NEW PROGRAM PROPOSAL FORM

Name of Institution: University of South Carolina Columbia

Name of Program (include degree designation and all concentrations, options, or tracks): Master of Science in Information Security and Cyber Leadership

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 2023

CIP Code: 11.0401 Information Science/Studies

Delivery Site(s): 85750

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):
Kim M. Thompson, Associate Dean for Academic Affairs, 803-777-0224, kthompso@mailbox.sc.edu
Trena Houp, Director of Academic Programs and eLearning, 803-777-0460 or thoup@sc.edu

Institutional Approvals and Dates of Approval (include department through Provost/Chief Academic Officer, President, and Board of Trustees approval):
Provost Pre-authorization: 7/18/2022
College of Information and Communications: 8/29/2022
Graduate Council Committee on Science, Math and Related Professional Programs: 12/09/2022
Graduate Council: 12/12/2022
Provost: 1/25/2023
Board of Trustees Academic Excellence and Student Experience Committee: 2/24/2023
Board of Trustees: 2/24/2023

Background Information

The iSchool at the CIC proposes a fully online Master's in Information Security and Cyber leadership (MISCL). This new graduate degree program marries information science (with a focus on the theory, organization, and process of information) with cybersecurity (with a focus on assessment of security needs, recommending safeguard solutions, and auditing security devices, systems, and procedures) and leadership. Schools of Information across the United States are creating cyber certificates and graduate programs (e.g., UC Berkeley School of Information: Master of Information and Cybersecurity; UT Austin School of Information: Master of Science in Information Security and Privacy; University of North Texas College of Information, PhD Information Science with Cybersecurity Concentration) to meet the cybersecurity needs of our country. In the State of South Carolina, Governor McMaster has advocated for increasing cyber protections across state industries, creating a need for a workforce with the skills and knowledge that can meet the needs of the State. This proposed program supports the University of South Carolina (USC) strategic plan, which notes agility to serving the university and commitment to serving our students, community, and State with new academic and career opportunities. This program will be a pathway for individuals who wish to develop a specialization in the subject areas related to information security, cyber environments, communication, data management, information science and technology, and leadership.

Assessment of Need

Information security and leadership are at the heart of cyber environment operations. Cybercrimes are prevalent nationwide and have steadily worsened in recent years. Cybersecurity challenges have plagued the State of South Carolina; an example is over 20,000 fraudulent accounts created on the unemployment portal in 2021. Currently, in South Carolina, the cybersecurity industry has a $1.42 billion statewide impact annually (0.32% of GDP). Federal government agencies, including the Department of Defense, have been providing financial assistance or grants for cyber training programs for the State. Therefore, a critical task is to create an effective cybersecurity workforce for the State to meet the demand and fight against cybersecurity issues

Cyber security has become a national imperative in our country, and there is a critical need for cyber professionals in our state and beyond. In their 2017 report, the Cybersecurity professional organization (ISC)2 predicted a 1.8 million workforce deficit in the cybersecurity workforce in 2022. (https://www.isc2.org/News-and-Events/Press-Room/Posts/2017/06/07/2017-06-07Workforce-Shortage) This includes not only the tech-heavy programming positions, but also employment of managers, non-technical cyber-related work, and executive roles. According to the Bureau of Labor Statistics, employers will be hiring more cybersecurity professionals between now and 2029, or 31% more jobs than other industries combined. There is a much higher demand for cybersecurity skills than there are available employees with those skills. In fact, a 2020 study showed that by 2024 there would be three million cybersecurity jobs unfilled as opposed to 1 million in 2014. The Bureau of Labor Statistics states that the industry unemployment rate has stayed close to zero for over a decade, and someone with less than five years of experience in cybersecurity can earn around $100,000 a year.

Transfer and Articulation

No articulation agreement needed for this program, , however, USC Columbia allows up to 12 credit hours of graduate credit to be transferred into a master's program that requires 30-36 hours. We will also advertise the program to students who possess a bachelor's degree as well as engage in discussions with our transfer partnership about appropriate pathways to this graduate degree program. Transfer information for students interested in pursuing a bachelor's degree in preparation for this master's program is available at

https://sc.edu/about/offices_and_divisions/undergraduate_admissions/requirements/for_transfers/ with specific information targeted to the students enrolled in a South Carolina technical College institution available at https://sc.edu/about/offices_and_divisions/undergraduate_admissions/requirements/for_transfers/credits_from_sc_technical_colleges/.

Employment Opportunities

Occupation	State		Regional		Data Type and Source
	Expected Number of Jobs	Employment Projection	Expected Number of Jobs	Employment Projection	
Cyber Security Administration (in Columbia and Charleston, SC)	3,887				Kennedy & Company, 2022[1]
Information Security Analysts	1,325 (2018 statistics); 1,800 (2021 statistics)	1747* (projected for 2028)	19,500	35% from 2021-2031	South Carolina Department of Employment and Workforce; ONet and BLS Occupational Outlook Handbook
Cyber Security Administration (in Atlanta and Alpharetta, GA)			25, 272		Kennedy Report
Cyber Security Administration (in Charlotte, Raleigh, Durham, Cary, Greensboro, and Morrisville, NC)			16,725		Kennedy Report

* This is an 18% increase in jobs with 10% annual churn, but South Carolina has already blown through some of these projections.[2]

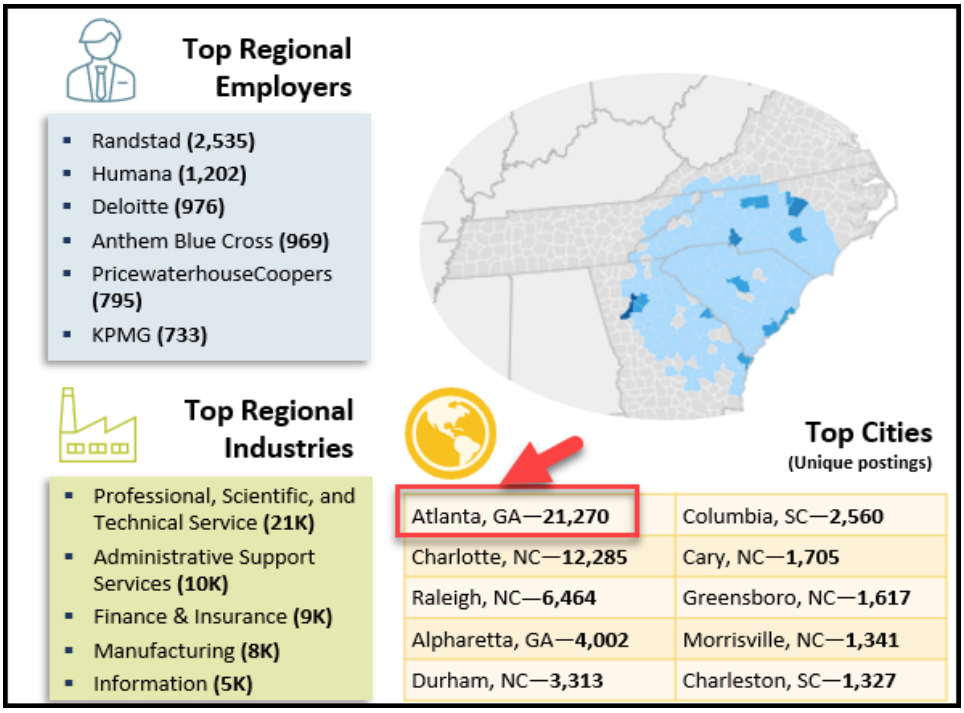
Supporting Evidence of Anticipated Employment Opportunities

The iSchool serves students in the State, the region, nationally, and internationally. Many alumni have become leaders in the state and southeastern region business, information, and technology-related

[1] Kennedy & Company is an education strategies consulting firm we commissioned explore the feasibility of creating new cyber content in the CIC. They reported marked and labor research, competitor analysis, and recommendations. The graphs and images included in this proposal are from this report.

[2] Ellzey, D. (2022, May 24). South Carolina Department of Employment and Workforce: A presentation at the South Carolina Cybersecurity Summit [PowerPoint Slides].

communities. Using the Emsi system to examine the labor market information between May 2021 and April 2022[3], a quarter of all jobs requiring a background in cyber operations were based in Atlanta. This was followed by Charlotte, where many bank headquarters are located, and the cities in the research triangle in North Carolina. The majority of regional jobs are in the scientific or technical service industry, but many of the top employers are "Big Four" accounting firms.



Because the iSchool is well-connected with alumni leaders in these areas, we will engage our alumni network to recruit student candidates. The iSchool needs to take responsibility for producing a competent workforce and leaders to meet the needs of the labor market in the Southeastern region.

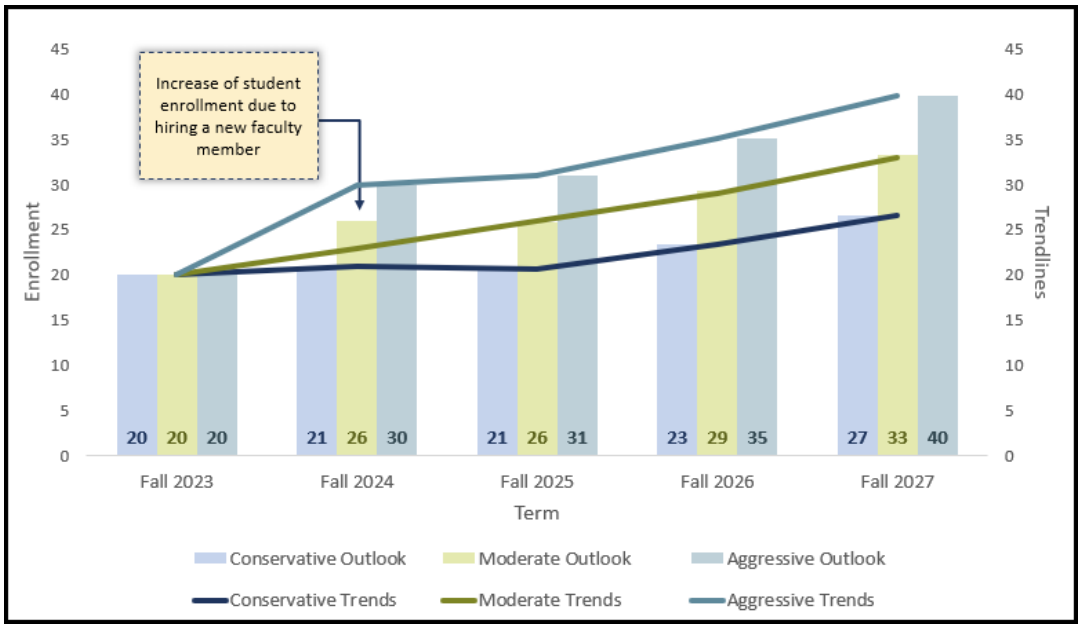
Description of the Program

Projected Enrollment			
Year	Fall Headcount	Spring Headcount	Summer Headcount
2023-2024	20	20	20
2024-2025	26	26	26
2025-2026	26	26	26
2026-2027	29	29	29
2027-2028	33	33	33

The headcounts provided above are a modest estimate of the projected enrollment. By using the iSchool's graduate-level graduation information from 2021 as the baseline data, we forecast growth rates of enrollments by county, region, and nation to calculate the estimated projected program enrollment. A linear regression analysis is calculated to make both conservative and aggressive

[3] Emsi: https://www.economicmodeling.com/

scenarios. We apply a 20% decrease in a conservative scenario and a 20% increase in an aggressive scenario for our estimations. According to the growth of the population and the potential degree recipients, the iSchool could expect approximately between 27 and 40 students in the non-technical cyber degree program by the Fall of 2027. The following shows the results of our calculations:



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

☐Yes

☒No

Curriculum

New Courses

The students enrolled in the MISCL program are required to complete 30 hours of coursework, including 12 hours of required courses. They tailor the remainder of their classes (18 hours) toward their career and research interests with the help of professional advisors of the program.

Since the content for the proposed program is closely related to the information science instruction we already do at the undergraduate and graduate level in the iSchool, the curriculum uses courses that are already approved in the iSchool curriculum.

The new courses noted here will be proposed as permanent courses in the 2023 academic year for Fall 2024. Four new courses will be created related to this program of study:

New required courses:

- ISCI 785 - Information Security, Ethics, and Leadership in Cyber Environments (3 Credits) Critical and analytical study of cyber-related leadership, information security, and information policy and ethical issues at the individual, institutional, and international levels.
- ISCI 786 - Cyber Security and Information Science (3 Credits) Provides students with essential skills and training in information and cyber security leading to the option to complete the CCSA certification process through Check Point Software Technologies.

New elective courses:

- ISCI 708 - Information and Communication Needs and Assessment (3 Credits) Communication models, major concepts, trends, and other related issues of information need and assessment with a focus on information seeking and use in digital age.
- ISCI 779 - Social Informatics (3 Credits) Design, uses, and effects of information and communication technologies from the standpoint that society and technology mutually shape one another.

And the title for ISCI 768 is in process of being changed from "Problems in Library and Information Agency Administration" to "Challenges in Information-Intensive Organization Administration"

Summary of Degree Requirements

Students in this program must complete 30 hours of coursework: 12 credits of required courses + 18 credits of electives. The electives can be taken to align with three areas of specialization: Intellectual Capital Management and Communication, Human Information Behavior, and Data Communication and Management.

Required (Core) Courses: 12 hours (substitutions must be specifically approved by the student's advisor and graduate director within their "home" program)

Course	Title	Credits
ISCI 785	Information Security, Ethics, and Leadership in Cyber Environments **[New]** (Currently offered as ISCI 795 Special Topics in International Information Issues: Information Security, Ethics, and Leadership in Cyber Environments)	3
ISCI 768	Challenges in Information-Intensive Organization Administration **[New Title]**	3
Select one of the following:		
ISCI 786	Cyber Security and Information Science **[New]** (Currently offered as ISCI 795 Special Topics in International Information Issues: Cyber Security and Information Science)	3
ISCI 787	Seminar in Applied Information Systems for Information Specialists	3
Select one of the following:		
ISCI 794	Internship in Library and Information Science	3
ISCI 798	Specialist Project Preparation	3

Elective Courses: 18 hours (substitutions must be specifically approved by the student's advisor and/or graduate director)

Course	Title	Credits
ISCI 534	Knowledge Discovery Techniques	3
ISCI 560	Information Visualization	3
ISCI 608	Information Behavior and Practices	3
ISCI 704	Leadership in Information Organizations	3
ISCI 706	Information Organization and Access	3
ISCI 708	Information and Communication Needs and Assessment **[New]**	3
ISCI 709	Fundamentals of Data and Digital Communications	3
ISCI 726	Knowledge Management for Library and Information Professionals	3
ISCI 734	Government Information Sources	3
ISCI 735	Metadata	3
ISCI 770	Design and Management of Databases	3
ISCI 772	Strategic Intelligence for Information Professionals	3
ISCI 776	Web Technologies for Information Specialists	3

ISCI 779	Social Informatics **[New]**	3
ISCI 780	Information Networks	3
ISCI 786	Cyber Security and Information Science **[New]** (Currently offered as ISCI 795 Special Topics in International Information Issues: Cyber Security and Information Science)	3
ISCI 787	Seminar in Applied Information Systems for Information Specialists	3
ISCI 788	Implementing Data and Digital Communications	3
ISCI 796	Independent Study in Library and Information Science	1-6
ISCI 805	Information Policy and Ethics	3
ISCI 806	Communication Processes and Information-Seeking Behavior	3

Note: the program advisor(s) will help students choose courses based on their career interests and goals.

Students may choose to follow one of the following three tracks.

Focus on Intellectual Capital Management and Communication

Course	Title	Credits
ISCI 560	Data Visualization	
ISCI 704	Leadership in Information Organizations	3
ISCI 726	Knowledge Management for Library and Information Professionals	3
ISCI 734	Government Information Sources	3
ISCI 772	Strategic Intelligence for Information Professionals	3
ISCI 776	Web Technologies for Information Specialists	3
ISCI 788	Implementing Data and Digital Communications	3

Focus on Human Information Behavior

Course	Title	Credits
ISCI 560	Data Visualization	3
ISCI 608	Information Behavior and Practices	3
ISCI 706	Information Organization and Access	3
ISCI 779	Social Informatics **[New]** (Currently offered as ISCI 795 Special Topics in International Information Issues: Social Informatics)	3

Focus on Data Management and Communication

Course	Title	Credits
ISCI 770	Design and Management of Databases	3
ISCI 776	Web Technologies for Information Specialists	3
ISCI 779	Social Informatics **[New]** (Currently offered as ISCI 795 Special Topics in International Information Issues: Social Informatics)	3
ISCI 780	Information Networks	3
ISCI 788	Implementing Data and Digital Communications	3

And other electives as approved by advisors.

Total Credit Hours Required: 30

Core curriculum will be offered throughout the academic year as follows. Electives offered for this degree program are also available for students in other graduate programs in the iSchool, so they will be offered on a rotation that suits students in the MISCL as well. A full-time student could complete this program of study in four semesters. For a student who starts in the Fall semester, the rotation might be as follows, for example:

Curriculum by Year					
Course Name	**Credit Hours**	**Course Name**	**Credit Hours**	**Course Name**	**Credit Hours**
Year 1					
Fall		**Spring**		**Summer**	
ISCI 785 Information Security, Ethics, and Leadership in Cyber Environments	3	ISCI 768 Challenges in Information-Intensive Organization Administration	3	ISCI 794 Internship in Library and Information Science	3
ISCI 787 Seminar in Applied Information Systems for Information Specialists	3	ISCI 786 Cyber Security and Information Science	3	(AND/OR ISCI 798 Specialist Project Preparation	3)
Elective	3	Elective	3		
Total Semester Hours	9	Total Semester Hours	9	Total Semester Hours	3-6
Year 2					
Fall		**Spring**		**Summer**	
Elective	3				
Elective	3				
(AND/OR Elective	3)				
Total Semester Hours	6-9				

Similar Programs in South Carolina offered by Public and Independent Institutions

Program Name and Designation	Total Credit Hours	Institution	Similarities	Differences
Master of Arts degree program in Intelligence and Security Studies	36	The Citadel		No online option More credit hours required
Master of Science degree program in Computer and Information Sciences with a specialization in Cybersecurity	33	The Citadel and College of Charleston (joint)		No online option More credit hours required
Certificate of Graduate Studies in Cyber Security Studies	12	College of Engineering and Computing, University of South Carolina		The program's curriculum emphasizes the technology side of cybersecurity systems. No online option Not a master's degree program Currently, no students have been enrolled between the Fall 2013 and Spring 2022 semester. This certificate program may become a pathway to the MISCL program.
Cybersecurity Management Certificate	12	Darla Moore School of Business, University of South Carolina		This is a new program. This program is focused on the management/financial side of cybersecurity. This certificate program may become a pathway to the MISCL program.

In South Carolina, at the graduate level, there are two master's level programs with related content:

1. The Citadel: MA Intelligence and Security Studies with a specialization in Cybersecurity (CIP Code 29.0201).
2. The Citadel and College of Charleston (joint): MS Computer and Information Sciences with a specialization in Cybersecurity (CIP Code 11.0701) and a PBCert Cybersecurity (CIP Code 11.0701)

These programs are focused on military intelligence and computer science angles of cybersecurity. The new MISCL will not be in direct competition with these programs.

At USC, we currently have two certificate programs related to cybersecurity:

1. College of Engineering and Computing: PBCert in Cyber Security Studies (CIP Code 11.1003)
2. Darla Moore School of Business: PBCert in Cyber Management (new)

The proposed MISCL does not seek to overlap with the existing certificates offered by the CEC and DMSB in this area. Both certificate programs may become pathways to the MISCL program.

The State of South Carolina also has undergraduate degrees related to cybersecurity, three of which are in the USC system. It is expected that graduates from these programs may consider completing the MISCL as well.

Faculty

The following is an outline iSchool faculty who will be teaching core and specialized electives for this MISCL program of study. The electives selected for this program are also on rotation to be taught for the Master of Data and Communication and the Master of Library and Information Science, so all iSchool 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 Full-time	**ISCI 768**	PhD Library and Information Studies, Florida State University	23 years experience teaching management and administration courses at graduate level
Associate Professor Full-time	ISCI 785, ISCI 805	PhD Communication and Information, University of Tennessee-Knoxville	Deep in research related to intellectual property, information policy, and international issues of information ethics and legal issues
Associate Professor Full-time	ISCI 779	PhD Library and Information Science, Rutgers University	Has taught Social Informatics at the undergraduate level for 6 years—is proponent for developing the new graduate-level version of this course
Associate Professor Full-time	ISCI 708	PhD Communication and Information, Kent State University	Has taught Information Needs at undergraduate level for 6 years—is proponent for developing the new graduate-level version of this course

Assistant Professor Full-time	ISCI 560	PhD Information Science, University of Wolverhampton	Created ISCI 560 course and teaches it for the Master in Data and Communication program; leads the Human Impact of Data Analytics Research Lab
Instructor Full-time (4+4)	ISCI 534, ISCI 709, ISCI 788, **ISCI 785, ISCI 786**	EdD Curriculum and Instruction, Valdosta State University MBA Columbia Southern University MEd Educational Technology, USC-Aiken BS Technology Support and Training Management, USC	Senior instructional designer (Center for Teaching Excellence USC), coordinator of online learning (Student Success Center at USC), instructional systems analyst (Georgia Regents University), and desktop technician (USC); currently teaches ISCI 534, ISCI 709, ISCI 788 for the Master in Data and Communication
Instructor Part-time (3+3)	**ISCI 785, ISCI 786**	MMA, USC 6 years teaching Media Arts 8 years teaching courses related to IT 2 years teaching CCSA training	Check Point training in CCSA instruction; 15 years Web and IT industry experience
Instructor Full-time (4+4) [New hire]	**ISCI 787, ISCI 794, ISCI 798**	PhD in related field	Will coordinate internships and specialist project preparation courses, teach ISCI 787 and other cyber courses as needed

Core courses noted in bold. Not all electives are listed here, as they will be taught on a looser rotation than the core, as they are also taught to meet the needs of Master in Data and Communication, Certificate in Data and Communication, and Master of Library and Information Science programs. Other faculty from the iSchool can teach electives as needed.

Total FTE needed to support the proposed program:
Faculty: 1 Professional Faculty hire (Shared with CISCL)
Staff: .10 Advisor allocation (shared with CISCL)
Administration: .10 Faculty allocation for program coordinator (shared with CISCL)

Faculty, Staff, and Administrative Personnel
One new Professional Faculty member (4+4 teaching) will be hired to fulfill the needs of this MISCL program. The iSchool expects to appoint this faculty member in the Fall semester in 2024.

Resources

Library and Learning Resources
As noted previously, cyber-related content is not particular to any one School or program. We currently have several cyber-related curricula in the College of Arts and Sciences, the College of Computer Science and Engineering, and in the Darla Moore School of Business. These resources, in addition to leadership and social informatics resources already provided by the USC Library System, will suffice for this program as well.

Student Support Services

The iSchool advising and admissions team already provide stellar services for our graduate students in the Master of Data and Communication, Certificate in Data and Comunication, and our Master of Library and Information Science programs. With the allocation of 10% additional support for advising (e.g., graduate assistant or additional portion of a FTE advisor) will provide the advising team time for admitting, advising, orienting, and administration of student records in the MISCL.

Physical Resources/Facilities

The proposed MISCL will be 100% online, so no new classroom space will be needed. In the CIC, since 2021 we have provided all students with access to Adobe Cloud software suite as a learning tool. Access to CheckPoint cloud software and other online resources, Brandwatch, and data visualization software will be required for several courses. The iSchool already partners with CheckPoint, and the use of the CheckPoint Software will be covered in our agreement with CheckPoint for students enrolled in the MISCL. Data visualization resources and user licenses for students of Brandwatch are already part of the CIC infrastructure, and the new program will provide additional use of resources already in place.

Equipment

The School of Information Science has strong relationships with two global cyber companies: Check Point and the Teneo Group. The iSchool is the first university in North America to partner with Check Point Software Technologies. The iSchool has a Memorandum of Understanding (MOU) with Check Point for an iSchool instructor to teach a class for their SecureAcademy Program. The one-semester, three-credit class, ISCI 795 - Special Topics in International Information Issues: Cyber Security and Information Science will lead to CCSA certification. Check Point has already donated over $450,000 dollars in resources towards this program, including the following:

- A Check Point Gateway appliance (server), plus software and licenses
- Average of 14,000 hours of Virtual Cloud Lab Services
- Nine Check Point engineers who served as guest lectures and support group

In addition, the iSchool has a strong relationship with The Teneo Group, one of Check Point's partners. This cyber industry leader is working with the iSchool to establish an internship program for our students. The Teneo Group piloted the program with our first iSchool intern this summer. The company has already hired one of our rising seniors to work for them in 2023. Finally, the iSchool is currently in discussions with other companies in South Carolina to place our students in cyber-related internships and jobs. For example, in July 2022, we met with PC Matic, an award-winning anti-virus cyber security company based in Myrtle Beach, to collaborate on internship plans. There will be future meetings this fall to discuss additional collaborations.

Impact on Existing Programs

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

☐Yes

☒No

While these above-listed programs provide content at the undergraduate and graduate (certificate) related to cybersecurity, as noted by the varying CIP Codes, they each approach cybersecurity from a different angle. The proposed master's program brings in yet another facet of cybersecurity: a focus on the information science and leadership facets of cybersecurity. This program will be a pathway for individuals who wish to develop a specialization in the subject areas related to information security, cyber environments, communication, data management, information science and technology, and

leadership. In addition, this program will also serve as an advanced study program for individuals who want to pursue graduate studies at the USC. In short, this program intends to educate a competent workforce with sophisticated communication, information, people, and technology skills to meet the demands of both the public and private sectors.

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	$206,010.00	$206,010.00	$61,803.00	$267,813.00		$267,813.00	$30,901.50	$298,714.50	$41,202.00	$339,916.50	$339,916.50	$1,380,267.00
Program-Specific Fees	$15,840.00	$15,840.00	$4,752.00	$20,592.00		$20,592.00	$2,376.00	$22,968.00	$3,168.00	$26,136.00	$26,136.00	$106,128.00
Special State Appropriation												
Reallocation of Existing Funds												
Federal, Grant, or Other Funding												
Total	$221,850.00	$221,850.00	$66,555.00	$288,405.00		$288,405.00	$33,277.50	$321,682.50	$44,370.00	$366,052.50	$366,052.50	$1,486,395.00
Estimated Costs Associated with Implementing the Program by Year												
Category												
Program Administration and Faculty/Staff Salaries	$97,500.00	$97,500.00		$97,500.00		$97,500.00		$97,500.00		$97,500.00	$97,500.00	$487,500.00
Facilities, Equipment, Supplies, and Materials	$1,000.00	$1,000.00	$1,000.00	$2,000.00	$1,000.00	$3,000.00	$1,000.00	$4,000.00	$1,000.00	$5,000.00	$5,000.00	$15,000.00
Library Resources												
Other -Marketing	$10,000.00	$10,000.00	$10,000.00	$20,000.00	$10,000.00	$30,000.00	$10,000.00	$40,000.00	$10,000.00	$50,000.00	$50,000.00	$150,000.00
Other – USC Participation Tax (17% of tuition revenue)	$35,021.70	$35,021.70	$10,506.51	$45,528.21		$45,528.21	$5,253.26	$50,781.47	$7,004.34	$57,785.81	$57,785.81	$234,645.39
Total	$143,521.70	$143,521.70	$21,506.51	$165,028.21	$11,000.00	$176,028.21	$16,253.26	$192,281.47	$18,004.34	$210,285.81	$210,285.81	$887,145.39
Net Total (Sources of Financing Minus Estimated Costs)	$78,328.30	$78,328.30	$45,048.49	$123,376.79	$(11,000.00)	$112,376.79	$17,024.25	$129,401.04	$26,365.66	$155,766.70	$155,766.70	$599,249.61

Budget Justification

Tuition and program fee estimates are modeled on graduate resident tuition rate of $527.25 per credit hour, graduate program fee of $44.00 per credit hour, and the enrollment figures provided on the second tab. The enrollment estimates are provided by a program interest study conducted by Kennedy & Co. Estimated costs include $75,000 salary for an additional faculty member and associated fringe. Equipment and supplies are estimated at $1,000 per year. No additional facilities will be required. Marketing expense is estimated at $10,000 per year and will build on marketing efforts established with the certificate program.

The MISCL and CISCL programs will complement each other in terms of instruction, administration, and advising. Resources will be shared between the two new programs.

Evaluation and Assessment

All students will submit an end-of-program portfolio. Students will choose an example of work they have completed as part of one of the courses relating to each learning outcome and will present a work sample. Selected work samples may include, but are not limited to, research papers, projects, and posters; professional briefs; recorded presentations; and other completed course assignments. In addition to the selected work sample, students must also provide a reflective essay that analyzes and clearly describes how the selected work sample demonstrates competency in this area and achievement of this learning outcome. Faculty advisors score the work sample and the reflective essay based on a scoring guide/rubric. In order for the learning outcome to be considered achieved, 85% of all graduating students should score proficient (61%) or higher on the information and its organization category.

The iSchool uses an exit survey for all graduates of our programs. These data are used in conjunction with the end-of-program portfolio to evaluate our degree programs and make modifications as needed. This exit survey also requests a non-USC email address for each graduate. Six months after graduation we contact them to collect employment data for an additional layer of program assessment.

Program Objectives	Student Learning Outcomes Aligned to Program Objectives	Methods of Assessment
Analyze human information behavior and information security phenomena in cyber environments	• Distinguish the contexts of human information behavior - institutional, organizational, and social. • Understand various users and uses of information, and related information seeking processes. • Survey foundational and current research on information use and users and assess its application to the development of information systems and services. • Explain the factors that impact the transfer and exchange of information and the differences among various user groups, including	End-of-program portfolio

	researchers, professionals, the general public, and children.	
Explain the structure of a cybersecurity system, implement the system, handle the system operations, and evaluate the system efficiency	• Explain and demonstrate how Check Point R81 Security Management products work and how they protect networks. • Produce the essential elements of a security policy (informed by the elements and capabilities of Check Point R81 Security Management). • Implement information skills gained through collaboration with industry leaders, architects, and instructors. • Enable application control and URL filtering software. • Apply tools designed to monitor data, determine threats, and recognize opportunities for performance improvements across Cloud Security, Mobile Security, and End Point Security. • Upon application, students will articulate how this Intrusion Prevention System is configured, maintained, and tuned. • Administer an Infinity Threat Prevention System across networks.	End-of-program portfolio
Strategically analyze the external and internal environments of an organization to create and facilitate a human-systems integration process	• Describe and discuss the general range of administrative problems of information intensive organizations along with a range of relevant solution strategies. • Diagnose and propose creative solutions for administrative problems in a particular type of information agency based on a broad systems level understanding of problem(s) at	End-of-program portfolio

	hand and relevant evidence from an organization or context of personal interest. • Develop and present such tools as strategic, financial, communication, disaster, and accessibility plans to either address current administrative problems or attack future ones before they occur.	
Create teams for human-systems integration environments and facilitate team communication and coordination	• Apply evidence-based decision-making -- informed by an organization's strategic vision -- to complex leadership and project management issues • Identify the steps of a needs assessment process and apply it to organizational challenges • Identify various sources of revenue and select an appropriate budget model based on project needs and resource constraints. • Outline the process for acquiring and implementing technology resources. • Assemble a variety of interpersonal managerial tools such as recruiting, hiring, orientation, evaluation, and facilitation of critical conversations. Define and explore the concepts of community, community ownership, and community engagement	End-of-program portfolio
Develop information policies and regulations for human-systems integration and cyber information security system environments	• Define cyber and information policy, and cyber and information ethics • Identify and explain at least 3 information policy issues • Identify and explain at least 3 information ethics issues • Articulate at least 1 technological innovation that has historically or currently	End-of-program portfolio

	shaped information policy and ethics • Apply at least 1 tool for analyzing information policy problems and propose policy solutions • Identify at least 1 career opportunity in the information policy and ethics sub-discipline	

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

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.

The ISCI 795 Special Topics in International Information Issues: Cyber Security and Information Science and ISCI 786 Cyber Security and Information Science courses provide students with essential skills and training in information and cybersecurity leading to the option to complete the Check Point Certified Security Administrator (CCSA) certification process through Check Point Software Technologies.

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