set program standards.	This will be assessed bi-annually by the Graduate Assessment Subcommittee of the CJ Graduate Committee.
Employ specialized software appropriate for each investigative stage.	Successful completion of an exercise assigned in class.	The course instructor will introduce students to a range of specialized software.	This will be assessed bi-annually by the Graduate Assessment Subcommittee of the CJ Graduate Committee.
Execute cybersecurity and digital forensic investigations under appropriate ethical guidelines.	Successful completion of cybersecurity and digital forensic investigations.	The course instructor will assign readings on ethical frameworks for cyber security work, including state and federal laws.	This will be assessed bi-annually by the Graduate Assessment Subcommittee of the CJ Graduate Committee.
Assess common legal issues within cybersecurity.	Written assignment pertaining to common legal issues within cybersecurity.	The course instructor will assign readings on common legal issues within cybersecurity, including case studies.	This will be assessed bi-annually by the Graduate Assessment Subcommittee

			of the CJ Graduate Committee.
Compose a court-ready formal report for diverse types of incidents.	Successfully complete a court-ready formal report.	The course instructor will discuss program models for such reports and work with the departmental Graduate Committee to set program standards.	This will be assessed bi-annually by the Graduate Assessment Subcommittee of the CJ Graduate Committee.
Discuss complex cybersecurity issues within a socially just and ethical framework.	Class discussions and/or written assignment.	The course instructor will assign readings on ethical frameworks for cyber security work, including state and federal laws.	This will be assessed bi-annually by the Graduate Assessment Subcommittee of the CJ Graduate Committee.
Propose solutions for the discrimination, oppression, privilege, and social and economic resources that shape the field of cybersecurity and digital investigation.	Class discussions and/or written assignment(s).	The course instructor will assign readings on the current state of the field of cybersecurity and digital investigation.	This will be assessed bi-annually by the Graduate Assessment Subcommittee of the CJ Graduate Committee.

Form C: LOI Program Enrollment

	Year 1	**Year 2**	**Year 3**	**Year 4**	**Year 5**
New Full-Time	15	15	15	18	18
Continuing Full-Time	0	15	15	15	18
New Part-Time	4	4	4	4	4
Continuing Part-Time	0	4	8	12	12
Total	19	38	42	49	52

Form D: LOI Budget

Year	Average credits per year per full-time student	Number of full-time students	Average credits per year per part-time student	Number of part-time students	Total Gross Revenue*	Instructor Cost**	DGCE Grad Chair*	Total Net Revenue
YEAR ONE	18	15	12	4	$160,005	$22,000	$4,000	$134,005
YEAR TWO	18	30	12	8	$329,607	$22,000	$5,000	$302,607
YEAR THREE	18	30	12	12	$365,119.2	$22,000	$6,000	$337,119.2
YEAR FOUR	18	33	12	16	$432,150.7	$24,000	$7,000	$401,150.7

**The chart assumes four off-load instructors at $5,500 a course for three years and $6,000 a course in year four. The chart assumes two on-load courses per semester for the program. CoGS provides revenue to department budgets for adjuncts to serve undergraduate students. The program will have its own graduate chairperson. The budget is calculated using the per credit cost in Fall 2022.

We plan to hire an additional faculty member who will serve in this program as well as offering undergraduate courses in Criminal Justice.

Program software costs $5,000 a year and this cost is already covered by the existing Cybersecurity and Cybercriminology Graduate Certificate.

Program faculty are working with the Dean of the Library, Kevin Kidd, to ascertain if new library materials should be ordered.