Public Comment: August 5 - August 20, 2024

Letter of Notification (LON) - Abbreviated

Bachelor of Science in Applied Cybersecurity

College of Emerging and Collaborative Studies

THE UNIVERSITY OF TENNESSEE KNOXVILLE

Updated: August 5, 2024

Table of Contents

Section I: Overview

Program Information

Institution:	University of Tennessee Knoxville
College/School/Division:	College of Emerging and Collaborative Studies
Department:	College-wide
Title of Degree Program:	Bachelor of Science in Applied Cybersecurity
Degree Designation:	Bachelor of Science
Concentrations:	None
CIP Code:	11.1003
CIP Code Title:	Computer and Information Systems/ Security/ Auditing/ Information Assurance
CIP Code Definition:	A program that prepares individuals to assess the security needs of computer and network systems, recommend safeguard solutions, and manage the implementation, auditing, and maintenance of security devices, systems, and procedures. Includes instruction in computer architecture, programming, and systems analysis; networking; telecommunications; cryptography; security system auditing and design; applicable law and regulations; risk assessment and policy analysis; contingency planning; user access issues; investigation techniques; and troubleshooting.
SOC Codes/Titles:	11-3021 -- Computer and Information Systems Managers 15-1212 -- Information Security Analysts 15-1231 -- Computer Network Support Specialists 15-1241 -- Computer Network Architects 15-1242 -- Database Administrators 15-1243 -- Database Architects 15-1244 -- Network and Computer Systems Administrators
Proposed UT BOT Approval:	February 2025
Proposed THEC Approval:	May 2025
Proposed Implementation Date:	August 2025

Academic Program Liaisons:

Karen Galicia, Director of Academic Affairs
University of Tennessee System
Office of Academic Affairs, Research, and Student Success
Phone: 865-974-2104
Email: galicia@tennessee.edu

Vandana Singh Avasty, Program Director
College of Emerging and Collaborative Studies
University of Tennessee, Knoxville
Phone: 865-974-2785
Email: vandana@utk.edu

System Letter of Support

THE UNIVERSITY OF TENNESSEE SYSTEM

ACADEMIC AFFAIRS, RESEARCH AND STUDENT SUCCESS

July 11, 2024

Dr. Steven Gentile, Executive Director
Tennessee Higher Education Commission
312 Rosa L Parks Ave., 9th Floor
Nashville, TN 37243

Dear Dr. Gentile

On behalf of the University of Tennessee, Knoxville, please accept this Letter of Notification (LON) for a proposed Bachelor of Science in Applied Cybersecurity. This program, modeled after the recently approved Data Science and Artificial Intelligence BS degrees in the College of Emerging and Collaborative Studies (CECS), will enable students across the university to take topics relevant to their interests and future careers in a classroom setting that includes a variety of student backgrounds. The applied nature of this degree emphasizes the practical implementation and real-world application of cybersecurity principles and technologies, which students will learn through hands-on experiences. The UT System Office has reviewed the proposal and believes it offers a strong complement to the existing programs in the college. We look forward to receiving an evaluation of the LON by THEC staff.

Sincerely,

Bernie Savarese, Ed.D.
Vice President of Academic Affairs, Research, and Student Success
University of Tennessee System

CC: Donde Plowman
John Zomchick
Ozlem Kilic
Heather Hartman
Vandana Singh Avasty
Karen Galicia
Betty Dandridge Johnson

400 W. Summit Hill Drive (physical) • 505 Summer Place (postal) • UT Tower 1258 • Knoxville, TN 37902 • (865) 974-3843
aass.tennessee.edu

Campus Letter of Support

THE UNIVERSITY OF TENNESSEE KNOXVILLE
OFFICE OF THE PROVOST

May 24, 2024

President Randy Boyd
505 Summer Place / UT Tower
Knoxville, TN 37902

President Boyd:

Please accept the attached Letter of Notification for a new undergraduate degree, Bachelor of Science in Applied Cybersecurity, in the College of Emerging and Collaborative Studies at the University of Tennessee, Knoxville (UTK).

The proposed program, Bachelor of Science in Applied Cybersecurity (BSCYBR), is being developed to prepare students for participation in the rapidly increasing workforce in cybersecurity. As organizations face mounting threats to maintaining safe virtual work environments, the need for skilled workers in cyber security is bound to continue to increase. Applied cybersecurity skillsets are and will continue to be necessary across industries, including healthcare, government, technology, and business. The BSCYBR undergraduate program at the College of Emerging and Collaborative Studies (CECS) at UTK will offer an interdisciplinary curriculum delivered by faculty from across the university.

Approved by the Board of Trustees in the spring of 2023, CECS is a new college created to host emerging, future-oriented interdisciplinary programs at UTK. Together with three new degree programs recently approved by THEC—Data Science, Artificial Intelligence, and Innovative Transdisciplinary Studies—BSCYBR will be responsive to a growing interest in cybersecurity among our students while also supplying needed expertise to eager employers. CECS is building this undergraduate degree on an existing Applied Cybersecurity certificate and minor for undergraduate students. A graduate certificate in Cybersecurity will be launched in Fall 2024.

The four-year Applied Cybersecurity (CYBR) degree program is designed to offer a foundational understanding of cybersecurity concepts, data sources, and tools in a less technical context than a computer science degree. This program accentuates real-world applications across various disciplines. Furthermore, it aims to delve into the methods and components of cybersecurity solutions, assessing potential sources of bias, social impacts, and other ethical considerations related to cybersecurity. These skills are integral for the rapidly growing cybersecurity sector.

The proposed Applied Cybersecurity program at UTK aligns seamlessly with the university's mission as a leading land-grant research institution. The program mirrors UTK's commitment to applied research and community engagement by emphasizing hands-on learning and community impact. It strengthens ties with strategic partners like the Oak Ridge National Laboratory, driving innovation in intelligent machines and society. Furthermore, the program aligns with UTK's goal of preparing its graduates to be industry, government, and community leaders. Given the high demand for cybersecurity professionals, many of these graduates will likely remain in Tennessee, contributing to the state's growth.

CECS is resourced sufficiently to deliver the courses for BSCYBR. CECS instructors will provide instruction for the core courses for the CYBR degree. Upper-level electives will be selected from existing offerings from multiple colleges on campus and CECS certificates.

This proposed program has the full support of the campus administration. We will be seeking approval for the program through the regular campus curricular processes. While we go through the campus processes for approval and to save

Office of the Provost and Senior Vice Chancellor
527 Andy Holt Tower, Knoxville, TN 37996-0152
865-974-2445 865-974-4811 fax provost.utk.edu

time, we request transmission to THEC for approval. Please contact me if you have any questions or need additional documentation.

Thank you in advance for your attention to this matter.

Sincerely,

John P. Zomchick
Provost and Senior Vice Chancellor

cc: Donde Plowman
Bernie Savarese
Karen Galicia
Betty Dandridge Johnson
Ozlem Kilic
Vandana Singh
Heather Hartman

Section II: Background

Purpose and Nature of Academic Program

Background and Context of the Proposed Program

The College of Emerging and Collaborative Studies (CECS) engages students in emerging new fields of study, which are typically highly interdisciplinary and, therefore, do not fit in conventional colleges or departments on campus. By integrating offerings across campus (there are currently 900 different degree topics taught at UT), CECS aims to reduce redundancy in the delivery of topics such as data science and artificial intelligence. These topics are relevant to engineering, natural and social sciences, business, and agriculture. For instance, students from all colleges on campus have been registering for CECS courses since Fall 2023.

UTK proposes a new Bachelor of Science in Applied Cybersecurity (BSCYBR). Inspired by the success of Data Science and Artificial Intelligence in CECS, the BSCYBR will mirror this approach by enabling students across the university to take topics relevant to their interests and future careers in a classroom setting that includes a variety of student backgrounds and interests. CECS is building this undergraduate degree on an existing Applied Cybersecurity certificate and minor for undergraduate students and a graduate certificate approved to launch in Fall 2024.

Rooted in an environment that celebrates interdisciplinary instruction and collaboration, the BSCYBR program operates alongside other forward-thinking CECS majors like Data Science and Applied Artificial Intelligence. This setup fosters a rich, collaborative intellectual environment where students, regardless of their major, can delve into cybersecurity applications and related technologies across diverse fields such as social sciences, natural sciences, business, and communications. CECS offers a dedicated drop-by advising office to ensure consistent guidance and support, assisting students in course planning, internship placements, and bespoke career advice, ensuring their educational journey seamlessly aligns with their future professional aspirations. This proposed program aims to produce graduates equipped with a blend of technical prowess and interdisciplinary acumen, ready to navigate and influence the dynamic landscape of the AI-driven future in the field of cybersecurity. The applied nature of this degree emphasizes the practical implementation and real-world application of cybersecurity principles and technologies – students will learn through hands-on work to secure systems and respond to cyber threats. The key distinguishing aspect is the emphasis on the implementation of relevant technology, hands-on skills to identify, mitigate, and prevent security threats, learning operational security (which is relevant to practitioners in all domains), and incident handling to actively respond to security incidents as they occur, including forensics and post-incident analysis.

Program Purpose

The Bachelor of Science in Applied Cybersecurity (BSCYBR) will prepare students to meet the rapidly increasing demand for cybersecurity professionals as organizations face increasing cyber threats and challenges in maintaining safe virtual work environments. The future of the workplace will rely heavily on applied cybersecurity skill sets across numerous industries, including healthcare, government, technology, and business. Applied cybersecurity focuses on real-world environments from all domains, in contrast to mostly technical focus in traditional engineering cybersecurity programs. The BSCYBR undergraduate program will provide an interdisciplinary curriculum building on the expertise of faculty across the university, including faculty from information sciences, law schools, business, agriculture, and other disciplines.

Program Design and Delivery

The proposed program will offer a foundational understanding of cybersecurity concepts, data sources, and tools in a less technical context than a traditional computer science degree. Unlike other cybersecurity programs, this program emphasizes real-world applications across various disciplines. Furthermore, it aims to delve into the methods and components of cybersecurity solutions, assessing potential sources of bias, social impacts, and other ethical considerations related to cybersecurity. These skills are integral to the rapidly growing cybersecurity sector.

The program will be completed by earning 120 credit hours, as required for any bachelor's degree at the University of Tennessee, Knoxville. Of the 120 credit hours, 27 will be CECS core courses taught by CECS full-time faculty and CECS Faculty Fellows appointed from across disciplines at UTK. Additionally, students will complete 6 to 12 credit hours in research, service, and internships to further strengthen their employable skills, expertise, and network. These courses will be taught by CECS faculty and supported by the CECS Director for Partnerships and Engagement and the UTK Center for Career Development to connect CECS students with future employers. Students at UT-Knoxville must fulfill their mandatory VolCore requirement, typically between 51 to 58 credit hours in multiple themes. The remaining 36 credit hours will be selected by students based on their interests in the form of certificates and minors. The program does not offer any concentrations.

Program Modality

The program will be taught in a hybrid format, utilizing a combination of online and face-to-face courses.

Target Audience

The target audience for the proposed program is multifaceted, reflecting the dynamic nature of today's academic and professional landscapes. One significant demographic includes highly focused and motivated students eager to harness the potential of emerging fields like AI and cybersecurity for specific career trajectories, aiming to be at the forefront of the workforce after graduation. In

contrast, there is a segment of students uncertain about their ideal career paths, seeking a platform to explore diverse options while building robust and employable skills. Our collaboration with the Center for Career Development's advising team and esteemed industry partners ensures these students can optimize their credit hours toward gainful employment. Additionally, our program extends its reach to individuals who have completed community college studies or have garnered relevant work experience and now aspire to elevate their academic and professional portfolios with a 4-year degree in an emerging and impactful field. This customizable[1] cybersecurity degree is designed to be inclusive, accommodating a wide array of learners: from UTK honors students and those transitioning with relevant AAS skills via the Tennessee Transfer Pathway (TTP) to professionals aiming to refine their skills in alignment with evolving industry demands. High school graduates within Tennessee and beyond are invited to embark on this transformative journey, tailoring their bachelor's degree at CECS to fit their unique aspirations and career visions.

[1] The degree is customizable to students in that they can choose from a selection of available undergraduate certificates to develop a curriculum that meets each student's unique interests and career goals.

Alignment with State Master Plan and Institutional Mission

State Master Plan[2]

By enabling students from diverse backgrounds to customize their own bachelor's degree, the BSCYBR degree aligns with the "Drive to 55" objective of the THEC Master Plan for postsecondary education, by which 55% of Tennessee's working-age population (ages 25-64) would attain a postsecondary credential by 2025. CECS aims to capture a significant fraction of the Tennessee Transfer Partnership (TTP) students annually to position them to enter the workforce with highly advanced skills at the forefront of the innovation economy. This aim and vision of CECS is supported by the Chancellor of the Tennessee Board of Regents, Dr. Tydings, as evidenced in her letter of support attached in Appendix A. In their 2021 Report, the Tennessee Higher Education Commission reported that students (in the 2014 cohort) who complete a vertical transfer (from a two-year institution to a four-year institution) earned a wide variety of degrees, with almost three-quarters earning a degree in six years, including over 25% of students earning both an associate and a bachelor's degree.

UT Knoxville has the highest graduation and first-to-second-year retention rates among the state's public institutions and has developed innovative programs and support structures to help students thrive in and out of the classroom. As a doctoral university holding the highest Carnegie classification for research activity and designated as a Carnegie Community Engaged Institution, UT-Knoxville allows students to learn from faculty at the forefront of their fields.

The BSCYBR program is expanding the University of Tennessee, Knoxville's mission of innovation, customization, and quality education. Through internship placements, research courses, and capstone projects, BSCYBR students can conduct real-world research that affects their communities and allows them to work alongside faculty in campus laboratories and the field.

Institutional Mission

Importantly, this program aligns directly with The University of Tennessee, Knoxville mission, which states:

> *We are a diverse community with a shared commitment to discovery, creativity, learning, and engagement. At UT Knoxville, we: Empower learners of all ages and backgrounds to achieve their dreams through accessible and affordable education and state-of-the-art research training opportunities. Advance the prosperity, well-being, and vitality of communities across Tennessee and around the world through our research, teaching, service, and engagement. Commit to excellence, equity, and inclusion within the university, across the state, and in all our global activities.*

[2] https://www.tn.gov/content/dam/tn/thec/bureau/research/other-research/master-plan/finalmp.pdf

The proposed Applied Cybersecurity program at UTK aligns seamlessly with the university's mission as a leading land-grant research institution. The program mirrors UTK's commitment to applied research and community engagement by emphasizing hands-on learning and community impact. It strengthens ties with strategic partners like the Oak Ridge National Laboratory, driving innovation in intelligent machines and society. Furthermore, the program aligns with UTK's goal of preparing its graduates to be industry, government, and community leaders. Given the high demand for cybersecurity professionals, many of these graduates will likely remain in Tennessee, contributing to the state's growth. The Applied Cybersecurity program fits seamlessly within UTK's organizational structure, reinforcing its mission, partnerships, and vision for its graduates.

Moreover, the proposed program aligns with UTK's organizational structure and overall mission as a state's flagship land-grant research institution. The program adds to the portfolio of UTK's forward-thinking academic offerings, reflecting its commitment to staying at the forefront of technology and innovation. The interdisciplinary nature of the program will encourage collaboration among various academic departments, leveraging the strength of over 1,800 full-time faculty members across diverse fields.

The applied nature of this program also aligns with UTK's dedication to hands-on coursework and real-world research experiences. Students will be able to conduct research and develop solutions that directly impact their communities, echoing the university's commitment to community engagement. The Applied Cybersecurity program could contribute to UTK's standing as a top institution for research activity and community engagement and aligns with UTK's goal to equip its graduates to become industry, government, and community leaders, particularly in the growing AI and cybersecurity sector. With the high demand for AI-skilled cybersecurity professionals, many of these graduates will likely remain in Tennessee, fulfilling UTK's vision of giving back to the state through its alumni.

Institutional Capacity to Deliver the Proposed Program

The Applied Cybersecurity program will increase UT Knoxville's overall impact by catalyzing innovative, intercollegiate undergraduate courses, stackable certificates, minors, and bachelor's programs. CECS programs will attract new students from across the state because interest in cybersecurity programs is increasing. Computer science programs do not offer a pathway to students who do not have computer science foundation courses. The CECS program will fill that gap by creating core courses that students from STEM and non-STEM backgrounds can take and progress towards specializations for non-programming professional opportunities.

CECS has developed a straightforward rubric for revenue sharing via student credit hour (SCH) allocation, given that UTK now uses a budget allocation model (BAM) under which colleges manage their revenues and expenditures. The basic model is that 80% of the SCH goes to the college teaching the course, with 20% going to the student's home college. Students majoring in the program would be CECS students, so when they take a gateway course such as CYBR 101, CECS keeps 100% of the SCH. When students from other colleges take CYBR 101, CECS retains 80% of the SCH; when CECS students take electives in other colleges, those colleges retain 80% of the SCH. It is a simple and effective resource allocation model that promotes buy-in from other colleges since they will receive 80% of the revenue from CECS students.

CECS supports sustainability in this program at multiple levels. CECS is hiring a full-time lecturer to support the CECS courses in the applied cybersecurity program. One full-time lecturer teaches up to eight courses per year. The Program Directors and Program Coordinators, appointed by CECS, oversee the curriculum and enrollment, course scheduling, assessment, accreditation, capstone, and research course contents. The Program Directors collaborate with the faculty across UTK to develop and approve new certifications and minors. The CECS Director of Marketing oversees advertising, outreach, and prospective student recruitment. The CECS Director of Advising oversees the advising of all CECS majors in their degree program operations. The Director of Partnerships and Economic Development will also engage campus, community, and industry partners to support experiential learning in the program, fostering pathways to student employment.

The curriculum is supported by a campus-wide curriculum committee that works with the CECS Program Director and CECS-appointed Faculty Fellow as the lead. The committee develops and manages the curriculum, updates the courses, and selects relevant elective courses from across the university. This demonstrates the collaborative structure at the core of all CECS academic programs.

Existing Programs Offered at TN Institutions

The Classification of Instructional Programs (CIP) Code 11.1003 - Computer and Information Systems/ Security/ Auditing/ Information Assurance is the CIP code that most closely aligns with the proposed Applied Cybersecurity program. Using the 11.1003 CIP code, we identified nine programs at the bachelor's level in the field of cybersecurity. We found five institutions in Tennessee that offer a BS in Cybersecurity degree and four additional institutions that offer a BS in Computer Sciences (or computing) with a Cybersecurity concentration. These degrees are largely computer science-based, with all but one being housed in computer science or computing departments (MTSU's BS degree is housed in the College of Business, Department of Information Systems & Analytics). The four bachelor's programs that offer a Computer Science, Bachelor of Science program with a Cybersecurity concentration are classified with a CIP code of 11.0701 (Computer Science).

Table 1 outlines all public and private institutions that offer programs in the 11.1003 CIP code at various levels (Technical and Undergraduate Certificate – 4 programs; Bachelor's – 5 programs; Graduate Certificate – 3 programs; and Master's – 2 programs.

Program CIP Codes

Our proposed Applied Cybersecurity program significantly differs from the existing programs because we are creating a major for all students, not just computer science and programming majors. The program will broaden access to employment opportunities in cybersecurity-related areas. As evidenced by all the letters of support we have received from the industry, there is a great demand for students across domains to be skilled in applied cybersecurity competencies. The proposed program is unique and distinct from the existing cybersecurity programs because it focuses on cybersecurity infrastructure as a whole, including management, risk management, cybersecurity policy frameworks, human factors in cybersecurity, AI and cybersecurity. etc. and not limited to programming for cybersecurity.

Table 1

Existing Programs in the State

Institution Name	Program Title and Degree Designation	CIP Code	Description/ Focus of Program	Degrees Awarded
Technical and Undergraduate Certificates (4) *				
Columbia State Community College	Cybersecurity Technical Certificate (24 SCH)	11.0103	According to the website, "This one-year program is designed to prepare graduates for entry level positions as information security analysts. This program focuses on network and computer security. The program will provide students with foundational knowledge and skills for COMPTIA Security+ certification. All technical certificate courses can be applied toward the A.A.S. degree in Computer Information Technology, Cyber Defense concentration.	2020-21: 2 2021-22: 9 2022-23: 0
Jackson State Community College	Cybersecurity Technician Technical Certificate	11.1003	The technical certificate consists of 10 courses that covers various topics such as Networking Security, Information Assurance, Digital Forensics, and Windows Server Administration.	2020-21: 5 2021-22: 1 2022-23: 1
Nashville State Community College	Information Security Technical Certificate (18 SCH)	11.1003	The Information Security Technical Certificate provides students with the necessary skills to protect an organization's resources using security tools on a variety of operating systems. The program covers methods employed by hackers to compromise computing devices and prepares students to recognize compromised systems. The program emphasizes the importance of security policies and the techniques to effectively design such policies. Prepares the student for the CompTIA Security+ certification exam, which is highly recommended for security professionals.	2020-21: 26 2021-22: 24 2022-23: 21 Figures include awards for 3 technical certificates in CIP Code 11.
University of Tennessee Southern	Cybersecurity Undergraduate Certificate	11.1003	An undergraduate certificate that includes courses in operating systems analysis, information systems security, digital forensics, and cyber-crime.	Not available

Institution Name	Program Title and Degree Designation	CIP Code	Description/ Focus of Program	Degrees Awarded
	(18 SCH)			
Bachelor's Programs (5)				
Lipscomb University	Cybersecurity Bachelor of Science	11.1003	Cybersecurity degree program covers the breadth of cybersecurity, from theoretical frameworks to models to policies and ethical practices. It focuses on security challenges, threats, and requirements for operating systems, computer architectures, networking protocols, and organization data and information. It ensures you will develop the necessary skills to become an indispensable asset in the technology field.	Not available
Middle Tennessee State University	Cybersecurity Management Bachelor of Science	11.1003	A major in Cybersecurity Management consists of 46 hours of information systems and cybersecurity management courses. The Cybersecurity Management program will provide students with the knowledge and skills to develop, maintain, and manage cybersecurity systems within a business context. Additionally, the degree will allow students to begin their careers in the field and to enter organizations with a focus on meeting their security needs. The program includes a required Business Administration minor.	Program implemented Jan 2024 Projected graduates starting in 2025-26: 4, 9, and 14
University of Tennessee at Chattanooga	Information Technology in Cybersecurity Bachelor of Applied Science	11.1003	The Information Technology in Cybersecurity program is a cohort-based program that has been developed for adult learners and transfer students, who have already completed their associate degree, and would provide an accelerated one-year curriculum. The program includes an internship to maximize student learning opportunities which will provide opportunities for the direct application of class concepts into workplace settings. Students enrolled in the program will be prepared to sit for high-level industry certifications such as Certified Information System Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA), and NIST Cybersecurity Framework (NCSF).	Program implemented Jan 2023 Projected annual graduates from 2023-27: 11, 22, 26,45, and 45

Institution Name	Program Title and Degree Designation	CIP Code	Description/ Focus of Program	Degrees Awarded
University of Tennessee at Martin	Cybersecurity Bachelor of Science	11.1003	The Bachelor of Science in Cybersecurity will prepare you to help companies manage vital information, perform penetration testing, and secure networks from intrusion." 51 hours of coursework within the Cybersecurity major. The 51 hours of coursework in the major consist of 36 hours of computer science courses, 28 hours of cybersecurity courses, and 7 hours of math courses.	Program implemented Aug 2022
University of Tennessee Southern	Cybersecurity Bachelor of Science	11.1003	The Cybersecurity major includes courses in mathematics, computer science, criminal justice, and business, and it prepares graduates for multiple careers in cybersecurity, including both technical and managerial paths. Of the 120 hours program requirement, 59 hours are cybersecurity courses.	Program implemented 2021 3 graduates in 2023-24
Graduate Certificate Programs (3) *				
Austin Peay State University	Cybersecurity Executive Graduate Certificate (15 SCH)	11.1003	The Executive Certificate program affords students an opportunity to study information security organizational structure design and management, policy and governance, risk management, legal and compliance issues, incident response and forensics team formation, training, financial management, and outsourcing.	Not available
Austin Peay State University	Risk Analysis Graduate Certificate (12 SCH)	11.1003	The Risk Analysis graduate certificate is designed for students or working professionals with a bachelor's degree who would like to gain skills in risk analysis. This certificate prepares students to recognize, assess, analyze, and manage risks inherent in all institutions. The twelve-hour graduate certificate is offered fully online and on-campus."	Program implemented Aug 2022 2022-23: 15 certificates awarded
University of Memphis	Cybersecurity & Inform Assurance Graduate Certificate (12 SCH)	11.1003	This certificate program highlights important aspects of information security and assurance technologies. These security standards specify the minimum knowledge, skills and abilities required to fulfill the duties of an information systems security professional, senior system manager, and system administrator.	2021-22: 7 2022-23: 2 2023-24: 1

Institution Name	Program Title and Degree Designation	CIP Code	Description/ Focus of Program	Degrees Awarded
Master's Programs (2)				
Middle Tennessee State University	Cybersecurity Management Master of Science	11.1003	This STEM-designated program, offered online with 7-week classes, provides a flexible and convenient learning environment tailored to the needs of working professionals. Explore topics such as risk management, incident response, security architecture, cybersecurity governance, and advanced threat analysis. With a curriculum that blends theoretical learning with practical application, you will master strategies for implementing robust security measures, establishing comprehensive security protocols, and managing evolving digital threats.	Program implemented May 2024
University of Tennessee Knoxville	Business Cybersecurity Master of Science	11.1003	The online 30-hour master's program lays the principal groundwork of business cybersecurity concepts. Along with sound technical training, graduates will be able to comprehend, communicate, and employ business strategies crucial to protecting data.	Program implemented Jan 2024

** At the University of Tennessee, Knoxville, the undergraduate and graduate certificates in Applied Cybersecurity (11.1003) will be implemented in fall 2024 and are not listed in Table 1.*

Accreditation

Like all academic programs at the University of Tennessee-Knoxville, the undergraduate major in Applied Cybersecurity will be regionally accredited by SACSCOC[3]. After three years, we plan to apply for the National Center of Academic Excellence in Cybersecurity (NCAE-C) in Cyber Defense (CD) designation. This is referred to as CAE-CD, and institutions are eligible to apply after they have completed three years.[4]

The Accreditation Board for Engineering and Technology (ABET) accredits programs in applied and natural science, computing, engineering and engineering technology. Since 2018, ABET began accrediting programs in cybersecurity. ABET accreditation would not be appropriate for the proposed Applied Cybersecurity program since this program's focus is not the "traditional" computing-based field. Therefore, the proposed Bachelor of Science in Applied Cybersecurity program will participate in the program evaluation in the 2030-35 Quality Assurance Funding program. Since the proposed program will enroll students in August 2025, the program will be classified as a new program and exempt from the 2025-30 QAF cycle.

[3] https://sacs.utk.edu/

[4] https://caecommunity.org/about-us/what-cae-cybersecurity

Section III: Feasibility Study

Local and Regional Workforce Needs/Demand

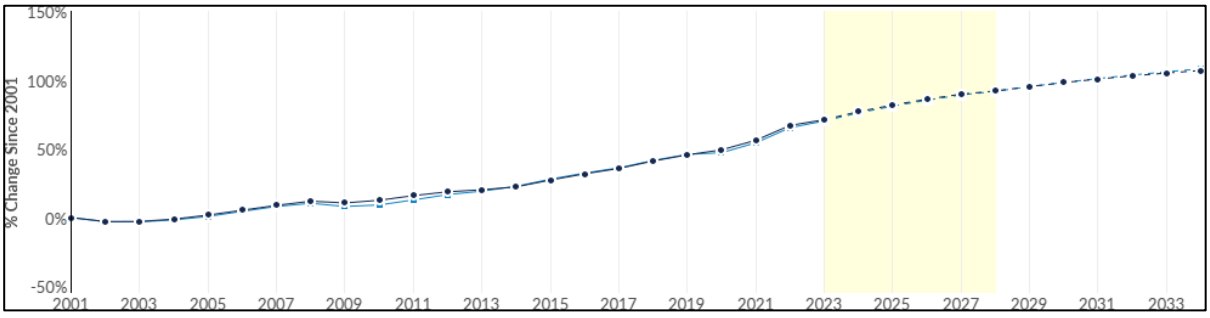
We conducted our analysis to assess local, regional, and employer demand through Lightcast (a labor market analytics firm that combines data from government sources like the Bureau of Economic Analysis, U.S. Census Bureau, and Bureau of Labor Statistics into one dataset that details industries, occupations, demographics, academic programs, and more). For this analysis, we used the term Region to include Tennessee, North Carolina, Virginia, Kentucky, Mississippi, Arkansas, Alabama, Georgia, and Missouri.

Anticipated Job Openings and Workforce Projections: 2024 – 2033

Jobs have been steadily increasing in the region since 2001 and are expected to grow at a higher rate in the next 5 to 10 years, as shown in Figure 1 below.

Figure 1:

Percent Change in Jobs since 2001 (Source: Lightcast)



The anticipated job openings for the next five years are projected to show a **12.2% increase in the region**, comparable to the 12.6% expected growth in the number of jobs nationwide. See Table 2.

Table 2*:*

Percent Change in Jobs: 2023 to 2028 (Source: Lightcast)

	2023 Jobs	2028 Jobs	Change	% Change
Region	1,086,062	1,218,873	132,811	12.2%
Nation	6,423,475	7,235,569	812,094	12.6%

For the Job Title Information Security Analysts, a growth of 16.5% is expected by 2028. (Source: Lightcast Target Occupations growth). Looking at occupations by state, we found that, specifically for Tennessee, an 18% higher growth rate in jobs is expected, higher than the neighboring states.

Table 3:

Occupation Growth Rate by States in the Region (Source: Lightcast)

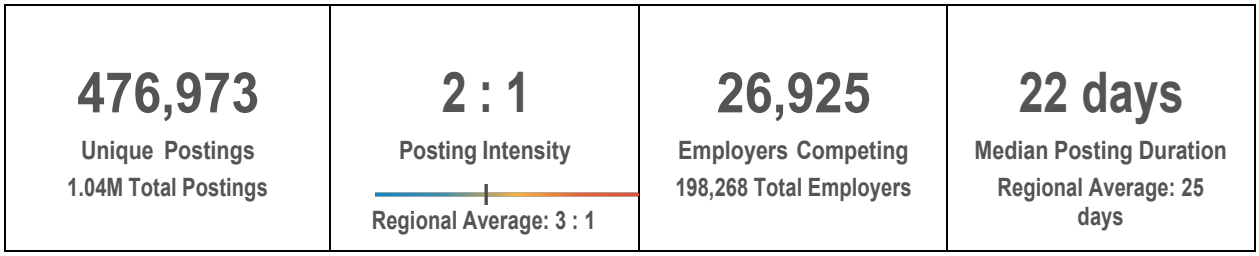
State	2024 Jobs	2034 Jobs	2024 -2034 Change	2024 -2034 % Change
Virginia	88,950	98,042	9,092	10%
Georgia	83,176	96,039	12,863	15%
North Carolina	81,541	92,467	10,926	13%
Tennessee	47,444	55,896	8,452	18%
Missouri	46,747	49,875	3,128	7%
Alabama	27,950	30,437	2,487	9%
Kentucky	20,516	22,367	1,851	9%
Arkansas	12,685	14,505	1,820	14%
Mississippi	9,911	11,640	1,729	17%
Total	**418,919**	**471,268**	**52,349**	**12%**

Labor Market Analysis

From June 2023 to May 2024, there were 1.04M total job postings for this area, of which 476,973 were unique. These numbers give us a Posting Intensity of 2-to-1, meaning that there is one unique job posting for every two postings.

Figure 2

Unique Job Postings: June 2023 to May 2024 (Source: Lightcast)



Similar Academic Programs and Local Demand

The regional job posting breakdown shows that Tennessee and neighboring states are hiring in this area of expertise. Nashville is one of the cities in Tennessee that is a high-employment area for expertise in cybersecurity.

Table 4:

Unique Job Postings in Selected States. (Source: Lightcast)

State	Unique Postings (Jun 2023 - May 2024)
Virginia	148,481
Georgia	85,282
North Carolina	83,257
Missouri	41,449
Tennessee	36,960

Potential Jobs for Applied Cybersecurity Graduates

According to the Lightcast report, the average monthly postings for Applied Cybersecurity related jobs in the region in the last ten years (from May 2014 - May 2024) are 18,245 with the number of monthly hires being 14,313 showing a deficit of about four thousand skilled candidates. This is also reflected in the number of graduates (13,935) from the regional programs in 2023 as shown in Figure 5. The total number of degree completions in the region are lagging behind the total number of employees needed. Our proposed program will play a part in reducing this deficit in the six occupations listed below in Table 6. Four of the six occupations align with the CIP code 11.1003 for the proposed Applied Cybersecurity program. These occupations are Computer Network Architects (15-1241), Network and Computer Systems Administrators (15-244), and Computer and Information Systems Manager (11-3021), and Computer Network Support Specialists (15-1231).

Figure 3 Program Completions CIP Code 11.1003 by Delivery Method (Source: Lightcast)

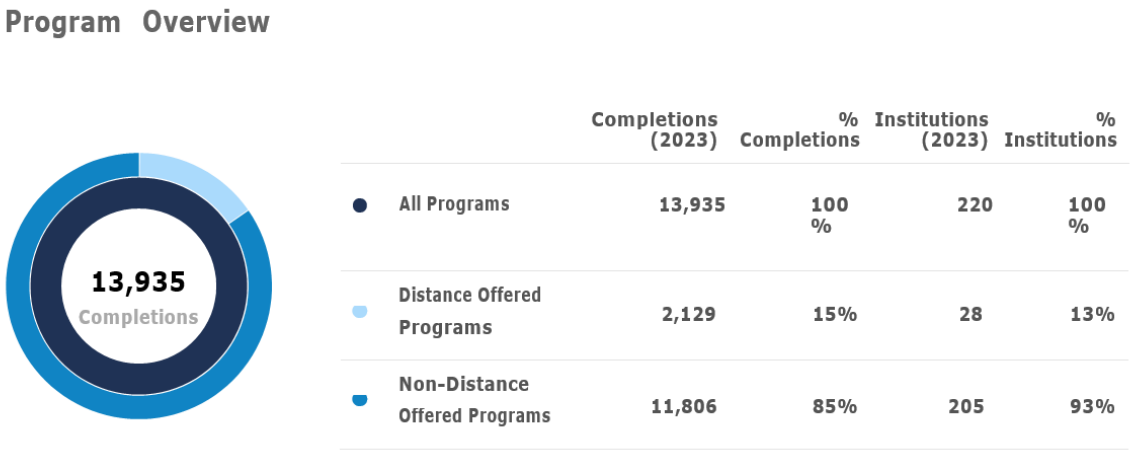


Table 5

Average Monthly Posting and Average Monthly Hires (Source: Lightcast)

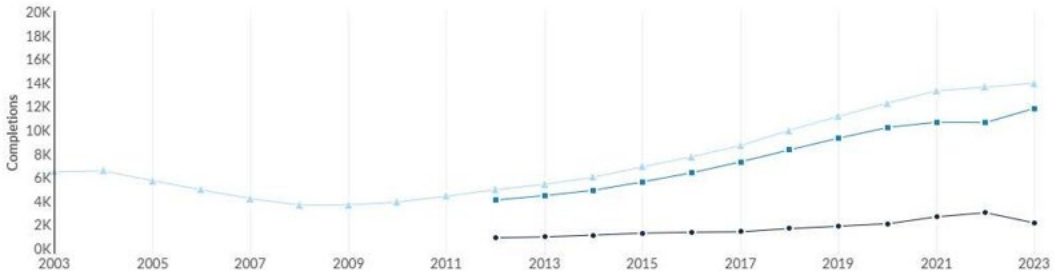
SOC Code and Occupation	Avg Monthly Postings May 2014 – May 2024	Avg Monthly Hires May 2014 – May 2024
15-1299 Computer Occupations, All Other	9,298	3,055
15-1232 Computer User Support Specialists	3,888	4,292
15-1241 Computer Network Architects	2,385	1,388
15-244 Network and Computer Systems Administrators	2,147	1,772
11-3021 Computer and Information Systems Manager	322	2,574
15-1231 Computer Network Support Specialists	204	1,232

Overall, the degree programs offered as well the degree completions in this field have consistently increased in the last ten years (Figure 7) demonstrating a need and growth in the area. The University of Tennessee, Knoxville and the College of Emerging and Collaborative Studies is in a great position to contribute to this area of growth in the region and produce high quality graduates to meet the regional demand in applied cybersecurity

Figure 4

Degree Completions:– 2012 - 2023

Regional Trends



	2012 Completions	2023 Completions	% Change
Distance Offered Programs	876	2,129	+143.0%
Non-Distance Offered Programs	4,059	11,806	+190.9%
All Programs	4,935	13,935	+182.4%

Appendix A: Letters of Support

The following partners have provided letters of support for the proposed Bachelor of Science in Applied Cybersecurity:

1) Dr. David White
   Interim Dean
   Herbert College of Agriculture University of Tennessee Knoxville
   Knoxville, TN
2) Dr. Jothany Reed
   Vice Chancellor of Academic Affairs
   Tennessee Board of Regents – The College System of Tennessee
   Nashville, TN
3) Mr. David B. Rausch
   Director, Tennessee Bureau of Investigation
   Nashville, TN

HERBERT
COLLEGE OF AGRICULTURE
THE UNIVERSITY OF TENNESSEE, KNOXVILLE

Office of the Dean
2621 Morgan Circle
126 Morgan Hall
Knoxville, TN 37996
865-974-7303
herbert.tennessee.edu

03/05/24

To whom it may concern,

As Interim Dean of the Herbert College of Agriculture, I am writing to support launching the new undergraduate degree, Bachelor of Science in Applied Cybersecurity, in the College of Emerging and Collaborative Studies at the University of Tennessee Knoxville.

The proposed program, Bachelor of Science in Applied Cybersecurity (BSCYBR) will provide an interdisciplinary curriculum building on the expertise of faculty across the university. The CECS Customizable degree is not only about topics but about the ability to bring interdisciplinary teams together quickly and to apply innovative approaches to solve real-world problems.

For the applied cybersecurity degree, each CECS student is required to take at least one service-research course and one internship course off campus. Herbert will be able to assist CECS in engaging industry and community partners with internship and service opportunities for students. Across Herbert departments and other Institute of Agriculture units, faculty and students partner with numerous organizations, including ORNL, Volkswagen, Jack Daniels Distillery, and Tyson Foods, and are able to conduct real-world research at our 10 AgResearch education centers spread across the state.

Related to CECS, Herbert offers a wealth of instruction and research (capstone project) opportunities across our 11 majors that are highly aligned with Data science, AI, and Cybersecurity applications. Our new faculty appointments in precision agriculture, for instance, establishes strengths in applying statistics and data science to agriculture sciences and natural resources management. The UT Precision Livestock Farming program, for example, is essentially based on data science through the real-time monitoring of images, sounds, and physiological and environmental data in livestock and poultry housing, feeding, and watering systems, as well as other production system components.

In summary, we are looking forward to partnering with the CECS Applied Cybersecurity degree program. Herbert College of Agriculture fully understands the need for students in the future workforce to combine a wide range of skills and emerging disciplines to address the complex challenges of population growth, evolving technology, and increasing globalization, including data-driven intelligence solutions for food and nutrition security, climate-adapted agriculture, and the evolving economy.

Please let me know if I may be of any further assistance in this regard.

Sincerely,

David G. White, Ph.D.
Interim Dean, Herbert College of Agriculture
University of Tennessee Institute of Agriculture
University of Tennessee Knoxville

THE COLLEGE SYSTEM of TENNESSEE
1 Bridgestone Park, Third Floor
Nashville, Tennessee 37214
615-366-4400 OFFICE 615-366-3922 FAX
tbr.edu

February 28, 2024

To Whom It May Concern:

As the Vice Chancellor of Academic Affairs at the Tennessee Board of Regents, I am writing in support of the customizable applied cybersecurity degree being developed at the College of Emerging and Collaborative Studies (CECS). This 4-year degree, highly accessible to community colleges of Tennessee, will instill workforce skills relevant to emerging fields, including applied cybersecurity, Artificial Intelligence, and Data Science, customized to apply to the areas of each student's interest. With access to 4-year higher education via the Tennessee Transfer Pathway (TTP), the CECS cybersecurity degree will channel Tennessee community college graduates into employment in the new innovation economy centered around a safer digital economy.

As a home for new cohorts of interdisciplinary UTK students seeking future-oriented degrees, CECS was mandated by the UT Board of Trustees to enhance student engagement, creativity, and collaboration. With new majors in CECS in emerging topics, CECS will provide highly motivated students from STEM fields in the applied Cybersecurity program with the core set of classes as a basis for the foundational knowledge, as well as advising and informal interaction that is crucial for students to develop their own 4-year curriculum and career goals.

Among 4-year colleges and universities in Tennessee, CECS is unique in how it engages industry and community partners with internship and service opportunities for students. The goal is for each student to engage with the real world in preparation for future employment. The requirement for each CECS student to take at least one service-research course and one internship course off campus is an innovative approach to help CECS graduates develop awareness and align with workforce needs.

CECS aims to capture a significant fraction of the TTP students per year to position them to enter the workforce with highly advanced skills at the cutting edge of the innovation economy. Currently, CECS is working with the TBR to facilitate a transfer plan for students across the state of Tennessee. In a 2021 Report, the Tennessee Higher Education Commission reported that students (in the 2014 cohort) who complete a vertical transfer (from a two-year institution to a four-year institution) earned a wide variety of degrees, with almost three-quarters earning a degree in six years, including over 25% of students earning both an associate and a bachelor's degree. The cybersecurity degree can allow UT students to enter a wide range of the workforce sector. In Tennessee and the nation, almost every sector is now applying or seeking to apply A.I. and data science to their business, which also requires the continual evolution of the cyber defense component.

Along these lines, CECS is poised to continue to add new partnerships within the state—as well as nationally and even internationally. This will contribute highly skilled employees to the workforce of Tennessee, which in turn attracts new and established companies to invest in our state. The cybersecurity degree also expands the career aspirations of a diverse range of students, many of whom use the Tennessee Transfer Pathway to pursue a 4-year degree directly after community college or after a period of work experience as CECS will be flexible to recognize such experiences as credit.

In our rapidly evolving world, where new technologies and industries emerge unprecedentedly, academic institutions must adapt to prepare graduates for the future. The state of Tennessee would benefit from CECS's certificate programs, combining disciplines and integral entrepreneurial skills that will fuel the state's economy and prosperity. For these reasons, I strongly support the creation of the custom degree under CECS.

Jothany Reed, Ed.D.
Vice Chancellor for Academic Affairs
TBR – The College System of Tennessee
jothany.reed@tbr.edu

TENNESSEE BUREAU OF INVESTIGATION
901 R.S. Gass Boulevard
Nashville, Tennessee 37216-2639
(615) 744-4000
Facsimile (615) 744-4500
TDD (615) 744-4001

BILL LEE
GOVERNOR

DAVID B. RAUSCH
DIRECTOR

March 7, 2024

To Whom It May Concern:

I am writing to convey enthusiastic endorsement of the Tennessee Bureau of Investigation for the establishment of a collaborative partnership with the University of Tennessee, Knoxville's College of Emerging & Collaborative Studies in the development and launch of the Bachelor of Science in Applied Cybersecurity.

Cybersecurity is of paramount importance at TBI, both because we must defend our own systems and data, and because our cybercrime investigators work with our partners in State government and the law enforcement community to respond to criminal acts against government, businesses, and private citizens. In support of these goals, TBI must seek out the best and the brightest to securely manage information, mitigate external threats, and reinforce the resilience of digital systems, as well as understand the ways in which they can be compromised by threat actors.

The Applied Cybersecurity degree program at CECS appears thoughtfully designed to provide students with a foundational understanding of cybersecurity concepts, data sources, and tools, presented in a comprehensive yet accessible context. TBI is always looking for opportunities to meet and collaborate with the next generation of network defenders and cyber investigators. As a result, we see significant value in collaborating with the faculty and students involved in shaping this innovative program.

In the dynamic landscape of the IT industry, a Bachelor of Science program in Applied Cybersecurity positions students effectively for success, aligning with the ever-evolving needs of our digital world. TBI would surely benefit from an institution with the resources and reputation of the University of Tennessee to establish this program so that we can join together in protecting Tennessee from cyber threats.

We are enthusiastic about the potential opportunities this collaboration will bring to students, faculty, and the broader IT community.

Sincerely,

David B. Rausch
Director
Tennessee Bureau of Investigation

Appendix B: Supplemental Information for Feasibility Study

Two surveys of current undergraduate students at the University of Tennessee Knoxville indicated a strong interest in the undergraduate major in cybersecurity. The first survey was distributed to two undergraduate listservs to ensure a diversity of disciplines in the responses. The survey was distributed to undergraduate students in the Tickle College of Engineering (3716 students) and the School of Information Sciences (199 students) at UTK. The survey was distributed for one week in July 2023. As of August 1st, 2023, 281 responses were received, making it a response rate of a little above 7%. The response rate is impacted by the fact that this is a summer semester, and not all the students register for summer classes – reducing the total number of students available to respond.

Below are results from a few questions from the survey conducted to document student interest in an undergraduate major.

Question 1 - If a multidisciplinary BS in Emerging and Collaborative Studies had been available to you and offered a choice of different areas of study, how interested would you have been in pursuing each area of study or major?

The results in Table A1 indicate that more than 60% of the students who responded to the survey indicated an interest in a cybersecurity program. This was the highest-rated program among the ten options provided to the students.

Table A1

Interest in Different Programs Planned by CECS

#	Question	Extremely interesting Number (%)	Moderately interesting Number (%)	Not interesting at all Number (%)
1	Cybersecurity	58 (21)	127 (45)	81 (29)
2	Artificial Intelligence	99 (35)	124 (44)	43 (15)
3	Data Science	70 (25)	115 (41)	81 (29)
4	Human-Computer Interaction	74 (26)	110 (39)	83 (30)
5	Design Studies	61 (22)	99 (35)	107 (38)
6	Graphic Design Studies	47 (17)	92 (33)	127 (45)
7	User Experience Design	48 (17)	94 (33)	125 (44)
8	Law Tech	32 (11)	88 (31)	147 (52)
9	Game Design	97 (35)	93 (33)	97 (35)
10	Sustainability	73 (26)	113 (40)	81 (29)

Question 3 - If a multidisciplinary BS in Emerging and Collaborative Studies had been available to you and offered a choice of different certificates, how likely is it that you would have selected this certificate or major?

Table A2

Interest in the Selection of a Certificate from CECS

#	Question	Extremely interested Number (%)	Moderately interested Number (%)	Not interested at all Number (%)
1	Cybersecurity	55 (20)	102 (36)	111 (40)
2	Artificial Intelligence	73 (26)	118 (42)	74 (26)
3	Data Science	62 (22)	97 (35)	105 (37)
4	Human-Computer Interaction	42 (15)	101 (36)	124 (44)
5	Design Studies	41 (15)	89 (32)	137 (49)
6	Graphic Design Studies	38 (14)	82 (29)	146 (52)
7	User Experience Design	31 (11)	84 (30)	151 (54)
8	Law Tech	24 (9)	81 (29)	162 (58)
9	Game Design	50 (18)	103 (37)	114 (41)
10	Sustainability	45 (16)	106 (38)	116 (41)

More than 50% of students who responded said that they would have selected the cybersecurity program if it had been available when they joined the University of Tennessee Knoxville.

A new survey was sent to the CECS committee in February 2024, asking the students specifically about the cybersecurity program that CECS intends to develop. This survey was sent to approximately 1,000 students in different undergraduate classes at UTK. As of August 1st, 2023, 93 responses were received, making the response rate a little above 9%.

The results of this survey are presented below.

Survey Question 1 -If a BS in "Applied Cybersecurity" with opportunities for multidisciplinary education (with certificates in Data Science, Artificial Intelligence, Human-Computer Interaction, Cyber Law, Game Design, etc.) had been available for non-computer science majors when you were choosing your major at UT, how interested would you have been in this major?

Table A3

Interest in the Selection of a Certificate from CECS

Extremely Interested	Neither Likely nor Unlikely	Extremely Unlikely
44 (47%)	37 (40%)	12 (13%)

The results from this new survey in February 2024 show that about half of the students who took the survey are extremely interested in the Applied Cybersecurity program, with about forty percent undecided. This is a positive indication of students' interest in this program.

Survey Question 2 - If a BS in "Applied Cybersecurity" had been available to you and offered a choice of different areas of concentration, how interested would you have been in pursuing each concentration or major?

Table A4

Interest in the Selection of a Certificate from CECS

#	Question	Extremely Interested	Moderately Interested	Not interested at all
1	Cybersecurity	20 (21%)	59 (63%)	16 (17%)
2	Cryptology	15 (16%)	49 (52%)	32 (34%)
3	Artificial Intelligence	43 (46%)	44 (47%)	8 (8%)
4	Data Science	53 (56%)	36 (38%)	7 (7%)
5	Human-Computer Interaction	29 (31%)	51 (54%)	26 (27%)
6	Law Tech	14 (15%)	31 (33%)	51 (54%)
7	Game Design	26 (27%)	40 (43%)	30 (32%)

The results from this question about different areas of concentration demonstrate that the cybersecurity option will be very popular, with about 85% of students indicating some interest in the concentration. A specialization in Artificial intelligence is the most popular, with more than 90% of students indicating an interest. Similarly, the Applied Cybersecurity major with a concentration in Data Science has a large appeal to the students surveyed—over 90% indicating some interest in this combination.

Results from both surveys are very positive about student interest in Applied Cybersecurity. The College of Emerging and Collaborative Studies, with its existing undergraduate majors in Applied Artificial Intelligence and Data Science (to be launched in Fall 2024), is well prepared to meet this overwhelming student interest in these emerging fields.