NEW PROGRAM PROPOSAL FORM

Name of Institution: South Carolina State University

Name of Program (include degree designation and all concentrations, options, or tracks):
MS in Cybersecurity

Program Designation:

- ☐ Associate's Degree
- ☒ Master's Degree
- ☐ Bachelor's Degree: 4 Year
- ☐ Specialist
- ☐ Bachelor's Degree: 5 Year
- ☐ Doctoral Degree: Research/Scholarship (e.g., Ph.D. and DMA)
- ☐ Doctoral Degree: Professional Practice (e.g., Ed.D., D.N.P., J.D., Pharm.D., and M.D.)

Consider the program for supplemental Palmetto Fellows and LIFE Scholarship awards?

- ☐ Yes
- ☒ No

Proposed Date of Implementation: Fall 2025

CIP Code: 43.0404

Delivery Site(s): South Carolina State University, Main Campus, Orangeburg, South Carolina

Site Code(s): 50602

Delivery Mode:

- ☐ Traditional/face-to-face
  *select if less than 25% online
- ☐ Distance Education
  - ☒ 100% online
  - ☐ Blended/hybrid (50% or more online)
  - ☐ Blended/hybrid (25-49% online)
  - ☐ Other distance education (explain if selected)

Program Contact Information (name, title, telephone number, and email address):

Dr. Nikunja Swain, Chair
201 Engineering and Computer Science Complex
South Carolina State University
Orangeburg, SC 29117
Telephone: (803) 536-8675, Email: swain@scsu.edu

Institutional Approvals and Dates of Approval (include department through Provost/Chief Academic Officer, President, and Board of Trustees approval):

Chair, Department of Computer Science	03-27-2023
Dean, College of Science, Technology, Engineering, Math., and Transportation	03-30-2023
Educational Policies Council:	05-04-2023
Faculty Senate:	12-12-2023
Vice president of Academic Affairs:	05-04-2023
President:	05-17-2024
Board of Trustees:	05-17-2024

Background Information

State the nature and purpose of the proposed program, including target audience, centrality to institutional mission, and relation to the strategic plan.

Nature and Purpose

The MS in Cybersecurity program aims to provide students with knowledge and skills to secure network, systems, and data, plan and develop security solutions, and perform analysis to obtain insights on vulnerabilities, and security incidents. Therefore, the Master of Science in Cybersecurity program would offer three areas of concentration (tracks) of study within the major field of Cybersecurity, including: 1) Network Defense, 2) Digital Forensics, and 3) Cyber-Physical Systems Security (CPS). Another feature is that 16 out of the 21 courses include online hands-on labs that will provide students with the practical skills necessary to solve real-world cybersecurity problems. Finally, the proposed curriculum is different from the existing curriculum at Institutions in South Carolina in terms of incorporating data analytics and machine learning from a security perspective. thereby allowing students to have a competitive edge in the future workplace. Graduates of the proposed program can pursue careers paths such as information security analyst, Cybersecurity engineer, penetration tester, and digital forensics analyst.

Target Audience

The target audience of this program includes students who are interested in pursuing a career in Cybersecurity. Due to blended nature, our program can serve the needs of both traditional and non-traditional students. The asynchronous approach of this proposed degree program provides the students with flexibility of learning, time management, learning at one's own space, visiting the course material as needed, and asking questions in the discussion forum to clarify concepts.

The target audience for this online graduate program includes both STEM and non-STEM majors from colleges and universities across South Carolina, the Southeast, and the nation. Students with bachelor's degree in STEM or related fields with undergraduate preparation in cybersecurity can directly start the MS coursework. Students with bachelor's degrees without undergraduate preparation in cybersecurity will need to complete an introductory undergraduate cybersecurity course before beginning the coursework of the MS degree curriculum.

Because the program is 100% online, we are expecting an enrollment of 10 students per year in the program. This estimate is derived from several factors, including the topic's significance, personal observations, and communications with members of our Industrial Advisory Council (IAC), inquiries from undergraduate students, and anticipated workforce development needs in South Carolina.

All discussions about the MS in Cybersecurity program took place through presentations given to the IAC members by the Chair of the Computer Science and Mathematics Department during IAC meetings in early 2021. These presentations offered IAC members an overview of the proposed program, its curriculum, assessment methods, implementation timeline, and progress updates.

The Office of Financial Aid (OFA) coordinates all financial assistance offered to South Carolina State University (SCSU) students and is charged with the responsibility of assuring that federal, state, and institutional policies are operationally effective. The university's philosophy is to offer access and choice to students who would otherwise be unable to attend SCSU without financial support. The graduate assistantship program provides full-time, degree-seeking graduate students with opportunities for academic growth and development. It aims to offer financial assistance to qualified students, facilitating their pursuit of academic goals.

Background

With the advancement in information and communication technologies, cyberspace has become an indispensable part of today's society. There has been a significant growth in the online activities of individual users, government, and industry. The abundance of data and resources on cyberspace makes it a lucrative battlefield for hackers to carry out malicious acts such as phishing, identity thefts, denial-of-service, and ransomware. More importantly, complex, and sophisticated cyber-attacks such as advanced persistent threats pose serious risks to critical infrastructures such as energy, transportation, financial services, agriculture, healthcare, and public health.

Data breaches have been on the rise for several years, and sadly, this trend isn't slowing down. Data breaches have affected companies and organizations of all shapes, sizes, and sectors such as Apple, Meta, Twitter, T-Mobile, Colonial Pipeline, and they are costing US businesses millions in damages (https://tech.co/news/data-breaches-updated-list), According to Cybersecurity Ventures, the global annual cost of cybercrime is predicted to reach $9.5 trillion USD in 2024. Compounding this is the rising cost of damages resulting from cybercrime, which is expected to reach $10.5 trillion by 2025 (https://www.esentire.com/resources/library/2023-official-cybercrime-report). As a result, cybersecurity is extremely important to safeguard data, systems, and networks and protect the critical infrastructure against malicious attacks and intrusions.

Centrality to Institutional Mission

The proposed program will support the mission of SCSU in preparing highly skilled, competent, and socially aware graduates to enable them to work and live productively in a dynamic, and global society. Through diverse and robust coursework focusing on advanced Cybersecurity skills such as penetration testing, digital forensics, malware analysis as well as knowledge and skills on cutting-edge technologies such as data analytics and IoT/cyber-physical systems, the program will enable students to excel in a competitive environment.

Relation to Strategic Plan

The proposed MS in Cybersecurity program aligns with the SCSU's strategic plan by promoting the goal "Increase the number of offered student internships and placement in jobs, graduate, and professional schools". With ever-increasing cyber-crimes, industry and public sector now have huge requirements for Cybersecurity professionals. However, there is a significant void as there is not enough talent to meet the demand. Our program aims to create a talent pool that will attract employers in different sectors. Moreover,

this program will serve as a steppingstone to pursue a Cybersecurity career and prepare students for advanced degrees in Cybersecurity.

The proposed program also fits with the goal "Realign academic programs to workforce demands and include experiential learning" of SCSU's strategic initiative on *transforming the curriculum and research programs*. The proposed program has been designed to impart unique and critical skills necessary for the future Cybersecurity workforce. Furthermore, the program focusses on experiential learning through hands-on training using state-of-the-art physical and virtual Cybersecurity laboratories.

We will use VPNs to connect the physical cybersecurity laboratory equipment, and the VPNs will be accessed using university network. The course instructors will setup weekly experiments for the students, and the students will be able to complete the experiments remotely. Also, we plan to provide monthly in-person sessions to facilitate the hands-on laboratory training.

Assessment of Need

Provide an assessment of the need for the program for the institution, the state, the region, and beyond, if applicable.

According to Cyberseek.org (https://www.cyberseek.org/heatmap.html), there are currently 448,083 cybersecurity job openings with 1,098,481 total number of cybersecurity openings nationally. In South Carolina, the current cybersecurity workforce is 5,351 and the number of job openings is 12,432. Therefore, there is a need to design a graduate curriculum that offers courses tailored to address the national security issues and the requirements of the employers in the cybersecurity field in South Carolina and all over the nation. The proposed graduate program can be pursued by working individuals as it is offered 100% online.

Additionally, the IAC committee members were very supportive of the MS in Cybersecurity proposal with at least two members expressing their desire to hire a few graduates from the program. Also, we have received inquiries from at least 15 continuing students and graduates about the start date of the program.

Transfer and Articulation

Identify any special articulation agreements for the proposed program. Provide the articulation agreement or Memorandum of Agreement/Understanding.

Currently, there are no special articulation agreements for this program.

Employment Opportunities

Occupation	State		National		Data Type and Source
	Expected Number of Jobs	Employment Projection	Expected Number of Jobs	Employment Projection	
Information Security Analyst	1,590 (2020)	2,200 (2030)	168,900 (2022)	32% growth 222,200 (2030)	O*NET online
Security Management Specialist	5,410 (2020)	4% 5,640 (2030)	1,174,800 (2022)	4% 1,223,600	O*NET online
Computer Network Support Specialist	1,590 (2020)	15% 1,830 (2030)	177,900 (2022)	7% 190,400 (2032)	O*NET online
Digital Forensics Analyst	2,540 (2020)	15% 2,910 (2030)	449,400 (2022)	10% 493,100 (2032)	O*NET online
Security Architect/Managers	5,260 (2020)	13% 5,920 (2030)	127,000 (2022)	5% 132,800 (2032)	O*NET online

Supporting Evidence of Anticipated Employment Opportunities

Provide supporting evidence of anticipated employment opportunities for graduates.

South Carolina is home to major corporations such as Savannah River Nuclear Solutions, Michelin, Boeing, Flour Corporation, EATON, BMW, Volvo, and others. According to cyberseek.org, currently there are 3000+ job openings in South Carolina (Columbia, Charleston, Greenville, and Myrtle Beach), yet state institutions do not produce enough graduates in cybersecurity, both in undergraduate and graduate level, to meet the current and projected demand for the growing cybersecurity and related occupations. According to Franklin University (https://www.franklin.edu/colleges-near/south-carolina/cybersecurity-degrees), Degree completions in cybersecurity at institutions in South Carolina have been growing over the past 5 years. In 2022, students completed 115 cybersecurity-related degree programs that were offered

by South Carolina colleges and universities. That was an increase of 721% from completions reported in 2018 (8 degrees).

The number of cybersecurity degrees awarded has also increased at the national level. We compiled the number of undergraduate and graduate degrees awarded in cybersecurity by postsecondary institutions in the US from the academic year 2017-2018 through 2021-2022. We obtained the data using the Integrated Post Secondary Education Data System available at the National Center for Education Statistics (https://nces.ed.gov/ipeds). As shown in the table below, the number of undergraduate cybersecurity degrees awarded nearly doubled from 2018 to 2022. The number of graduate (Master's and Doctoral) degrees increased by 36% from 2018 to 2022.

Cybersecurity Degrees Awarded

Academic Year	Undergraduate	Graduate (Master's and Doctoral)
2021-2022	8297	7767
2020-2021	7235	6554
2019-2020	6388	6905
2018-2019	5383	6049
2017-2018	4268	5718

Note: The data in the above table represent the total degrees for four field of study: 1) Computer and information systems security/auditing/information assurance, 2) Cyber/computer forensics and counterterrorism, 3) Cybersecurity defense strategy/policy, and 4) Cyber/electronic operations and warfare.

Since South Carolina State University is well-connected with alumni leaders in these areas, we will engage our alumni network for recruitment, retention, and job placement. This will help us for producing a competent workforce and leaders to meet the needs of the labor market in the Southeastern region.

Description of the Program

Projected Enrollment			
Year	Fall Headcount	Spring Headcount	Summer Headcount
2025-2026	5	5	
2026-2027	7	7	
2027-2028	9	9	

2028-2029	11	11	
2029-2030	13	13	

Explain how the enrollment projections were calculated.

This estimate is based on the importance of the topic, and personal observations/communications with our Industrial Advisory Council Members such as SRNL, Boeing, Eaton using a Google search, and enquiries from our undergraduate students.

Besides the general institutional admission requirements, are there any separate or additional admission requirements for the proposed program? If yes, explain.

☐ Yes
☒ No

Curriculum

Program Description

The Master of Science in Cybersecurity requires completion of thirty-six (36) credit hours that include 18 credits of core courses, 9 credits of concentration (track) courses, and 9 credits of cybersecurity capstone.

New Courses

List and provide course descriptions for new courses:

Core Courses (18 credit hours)

The core has six courses (18 credit hours) that introduce students to the fundamental concepts of cybersecurity, networking, legal and ethical issues in computing, digital forensics, cyber-physical systems, and data analytics. The core courses are listed below.

CSY 501: Cybersecurity Principles (3 credit hours)
CSY 502: Networking Essentials: (3 credit hours)
CSY 503: Legal and Ethical Issues in Computing (3 credit hours)
CSY 504: Digital Forensic Investigation and Analysis: (3 credit hours)
CSY 505: Introduction to Cyber-Physical Systems: (3 credit hours)
CSY 506: Introduction to Data Analytics: (3 credit hours)

Concentration (Track) (9 credit hours)

The MS program allows candidates to specialize in any of the three areas of concentration (tracks): 1) Network Defense, 2) Digital Forensics, and 3) Cyber-Physical Systems (CPS) Security. Each area of concentration (track) consists of four courses (3 credit hours, each). Students will need to complete any three of the four courses to satisfy the concentration (track) requirement.

1) Network Defense:

This area of concentration focusses on network security threats, defense mechanisms, security issues in emerging areas including cloud computing and blockchain, application of data analytic techniques to analyze and detect network threats, and ethical hacking techniques to discover vulnerabilities in networks and hosts. The list of courses and course descriptions for "Network Defense" concentration are provided below.

Courses:

- CSY 507: Network Security (3 credit hours)
- CSY 508: Cloud Security (3 credit hours)
- CSY 509: Data Analytics for Network Threat Monitoring (3 credit hours)
- CSY 510: Ethical Hacking (3 credit hours)

Course Description:

CSY 507: Network Security: This course introduces students to network security threats and defense mechanisms. It covers common network attacks, TCP/IP, cryptography fundamentals, design of firewalls, intrusion detection and prevention systems, and virtual private networks. Security solutions for wireless networks and mobile devices are also discussed. The course includes hands-on laboratory exercises. (3 credit hours). Pre-requisite: CSY 502 or Consent of Instructor.

CSY 508: Cloud Security: This course introduces students to the high-level concepts of cloud computing, cloud infrastructure, and cloud security design principles. It covers security design patterns, data and infrastructure security, identity management, policies, compliance, and risks. It also covers the cloud security guidelines set forth by cloud security Alliance (CSA), NIST, ENISA and ISO. This course includes hands-on laboratory exercises on a commercial cloud service provider. (3 credit hours). Pre- requisite: CSY 502 or Consent of Instructor.

CSY 509: Data Analytics for Network Threat Monitoring: This course introduces students to the data analysis techniques and tools for monitoring network threats. Topics include sensors that collect network

traffic data, Intrusion detection systems (IDS), mechanisms for storing network data such as traditional databases, big data systems such as Hadoop, and tools for analyzing NetFlow data. Students will also learn about Exploratory Data Analysis (EDA), tracking the identity of hosts from network traffic, modelling networks as graphs, network mapping, and analysis of insider threats. The course includes hands-on laboratory exercises. (3 credit hours). Pre-requisite: CSY 502 or Consent of Instructor

CSY 510: Ethical Hacking: This course provides an overview of penetration testing methodologies and tools used by ethical hackers. Topics include foot printing, social engineering, scanning, enumeration, hacking web servers and hacking wireless networks. Students will also learn how to discover vulnerabilities and apply countermeasures to protect networks and information systems. The course includes hands-on laboratory exercises. (3 credit hours). Pre-requisite: CSY 502 or Consent of Instructor.

2) Digital Forensics:

This area of concentration focusses on the forensic methods and tools used to investigate different operating systems, network-based intrusions, cyber-crimes, copy-right infringements, mobile devices and malware. The list of courses and course descriptions for "Digital Forensics" concentration are provided below.

Courses:

- CSY 511: Operating System Forensics (3 credit hours)
- CSY 512: Network Forensics (3 credit hours)
- CSY 513: Mobile Forensics (3 credit hours)
- CSY 514: Malware Analysis (3 credit hours)

Course Description:

CSY 511: Operating System Forensics: This course provides a basic understanding of file systems, digital media devices, and the boot processes of different operating systems including Windows, Linux and Mac OS. It introduces students to the forensic methods used for investigating Windows and Linux systems. Topics include memory analysis, log analysis, registry analysis, Linux forensics, and application password crackers. The course includes hands-on laboratory exercises. (3 credit hours). Pre-requisite: CSY 504 or Consent of Instructor.

CSY 512: Network Forensics: This course introduces students to the forensic methods and tools for network-based investigation. Students will learn to investigate network traffic, web attacks, router attacks, Denial-of-Service (DoS) attacks, internet crimes, e-mail crimes, trademark, and copyright infringements. The

course includes hands-on laboratory exercises. (3 credit hours). Pre-requisite: CSY 504 or Consent of Instructor

CSY 513: Mobile Forensics: This course introduces students to the forensic methods and tools for retrieving and analyzing data stored on mobile devices. Students will learn about the mobile forensic techniques for various platforms such as iOS and Android. Students will also learn how to document the evidence and prepare reports in mobile forensic investigations. The course includes hands-on laboratory exercises. (3 credit hours). Pre-requisite: CSY 504 or Consent of Instructor

CSY 514: Malware Analysis: This course introduces students to the tools and techniques needed to analyze malware threats. Topics include static analysis, dynamic analysis, debugging, code injection, hooking, and malware obfuscation techniques. Students will also learn how to detect malware and identify forensic artifacts using memory forensic techniques. The course includes hands-on laboratory exercises. (3 credit hours). Pre-requisite: CSY 504 or Consent of Instructor

3) Cyber-Physical Systems (CPS) Security:

This area of concentration focusses on security and privacy issues in CPS, security strategies and standards for industrial control system (ICS), methods for designing secure IoT systems, and application of data analytic techniques for security and efficiency of CPS. The list of courses and course descriptions for "CPS Security" concentration are provided below.

Courses:

- CSY 515: Security and Privacy of CPS (3 credit hours)
- CSY 516: Secure IoT Design (3 credit hours)
- CSY 517: Data Analytics for CPS (3 credit hours)
- CSY 518: Industrial Control Systems Security (3 credit hours)

Course Description:

CSY 515: Security and Privacy of CPS: This course provides students with an overview of security and privacy issues in cyber physical systems (CPS). Topics include privacy models, key management, and access control. Emerging threats and countermeasures for CPS domains including smart cities, energy, and healthcare are also discussed. (3 credit hours). Pre-requisite: CSY 505 or Consent of Instructor

CSY 516: Secure IoT Design: This course provides students with an overview of the process to design secure IoT systems. Topics include IoT security life cycle, cryptographic applications for IoT, identity and access

management, security controls for cloud environment, IoT privacy, and IoT compliance. Students will also learn how to plan and execute incident responses for IoT. The course includes hands-on laboratory exercises. (3 credit hours). Pre-requisite: CSY 505 or Consent of Instructor.

CSY 517: Data Analytics for CPS: This course introduces students to sensor signal processing, IoT gateways, optimization and decision-making, intelligent mobility, and implementation of machine learning algorithms in embedded systems. Students will also learn how to use big data techniques to process data and improve scalability, security, and efficiency of cyber physical systems. The course includes hands-on laboratory exercises. (3 credit hours). Pre-requisite: CSY 505 or Consent of Instructor.

CSY 518: Industrial Control Systems Security: This course provides students with an overview of cyber security strategies for industrial control systems (ICS). Topics include ICS operations, network architectures, protocols, applications, industrial cyber threats, security controls for industrial networks, vulnerability assessment, anomaly detection, standards, and regulations for ICS security. The course includes hands-on laboratory exercises. (3 credit hours). Pre-requisite: CSY 505 or Consent of Instructor

Cybersecurity Capstone (9 credit hours)

Students fulfill the capstone requirement by completing three courses: Cybersecurity Thesis-I (3 credit hours), Cybersecurity Thesis-II (3 credit hours) and Special topics in cybersecurity (3 credit hours). The MS in Cybersecurity program also offers a non-thesis option where students can complete two courses from any area(s) of concentration other than the area chosen by them to satisfy the thesis requirements. Students in non-thesis option will still need to complete the course "Special topics in cybersecurity".

Admission Requirements

Applicants seeking admission into the MS degree in Cybersecurity must have a bachelor's degree in STEM or related fields with undergraduate preparation in cybersecurity. Students with bachelor's degrees without undergraduate preparation in cybersecurity will be required to complete an introductory undergraduate cybersecurity course before starting the coursework of the MS degree curriculum. In addition to these requirements, the applicant must satisfy other graduate school requirements(https://scsu.edu/admissions/graduate-admissions.php).

Course Description (Core Courses and Capstone Courses)
Master of Science Degree in Cybersecurity

CSY 501: Cybersecurity Principles: This course introduces students to the fundamental concepts in cybersecurity. Topics include security design principles, access control, cryptography, network security, malicious software, operating system security, and IT security management. Advanced topics such as cloud and IoT security are also covered. The course includes hands-on laboratory exercises. (3 credit hours). Prerequisite: Admission to Graduate Program

CSY 502: Networking Essentials: This course introduces students to the basics of computer networks as well as advanced concepts in Ethernet and TCP/IP networks. Topics include routing protocols, router configuration, local, campus, and wide area network configuration, network security, wireless networking, optical networks, Voice over IP, the network server, and Linux networking. It also covers switch security, troubleshooting IP networks, authorization and access control, best practices for disaster recovery, network infrastructure configuration and management, and data traffic network analysis. The course includes hands-on laboratory exercises. (3 credit hours). Corequisite: CSY 501 or Consent of Instructor

CSY 503: Legal and Ethical Issues in Computing: This course provides an overview of the legal and ethical issues in computing. It covers compliance with laws concerning financial, health and children's information. Topics also include intellectual property laws, contract issues, and criminal laws in cyberspace. (3 credit hours). Corequisite: CSY 501 or Consent of Instructor

CSY 504: Digital Forensic Investigation and Analysis: This course provides an overview of the forensic procedures for investigating computers. Common computer crimes and relevant laws are discussed. It covers forensic methods for investigating incidents that involve networks, e-mails, mobile devices, cloud, and Internet of Things devices. The course includes hands-on laboratory exercises. (3 credit hours). Prerequisite: CSY 501 or Consent of Instructor

CSY 505: Introduction to Cyber-Physical Systems: This course provides students with an overview of cyber physical systems (CPS) focusing on applications and theoretical foundations. It covers CPS domains including medical and energy CPS, Wireless Sensor Networks (WSNs)/Internet-of-Things (IoT), symbolic synthesis, logical correctness, real-time scheduling, synchronization, model integration and CPS security. The course includes hands-on laboratory exercises. (3 credit hours). Pre-requisite: CSY 501 or Consent of Instructor

CSY 506: Introduction to Data Analytics: This course is an introductory course in machine learning. It covers topics in cleaning data, basics of statistics, probability & linear algebra, Hypothesis tests, regression, clustering, classification, mixture models, and neural networks. The best way to learn about a machine learning method is to program it and experiment with it. So, this course includes hands-on laboratory exercises that involve implementation of machine learning algorithms and experimentation to test the algorithms on some data. Also, students will be exposed to distributed machine learning and cloud-based machine learning. (3 credit hours). Pre-requisite: CSY 501 or Consent of Instructor

CSY 519: Cybersecurity Thesis-I: All candidates of MS degree in cybersecurity are required to complete a practical project to solve a real-world problem in a cybersecurity related topic. Students will complete their project using the knowledge and skills they acquire from the previous courses. The instructor will provide the students with necessary guidelines for the project. In this course, students will complete the design of their proposed system and submit a report outlining the problem statement, the design methodology and a plan to implement and evaluate a prototype of the proposed system. (3 credit hours). Prerequisite: CSY 501 or Consent of Instructor

CSY 520: Cybersecurity Thesis-II: This course is a continuation of CSY 519 and requires students to complete the implementation and evaluation of their prototype. Students will be required to submit a final project report and give an oral presentation on their findings in class. (3 credit hours). Pre-requisite: CSY 519 or Consent of Instructor.

CSY 521: Special Topics in Cybersecurity: This course provides an overview of the emerging topics in cybersecurity in the areas of moving target defense, blockchain, software defined networking, forensic analysis of cyber-physical systems such as connected car and Industrial control systems. (3 credit hours). Corequisite: CSY 520 or Consent of Instructor.

Total Credit Hours Required: 36

Curriculum by Year					
Course Name	Credit Hours	Course Name	Credit Hours	Course Name	Credit Hours
Year 1					
Fall		Spring		Summer	
CSY 501: Cybersecurity Principles	3	CSY 504: Digital Forensic Investigation and Analysis	3		
CSY 502: Networking Essentials	3	CSY 505: Introduction to Cyber- Physical Systems	3		
CSY 503: Legal and Ethical Issues in Computing	3	CSY 506: Introduction to Data Analytics	3		
Total Semester Hours	9	Total Semester Hours	9	Total Semester Hours	
Year 2					
Fall		Spring		Summer	
Concentration (Track)-Course #1	3	Concentration (Track)-Course #3	3		
Concentration (Track)-Course #2	3	CSY 520: Cybersecurity Thesis-II	3		
CSY 519: Cybersecurity Thesis-I	3	CSY 521: Special Topics in Cybersecurity	3		
Total Semester Hours	9	Total Semester Hours	9	Total Semester Hours	

Similar Programs in South Carolina offered by Public and Independent Institutions

Identify the similar programs offered and describe the similarities and differences for each program.

Although, at the national level there are 82 campus-based (https://cybersecurityguide.org/programs/masters-in-cybersecurity/) and 90 online Master's in Cybersecurity degree programs (https://cybersecurityguide.org/online/masters-in-cybersecurity/), there are only 8 institutions in South Carolina that offer graduate programs in Cybersecurity including Master and certificates. Moreover, both nationally and regionally, to the best of our knowledge, there is a gap in offering a cybersecurity program that covers the security of Cyber-Physical Systems, IoT systems, and security of industrial process control systems and industrial networks at depth. These courses are important as the students will gain knowledge, skills, and abilities to pursue a cybersecurity career in any critical infrastructure sector.

Program Name and Designation	Total Credit Hours	Institution	Similarities	Differences
MS in Applied Computing Cybersecurity Track	42	Clemson University	Both programs cover concepts of network security, malware analysis, and cybersecurity principles.	The program from Clemson offers a cybersecurity track with 5 courses in cybersecurity. In contrast, the proposed program from South Carolina State University is a graduate program of 36 hours of cybersecurity coursework and provides in-depth coverage of diverse cybersecurity topics.
MS in Computer Engineering - Cybersecurity	30	Clemson University	Few courses in Cybersecurity.	The program from Clemson University provides graduate education in Computer Engineering, Computer Science and Electrical Engineering with an emphasis on

				Cybersecurity. In contrast, the proposed program from South Carolina State University is a graduate program in cybersecurity that incorporates (a) data analytics, machine learning from a security perspective, and (b) three areas of concentration (tracks) that allows students to pursue a specialization (Network Defense, Digital Forensics, and Cyber Physical Systems Security) and gain a deep understanding of a specific cybersecurity topic.
MA in Intelligent and Security Studies – Cybersecurity Concentration	36	Jointly offered by the Citadel and College of Charleston	Both programs are offered 100% online. Both programs cover concepts of networking.	The proposed program from South Carolina State University is a graduate program in cybersecurity that incorporates (a) data analytics, machine learning from a security perspective, and (b) three areas of concentration (tracks) that allow students to pursue a specialization (Network Defense, Digital Forensics, and Cyber-Physical Systems Security) and gain a deep

				understanding of a specific cybersecurity topic.
MS in Computer Science and Information Sciences (Cybersecurity Specialization)	33	Jointly offered by the Citadel and College of Charleston	Both programs cover concepts on the principles of cybersecurity and networking.	The proposed program from South Carolina State University is a graduate program in cybersecurity that incorporates (a) data analytics, machine learning from a security perspective, and (b) three areas of concentration (tracks) that allow students to pursue a specialization (Network Defense, Digital Forensics, and Cyber-Physical Systems Security) and gain a deep understanding of a specific cybersecurity topic.
MS in Information Systems Technology with a Concentration in Security	33	Coastal Carolina University	Both programs offer courses on digital forensics, cybersecurity fundamentals, network security, and data analytics.	The proposed MS in Cybersecurity program addresses the current workforce needs of Industry, Academics, and Government by offering three areas of concentration (tracks): that allow students to pursue a specialization (Network Defense, Digital Forensics, and Cyber Physical Systems Security).

MS in Cybersecurity	30	Anderson University	Both programs are offered 100% online. Both programs cover concepts on penetration testing, cloud security and cybersecurity of critical infrastructures.	The proposed program from SCSU offers 9 hours of cybersecurity capstone that includes thesis-I (3 hrs), thesis-II (3 hrs), and special topics in cybersecurity (3 hrs), whereas Anderson's program offers only 3 hours of capstone work chosen from a) Cybersecurity practicum (3 hrs), or b) Cybersecurity research.
MS in Cybersecurity	35	Claflin University	Both programs are offered 100% online. Both programs offer Ethical Hacking, Network Security, and Digital Forensics courses.	The proposed MS in Cybersecurity program addresses the current workforce needs of Industry, Academics, and Government by offering three areas of concentration (tracks): that allow students to pursue a specialization (Network Defense, Digital Forensics, and Cyber Physical Systems Security).
MA in Cybersecurity	30	Columbia International University (CIU)	Both programs offer courses on network security, digital forensics, ethical hacking, and laws and ethics in cybersecurity.	SCSU's program offers a holistic curriculum consisting of core (18 credit hours), concentration (track) (9 credit hours) and capstone (9 credit hours) courses. Moreover, SCSU's program allows students to specialize in one of the three areas of

				concentration (tracks): Network Defense, Digital Forensics, and Cyber Physical Systems Security.
Master of Science in Computer and Information Science (MSCI)-Cyber Security Track	30	University of South Carolina, Aiken	Both programs offer courses on networking, network security, computer forensics, Artificial Intelligence (AI), and Machine Learning (ML).	SCSU's program allows students to pursue a specialization in one of the three areas: Network Defense, Digital Forensics, and Cyber-Physical Systems Security.

Faculty

Rank and Full- or Part-time	Courses Taught for the Program	Academic Degrees and Coursework Relevant to Courses Taught, Including Institution and Major	Other Qualifications and Relevant Professional Experience (e.g., licensures, certifications, years in industry, etc.)
Professor, Department Chair	CSY 503, CSY 505	PhD – Electrical Engineering	Existing faculty teaching courses in Computer Science and Cybersecurity that are currently offered. IBM Instructor certificates in Data Science, Cloud Computing, AI, Machine Learning, Enterprise Design Thinking. Registered Professional Engineering in SC, ETAC of ABET Evaluator for Computer Engineering Technology, Electrical Engineering Technology, and Software Engineering. Involved in several individual funded grant proposals on Cybersecurity, AI, and Data Science.
Associate Professor	CSY 501, CSY 504	PhD- Computer Science and Information Engineering	Existing faculty teaching courses in Cybersecurity that are currently offered. IBM Instructor certificates in Data Science, Cloud Computing, AI, Machine Learning, Enterprise Design Thinking. Security+ Certification. Involved in several individual funded grant proposals on Cybersecurity, AI, and Data Science.
Associate Professor	CSY 502, CSY 506	PhD – Computer Information and Systems Engineering	Existing faculty teaching courses in Computer Science and Cybersecurity that are currently offered. IBM Instructor certificates in Cybersecurity, Data Science, Cloud Computing, AI, Machine Learning, Enterprise Design Thinking. Involved in several individual funded

			grant proposals on Cybersecurity, AI, and Data Science.
Instructor (Hired during Summer 2024)	**Concentration (Track) #1 Course 3, Concentration (Track) #2 Course 3**	MS – Machine Learning	Existing faculty teaching courses in Cybersecurity, Machine Learning, AI. Google Certificates in Machine Learning, AI.
Adjunct	**Concentration (Track) #3 Course 3, Special Topics**	MS – Computer Engineering	Existing faculty/System Administrator teaching courses in Computer Science/Cybersecurity. IBM and Google Certificates in Cybersecurity, Machine Learning, and AI
Assistant Professor – NEW	Concentration (Track) #1, Course 1, Course 2	PhD – Computer Science or related fields.	To teach Computer Science/Cybersecurity courses.
Assistant Professor – NEW	Concentration (Track) #2, Course 1, Course 2, Thesis I	PhD – Computer Science or related fields.	To teach Computer Science/Cybersecurity courses.
Assistant Professor – NEW	Concentration (Track) #3, Course 1, Course 2 Thesis II	PhD – Computer Science or related fields.	To teach Cybersecurity courses.

Core courses noted in bold.

Total FTE needed to support the proposed program:
Faculty: 9
Staff: 2
Administration: 1

Faculty, Staff, and Administrative Personnel

Discuss the Faculty, Staff, and Administrative Personnel needs of the program.

The program will be using the services of four existing faculty and one adjunct faculty who are currently teaching courses in our undergraduate computer science and cybersecurity programs. The program will hire 4 additional faculty by Fall 2025 in tenure track positions. These new hires will be devoting 25% of their time for teaching courses (2 courses for academic year), and 75% of their time for research activities.

Occasionally, classes may be taught by adjunct faculty who meet the requirements to teach graduate classes. The program currently uses the services of 1 Administrative Personnel, and 2 Staff (1 Systems Manager and 1 Laboratory Administrator/Technician). The program plans to use the services of these personnel for this proposed degree program.

Resources

Library and Learning Resources

Explain how current library/learning collections, databases, resources, and services specific to the discipline, including those provided by PASCAL, can support the proposed program. Identify additional library resources needed.

The Miller F. Whittaker Library's primary mission is to provide the resources, services, and an environment, which supports the teaching and research programs of the University. It is designed to accommodate the research and academic resource needs for both on-site and off-site students. The library's holdings for engineering and computing are as follows:

- Cybersecurity: E-books (3,057); printed books (2,265)
- Electrical Engineering: E-books (5,346); printed books (10,077)
- Computer Engineering: E-books (2,599); printed books (109)
- Mechanical Engineering: E-books (5,198); printed books (7,704)
- General Engineering: E-Books (393); printed books (3001)
- Computing: E-books (25,187); printed books (1,501)

Materials not owned by the library can be accessed through three interlibrary borrowing services 1) OCLC – An international borrowing service comprised of the United States and other participating countries, 2) PASCAL Delivers – A statewide service borrowing service comprised of 57 South Carolina libraries; and CHEC – A local or community borrowing service comprised of Claflin University, Orangeburg-Calhoun Technical College, and SC State University.

Library resources are available online through the main campus. Through the above and related consortia participation and purchases, the Miller F. Whittaker Library's website provides access to 114 online subscription databases and three (3) e-book collections to support academic research and study. These aggregate sources provide users access to over 781,490 e-books, 90,290 e-journals, and 3,901 e-newspapers on campus as well as off-campus through proxy authentication. These online resources are accessible to students currently enrolled at SC State University on-campus or at remote sites.

Students and faculty are instructed to use the online resources through various instructional resources. The library provides instructional flyers and related handouts on citing references, how to submit interlibrary loan requests, etc. Through BlackBoard, the university's learning management system, the library provides access to an interactive orientation video and related video tutorials on a variety of topics, including information literacy. Additionally, students and faculty have access to the vendor created video tutorials on the use of several of their databases.

Student Support Services

Explain how current academic support services will support the proposed program. Identify new services needed and provide any estimated costs associated with these services.

The Division of Student Affairs' mission is to create a community of learning that facilitates growth and discovery while fostering students' holistic development. This is accomplished by offering quality programs, activities and resources that enrich the overall student experience and promote civic and global responsibility through leadership and service. The following divisions are under the Division of Student Affairs:

- Campus Life
- Student Life & Leadership
- Housing & Residence Life
- Brooks Health Center
- Counseling & Self-Development Center
- Career Center
- Intramural Sports
- Cheerleaders

Details about these divisions can be found at https://scsu.oudeve.com/sc_state_about/leadership/student-affairs/index.php

Physical Resources/Facilities

Identify the physical facilities needed to support the program and the institution's plan for meeting the requirements.

The proposed program will use the existing Computing and Cybersecurity laboratory facilities in Computer Science and Mathematics Department. No new instructional equipment is needed for this proposed program.

Laboratory modules are used for teaching, research and outreach, and the design of laboratory modules reflect these uses. We use two different laboratory settings for our Cybersecurity courses – virtual and physical. *The virtual laboratory is from the NDG NetLAB+* (*https://www.netdevgroup.com/content/Cybersecurity*). This platform provides our students with laboratory experiences on number of Cybersecurity and Computer Science topics in an online environment. Our students conduct experiments in *NDG Forensics, NDG Ethical Hacking, and NISGTC Linux+.* This laboratory is also used by our academic partners at a distance.

The physical laboratory is designed with laboratory units/workstations from Marcraft (https://tech-labs.com/products/marcraft-cyber-security-essentials-concepts-practices). Currently, these workstations/units are used to provide our students with hands-on laboratory experiences on *physical security*, *application security, IOT/CyberPhysical Systems (industrial control systems), enterprise security, network security, forensics, penetration testing/malware analysis, and ethical hacking*. These labs can be converted for remote access with the addition of additional equipment.
Data Sciences (Machine Learning and Deep Learning) Laboratory is designed to provide our majors with experiences in Data-Driven Security. This laboratory is equipped with two Lambda Labs GPU servers and 4 Dell units with remote access capability.

Maintenance and upgrading of the laboratory facilities

UCITS is responsible for campus-wide computing, networking, telecommunications, and information technologies. The unit includes a helpdesk that responds to users' campus wide. There are several departments and units that have their own first-line technical support. The UCITS helpdesk also supports these individuals as needed, and the support from UCITS is adequate.

Impact on Existing Programs

Will the proposed program impact existing degree programs or services at the institution (e.g., course offerings or enrollment)? If yes, explain.

☐ Yes
☒ No

We are not expecting any major impact of this program on existing program.

Financial Support

Sources of Financing for the Program by Year												
	1st		2nd		3rd		4th		5th		Grand Total	
Category	New	Total	New	Total	New	Total	New	Total	New	Total	New	Total
Tuition Funding	114,600	114,600	160,440	160,440	206,280	206,280	252,120	252,120	297,960	297,960	1,031,400	1,031,400
Program-Specific Fees	0	0	0	0	0	0	0	0	0	0	0	0
Special State Appropriation	0	0	0	0	0	0	0	0	0	0	0	0
Reallocation of Existing Funds	0	0	0	0	0	0	0	0	0	0	0	0
Federal, Grant, or Other Funding	0	0	405,000	405,000	405,000	405,000	405,000	405,000	405,000	405,000	1,620,000	1,620,000
Total	114,600	114,600	565,440	565,440	611,280	611,280	657,120	657,120	702,960	702,960	2,651,400	2,651,400
Estimated Costs Associated with Implementing the Program by Year												
	1st		2nd		3rd		4th		5th		Grand Total	
Category	New	Total	New	Total	New	Total	New	Total	New	Total	New	Total
Program Administration and Faculty/Staff Salaries	0	0	405,000	405,000	405,000	405,000	405,000	405,000	405,000	405,000	1,620,000	1,620,000
Facilities, Equipment, Supplies, and Materials	25,000	25,000	25,000	25,000	25,000	25,000	25,000	25,000	25,000	25,000	125,000	125,000
Library Resources	20,000	20,000	20,000	20,000	20,000	20,000	20,000	20,000	20,000	20,000	100,000	100,000

Other (specify)	10,000	10,000	10,000	10,000	10,000	10,000	10,000	10,000	10,000	10,000	10,000	50,000
Total	55,000	55,000	460,000	460,000	460,000	460,000	460,000	460,000	460,000	460,000	1,895,000	1,895,000
Net Total (Sources of Financing Minus Estimated Costs)	59,600	59,600	105,440	105,440	151,280	151,280	197,120	197,120	242,960	242,960	756,400	756,400

Note: New costs - costs incurred solely as a result of implementing this program. Total costs - new costs; program's share of costs of existing resources used to support the program; and any other costs redirected to the program.

Budget Justification

Provide an explanation for all costs and sources of financing identified in the Financial Support table. Include an analysis of cost-effectiveness and return on investment and address any impacts to tuition, other programs, services, facilities, and the institution overall.

1. Tuition revenue is estimated based on the enrollment projections and the per-semester tuition rate of $5,730 (11,460/year)
    - The program costs expected are the following:
2. Three (3) new Computing/Cybersecurity faculty and one (1) Adjunct faculty:
    - We have funds from Battelle Savannah River (BSRA Grant Agreement) to hire 3 faculty with expertise in Computer Science, Cybersecurity, and Data Science. We plan to complete these hires by 2026. The total budget (salary and fringe benefits) per year is $405,000.
    - One (1) Adjunct Faculty with a total budget of $10,000/year.
3. Technology Upgrade:
    - Technology upgrade labs for online delivery, Netlab NDG laboratory platform annual maintenance fee, and supplies ($25,000/yr.) from year 1.
4. Library Collections:
    - Enhancing Library Collections in Cybersecurity and ACM Digital Library Annual Fee ($20,000) per year

The program costs are $55,000 during year 1, and $450,000 during years 2, 3, 4, and 5 with a total program cost of $1,895,000. The total funds generated from tuition and grants are $2,651,000. There is a total program income of $756,400. Since the total program income is $756,400, there is no cost to sustain the program.

Evaluation and Assessment

Our Computer Science (CS) program is accredited by CAC ABET since 2002 with established Program Educational Objectives, Student Learning Outcomes, and assessment and evaluation practices and methods. Here are the definitions of terminology used by ABET. We have used these definitions in formulating the PEO, Learning Outcomes, Assessment and Evaluation plans.

Definitions

While ABET recognizes and supports the prerogative of institutions to adopt and use the terminology of their choice, it is necessary for ABET volunteers and staff to have a consistent understanding of terminology. With that purpose in mind, the Applied and Natural Science Accreditation Commission, Computing Accreditation Commission, Engineering Accreditation Commission, and Engineering Technology Accreditation Commission will use the following basic definitions:

Commissions will use the following basic definitions:

Program Educational Objectives - Program educational objectives are broad statements that describe what graduates are expected to attain within a few years after graduation. Program educational objectives are based on the needs of the program's constituencies.

Student Outcomes - Student outcomes describe what students are expected to know and be able to do by the time of graduation. These relate to the knowledge, skills, and behaviors that students acquire as they progress through the program.

Assessment - Assessment is one or more processes that identify, collect, and prepare data to evaluate the attainment of student outcomes. Effective assessment uses relevant direct, indirect, quantitative, and qualitative measures as appropriate to the outcome being measured. Appropriate sampling methods may be used as part of an assessment process.

Evaluation - Evaluation is one or more processes for interpreting the data and evidence accumulated through assessment processes. Evaluation determines the extent to which student outcomes are being attained. Evaluation results in decisions and actions regarding program improvement.

Program Educational Objectives	Program Learning Outcomes Aligned to Program Educational Objectives	Methods of Assessment
To prepare students with the technical knowledge and skills needed to protect and defend computer systems, networks, and physical systems.	Conduct a cyber security risk assessment. Measure the performance and troubleshoot cyber security systems. Be able to use cyber security,	CSY 502 – Networking Essentials, CSY 504 – Digital Forensics Investigation, CSY 505 – Introduction to Cyber-Physical Systems: 80% of the students will be required to score at 80%

	information assurance, and cyber/computer forensics software/tools.	or more in selected CSY 502, 504, 505 course assignments and assessments
To develop graduates that can plan, implement, and monitor cyber security mechanisms to help ensure the protection of information technology assets.	Design and develop a security architecture for an organization. Implement cyber security solutions. Identify the key cyber security vendors in the marketplace.	CSY 501 – Cybersecurity Principles: 80% of the students will be required to score at 80% or more in in selected CSY 501 course assignments and assessments
To develop graduates that can identify, analyze, and remediate computer security breaches.	Analyze and evaluate the cyber security needs of an organization.	CSY 519 and CSY 520 – Thesis I and II: 80% of the students will be required to score at 80% or more in reports and presentations.
To develop practitioners who incorporate ethical, legal and social implications to outcomes of their profession.	Design operational and strategic cyber security strategies and policies.	CSY 503 – Legal and Ethical Issues in Computing: 80% of the students will be required to score at 80% or more in selected CSY 503 course assignments and assessments

Other methods of assessment that will be used are the Program Specific Graduate Exit Survey, Periodic Employer and Graduate Survey on Program Educational Objectives, and Outcomes.

Explain how the proposed program, including all program objectives, will be evaluated, along with plans to track employment. Describe how assessment data will be used.

Assessment of this program will be conducted in accordance with the guidelines developed by the Continuous Improvement Committee (C.I.C.) of the College of Science, Technology, Engineering, Mathematics, and Transportation at South Carolina State University. The program objectives will be reviewed by the members of the Industrial Advisory Council of the College every two years. This body meets once every semester. Course Learning Outcomes are established for all the individual courses associated

with the program, and these outcomes will be assessed each year. Continuous Improvement at the program level will be made based on the assessments of student learning outcomes at the course level and evaluation of the program outcomes at the program level. The assessments will be reviewed each year, and decisions about program improvement will be made annually based on those results. The continuous improvement process will also consider input from the C.I.C. The program will also undergo a standard program review every six years, as do all other ABET-accredited degree programs of the College. An additional assessment of the program success would be provided via a survey of the employed graduates.

The employment of graduates will be tracked using the following:

1. Program Specific Graduate Exit Survey
2. Periodic Employer and Graduate Survey on Program Educational Objectives, and Outcomes.
3. Records from the Career Service Center and Office of Alumni Relations
4. Locating alumni via social media

The data collected from these instruments will be used to review of Program Educational Objectives and Outcomes, and Program Curriculum as needed.

Accreditation and Licensure/Certification

Will the institution seek program-specific accreditation (e.g., CAEP, ABET, NASM, etc.)? If yes, describe the institution's plans to seek accreditation, including the expected timeline.

☒ Yes
☐ No

The program will seek CAC ABET accreditation after it produces at least one graduate from the program which is expected to be after 2 years of offering the program around 2027. Also, NSA-DHS has designated South Carolina State University as a National Center of Academic Excellence in Cyber Defense Education through academic year 2024 for the Bachelor of Science in Computer Science with Cybersecurity, and NSA has validated our Bachelor of Science in Computer Science with Cybersecurity Program of Study (PoS) through 2029. We will seek the CAE-R designation for our MS in Cybersecurity program around 2027.

Will the proposed program lead to licensure or certification? If yes, identify the licensure or certification.

☐ Yes
☒ No

Explain how the program will prepare students for this licensure or certification.

If the program is an Educator Preparation Program, does the proposed certification area require national recognition from a Specialized Professional Association (SPA)? If yes, describe the institution's plans to seek national recognition, including the expected timeline.

☐ Yes
☒ No