ACAP
9/29/16
Agenda Item 4a

Name of Institution: University of South Carolina

Name of Program: Master of Science in Information Security (MSIS)

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.)

Does the program qualify for supplemental Palmetto Fellows and LIFE Scholarship awards?

- ☐ Yes
- ☒ No

Proposed Date of Implementation: Spring 2017 CIP Code: 11.1003

Delivery Site(s): University of South Carolina - Columbia

Delivery Mode

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

Program Contact Information (name, title, telephone number, and email address)
Dr. Csilla Farkas
Associate Professor, Dept. of Computer Science and Engineering
Telephone: (803) 576-5762
Email: farkas@cec.sc.edu

Institutional Approvals and Dates of Approval

Graduate Council	October 26, 2015
USC Board of Trustees	June 24, 2016

Background Information

State the nature and purpose of the proposed program, including target audience and centrality to institutional mission. (1500 characters)

The purpose of the proposed program is to produce well-trained information security professionals. There is a world-wide shortage of security professionals. This shortage is predicted to increase to the point of becoming a global security problem in the future. Under the leadership of the Department of Computer Science and Engineering, the University of South Carolina (USC) has been systematically developing cyber security capabilities, and has established nationally ranked educational and research programs in the field. USC is presently the only higher education institution in South Carolina designated by the National Security Agency and the Department of Homeland Security as a National Center of Academic Excellence (CAE) in Information Assurance and Cyber Defense Education (2010-2020), and as a CAE in Information Assurance Research (2015-2020).

The proposed MS in Information Security (MSIS) will provide comprehensive graduate level training. The primary target audience is information security professionals with a Baccalaureate degree or its equivalent in computer science, engineering, or a related field. Students from other fields will be admitted, provided that they complete core technical background courses. Graduates of the program would be highly sought-after by a range of private sector industries already in the State of South Carolina as well as defense organizations, and state and local government agencies. The program supports the institutional mission in enabling protection of the quality of life for citizens of the State and the country, and promoting responsible citizenship in a changing world.

List the program objectives. (2000 characters)

The proposed MSIS aims to offer a high quality educational program for information security professionals. The core requirements provide the students with the knowledge and skills needed to successfully evaluate information security needs, identify appropriate counter measures, and implement security technologies. The focus area courses enable the students to concentrate on specific areas of interest, such as software, network, or database security. The proposed program is aligned with national guidelines for information security professionals. The following list presents the learning outcomes of the MSIS program.

Upon completing the MSIS program, students will be able to

- Perform information security risk assessment, identify potential threats, and develop threat mitigation strategies.
- Describe individual privacy rights, related laws and regulations, and the use of information assurance technologies to support the enforcement of these rights.
- Describe the responsibilities of all levels of users related to the threats against information systems.
- Describe security design principles and identify security mechanisms to implement desired security principles.
- Implement security defense technologies.
- Identify malicious activities and attacks, and recommend appropriate response capabilities.
- Carry out incident response activities and support cyber-crime investigation.
- Perform audit procedures, evaluate the strengths and weaknesses of the security mechanisms, and develop contingency plans.
- Communicate information security concepts to individuals with diverse levels of computing skills.

Assessment of Need

Provide an assessment of the need for the program for the institution, the state, the region, and beyond, if applicable. (1500 characters)

Cyber security labor market surveys predict a major workforce shortage. According to Symantec corporation, by 2019, the global workforce demand is expected to reach 6 million, with a 1.5 million shortfall. The Bureau of Labor Statistics indicates Information Security Professionals to be among the 20 fastest growing occupations. The expected growth between 2012 and 2022 is 37%; that is much faster than average growth.

USC is well positioned to provide information security leadership in South Carolina. USC has been systematically developing security capabilities since 2000. Information security is one of the strategic directions of USC. The proposed program supports the ongoing private-public partnership initiative in cyber security led by USC's Economic Engagement office. USC's collaboration with other higher education institutions, government agencies, and industry provides a strong foundation enabling USC to address the information security needs of the state.

The proposed program will be of interest to a wide group of computing professionals as well as to non-technical leadership. Information security has become a national and international concern. The enrollment in information security courses at USC has been increasing from 63 students during the school year 2013-2014, to 122 during the Summer and Fall semesters of 2015. The department has also received a large number of requests for a Master-level program in information security. These all indicate local and regional interest in the proposed program.

Employment Opportunities

Is specific employment/workforce data available to support the proposed program?

☒Yes

☐No

If yes, complete the table and the component that follows the table on page 4. If no, complete the single narrative response component on page 5 beginning with "Provide supporting evidence."

Employment Opportunities			
Occupation	**Expected Number of Jobs**	**Employment Projection**	**Data Source**
Information Security Analysts	75,100 (2012)	37% increase between 2012-2022	Bureau of Labor Statistics http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm
Security Analyst, Security Consultant		1.9 million in US (2019 with compound annual growth rate 6%)	The 2015 (ISC)2 Global Information Security Workforce Study https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC)%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf

Provide additional information regarding anticipated employment opportunities for graduates. (1000 characters)

Initiatives such as the National Security Agency and the Department of Homeland Security National Center of Academic Excellence in Information Assurance, aim to support cybersecurity workforce development. The National Initiative for Cybersecurity Careers and Studies (https://niccs.us-cert.gov/) concludes that the demand for cybersecurity specialists is growing and there are not enough cyber security professionals to keep pace with the requirements. Information Security Analyst is listed by the US News and World Report as number 3 on the list of the best technology jobs (http://money.usnews.com/careers/best-jobs/rankings/best-technology-jobs). USC's effort to develop information assurance capabilities will help to alleviate the impact of this national workforce shortage.

Provide supporting evidence of anticipated employment opportunities for graduates, including a statement that clearly articulates what the program prepares graduates to do, any documented citations that suggests a correlation between this program and future employment, and other relevant information. Please cite specific resources, as appropriate. (3000 characters)

Note: Only complete this if the Employment Opportunities table and the section that follows the table on page 4 have not previously been completed.

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

☒Yes

☐No

If yes, explain. (500 characters)

The proposed program will complement the existing programs at USC. The impact of the proposed program, if any, will be on the current graduate programs offered by the Department of Computer Science and Engineering. It is possible that the enrollment in these programs may shift slightly due to some students choosing information security over existing, more general, computing programs. However, we expect the overall enrollment in all our graduate programs to increase because of the broader audience of the new MSIS program.

List of Similar Programs in South Carolina

Program Name	Institution	Similarities	Differences
Graduate Certificate in Cybersecurity	The Citadel and College of Charleston http://www.citadel.edu/root /mathcs-programs/cyber-security-graduate-certificate	The 12 credit hours coursework is similar to the core requirements of the proposed M.S. in Information Security (MSIS) program.	The proposed MSIS provides a more comprehensive coverage of information security than the graduate certificate program. The main differences are: 1. MSIS requires 30 hours of coursework including 18 hours in courses on security related topics, whereas the Graduate Certificate requires 12 credit hours and only 6 of these credits are purely cyber security. 2. Students can engage in research by performing independent study or Thesis work. 3. MSIS includes secure software development as a core requirement. 4. Students can develop advanced knowledge and skills in specific focus areas, such as networking, software, and database security. 5. In addition to the technical areas, managerial, social, and legal aspects of cyber security are included. 6. Interdisciplinary activities are enabled by the 12 credit hours elective courses.
Master of Science in Information Systems Technology (MSIST) Information Security and Data Analytics Concentration	Coastal Carolina University https://www.coastal.edu /science/departments/cs/ majorsandminors/ graduateprogram/	1. The MSIST course work requires 4 information security courses (12 credit hours) that are similar to the core requirements of the proposed M.S. in Information Security (MSIS) program. 2. Both programs give the option on Thesis research for 6 credit hours. 3. Both programs allow that students enroll in additional elective courses on security.	The proposed MSIS emphasizes information security while the MSIST program of Coastal Carolina incorporates both information security and data analytics. The main differences are: 1. The MSIST program of Coastal Carolina requires 12 credits of information security courses (6 credit hours of core courses and 6 credit hours of elective courses). The proposed MSIS program of USC requires 18 credit hours of information security courses (9 credit hours of core courses and 9 credit hours of elective courses), thus ensuring a solid foundation in all aspects of information security. 2. The core course requirements of the proposed MSIS program include secure software development and network security; two of the most critical security fields. These courses offered as elective courses in the MSIST program of Coastal Carolina.
Graduate Certificate in Cyber Security Studies	University of South Carolina https://cse.sc.edu/ graduate/ias	4. The 12 credit hours of coursework is similar to the core requirements of the proposed M.S. in Information Security (MSIS) program.	Same as those for The Citadel's Graduate Certificate in Cybersecurity Note that the current Graduate Certificate in Cyber Security Studies is suitable for MS in Computer Science students, who are interested in other technical fields but would like to have graduate-level core training in information security.

Description of the Program

Projected Enrollment						
Year	Fall		Spring		Summer	
	Headcount	Credit Hours	Headcount	Credit Hours	Headcount	Credit Hours
2016-2017	8	72	8	72	8	24
2017-2018	10	90	10	90	10	30
2018-2019	12	108	12	108	12	36
2019-2020	14	126	14	126	14	42
2020-2021	14	126	14	126	14	42

Justification of projected enrollment: In recent years, the Department of Computer Science and Engineering has experienced a steady increase of enrollments in the information security courses. In particular, the 500-level courses are popular among the undergraduate computing students. Our goal is to encourage these students to continue their studies in one of the graduate-level information security programs offered by the CSE department. The following table shows the student enrollment in the security courses offered by the department during the last three years.

Enrollment in Information Security Courses

Date	CSCE course number							
	517	**522**	**590**	**715**	**727**	**813**	**824**	**TOTAL**
2015 Summer/Fall	20	53	26			23		**122**
2014-2015	18	33		19	14		10	**94**
2013-2014		34		9	10	10		**63**

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

☐Yes

☒No

If yes, explain. (1000 characters)

Are there any special articulation agreements for the proposed program?

☐Yes

☒No

If yes, identify. (1000 characters)

Curriculum by Category

The proposed M.S. in Information Security degree requires 30 credit hours of coursework consisting of 9 credit hours in required core courses, 9 credit hours of approved security focus area courses and 12 credit hours of elective graduate-level courses. At least 15 credit hours must be at 700-level or above. M.S. Thesis is optional but not required.

Admission Criteria

The admission criteria will generally conform to those currently required by the USC Graduate School and the Department of Computer Science and Engineering. In general, an applicant must have a Baccalaureate degree or its equivalent in engineering, computer science or a related field from an accredited institution. In addition, students from other areas, such as political science, law, criminology, medical informatics, will be admitted, provided that they complete core technical background courses. Admission will be based on the applicant's GRE score, letter of recommendation, and GPA.

Core courses (9 credits): Introduce foundational knowledge of current information security theory and practice.

- CSCE 522 – Information Systems Security Principles (3 credit hours)
- CSCE 548 – Building Secure Software (3 credit hours)
- CSCE 715 – Network Systems Security (3 credit hours)

Focus Area (9 credits): Enable students to focus on specific topics of interest.

- CSCE 517 – Computer Crime and Forensics (3 credit hours)
- CSCE 557 – Introduction to Cryptography (3 credit hours)
- CSCE 719 – Security and Privacy for Wireless Networks (3 credit hours)
- CSCE 727 – Information Warfare (3 credits)
- CSCE 747 – Software Testing and Quality Assurance (3 credits)
- CSCE 813 – Internet Security (3 credit hours)
- CSCE 824 – Secure Databases (3 credit hours)
- CSCE 846 – Software Reliability and Safety (3 credits)

Other electives (max. 12 credits):

- Any CSCE course above 500
  This may include CSCE 799 – MS Thesis preparation for maximum 6 credits.
- Any approved course

Total Credit Hours Required: 30

Course Descriptions for New Courses

No new courses are being proposed.

Faculty

Faculty and Administrative Personnel				
Rank	**Full- or Part-time**	**Courses Taught or To be Taught, Including Term, Course Number & Title, Credit Hours**	**Academic Degrees and Coursework Relevant to Courses Taught, Including Institution and Major**	**Other Qualifications and Comments (i.e., explain role and/or changes in assignment)**
Associate Professor	FT	CSCE 522 — Information Security Principles (3) *Fall 2015* CSCE 548 — Building Secure Software (3) *Spring 2012* CSCE 727 — Information Warfare (3) *Spring 2016* CSCE 813 — Internet Security (3) CSCE 824 — Secure Database Systems (3) *Spring 2016*	Ph.D Information Technology	Lead instructor for courses CSCE 522, 548, 727, and 824 • CSCE 522 will be offered in every Fall • CSCE 548 will be offered in every Spring and/or summer • CSCE 727 will be offered in every 4th semester • CSCE 824 will be offered in every 4th semester
Professor	FT	CSCE 557 — Introduction to Cryptography {=MATH 587} (3)	Ph. D., Mathematics	Teaching CSCE 557 for Spring 2016
Professor	FT	CSCE 522 — Information Security Principles (3)	Ph. D., Computer Science	Has taught undergraduate level information security course CSCE 201, and CSCE 522.
Professor	FT	CSCE 557 — Introduction to Cryptography {=MATH 587} (3) *Spring 2016*	Ph. D., Computer Science	Lead instructor for CSCE 557. The course is co-listed with the Department of Mathematics (MATH 587), and taught by faculty of either department. • CSCE 557 will be offered in every 4th semester
Assistant Professor	FT	CSCE 548 — Building Secure Software (3) CSCE 747 — Software Testing and Quality Assurance (3) *Spring 2016* CSCE 846 — Software Reliability and Safety (3)	Ph.D., Computer Science	Lead instructor for CSCE 747 and CSCE 846. • CSCE 747 will be offered in every Spring semester • CSCE 846 will be offered in every 4th semester

Associate Professor	FT	CSCE 715 — Network Systems Security (3) *Spring 2015* CSCE 813 — Internet Security (3) *Fall 2015*	Ph. D., Computer Science	Lead instructor for CSCE 715 and CSCE 813. • CSCE 715 will be offered in every Fall semester • CSCE 813 will be offered in every 4th semester
Professor and Chair	FT	CSCE 517 — Computer Crime and Forensics (3) CSCE 747 — Software Testing and Quality Assurance (3) CSCE 846 — Software Reliability and Safety (3)	Ph. D., Mathematics	Has taught CSCE 517, 747
Associate Professor	FT	CSCE 715 — Network Systems Security (3) CSCE 719 — Security and Privacy for Wireless Networks (3)	Ph. D., Electrical and Computer Engineering	Lead instructor for CSE 719. • CSCE 719 will be offered in every 4th semester
System Administrator	FT	CSCE 517 — Computer Crime and Forensics (3) *Summer 2015*	M.S., Computer Science and Engineering	Lead instructor for CSCE 517. • CSCE 517 will be offered in every summer semester

Total FTE needed to support the proposed program (i.e., the total FTE devoted just to the new program for all faculty, staff, and program administrators):

The graduate director and the administrative assistant will oversee 2 PhD and 4 Master's programs, amounting to 10% of effort for each Master's program. Each of the eight faculty and the instructor listed above contribute 10% of their effort towards teaching the students of the proposed program. Accordingly, the FTE's of the proposed program are:

Faculty: 0.9 Staff: 0.1 Administration: 0.1

Faculty /Administrative Personnel Changes

Provide a brief explanation of any additional institutional changes in faculty and/or administrative assignment that may result from implementing the proposed program. (1000 characters)

For the program administration, the graduate director is paid an amount equivalent to 10% of his/her salary for one month. In addition, 10% of the CSE department administrative assistant effort will be assigned to this program's administration.

This new program does not require any additional faculty hires. All the courses are already taught on a regular basis by the existing faculty members. The existing faculty include 8 full time faculty members and 1 instructor. Each of them will contribute 10% of their effort (with the rest devoted to the other 3 Master's and 2 PhD programs in the department), amounting to a total of 0.9 faculty FTE, towards teaching and mentoring the students of the proposed program.

Library and Learning Resources

Identify current library/learning collections, resources, and services necessary to support the proposed program and any additional library resources needed. (1000 characters)

The current holdings of the Thomas Cooper Library satisfy most of the current research and teaching requirements of the proposed program. We request $2,000 yearly to purchase additional materials that are not covered by the library budget of the College of Engineering and Computing.

Student Support Services

Identify academic support services needed for the proposed program and any additional estimated costs associated with these services. (500 characters)

No additional academic support services are needed for the proposed program.

Physical Resources

Identify any new instructional equipment needed for the proposed program. (500 characters)

No additional physical space will be needed for the proposed program.

Will any extraordinary physical facilities be needed to support the proposed program?

☐Yes

☒No

Identify the physical facilities needed to support the program and the institution's plan for meeting the requirements, including new facilities or modifications to existing facilities. (1000 characters)

No new facilities are needed.

Financial Support

Estimated New Costs by Year						
Category	**1st**	**2nd**	**3rd**	**4th**	**5th**	**Total**
Program Administration A 3% increase/year is calculated after the 1st year	1,271	1,309	1,348	1,388	1,430	6,746
Faculty Salaries (AVG. salary $104340)	93,906	96,723	99,625	102,614	105,692	498,560
Staff Salaries	4,750	4,893	5,040	5,191	5,347	25,221
Library Resources	2,000	2,000	2,000	2,000	2,000	10,000
Other*						
Total	**101,927**	**104,925**	**108,013**	**111,193**	**114,469**	**540,527**
Sources of Financing						
Category	**1st**	**2nd**	**3rd**	**4th**	**5th**	**Total**
Tuition Funding (21 credits/student /year) # of students enrolled	136,206 Instate: 4 Out-of-state: 4	175,365 Instate: 5 Out-of-state: 5	216,751 Instate: 6 Out-of-state: 6	260,463 Instate: 7 Out-of-state: 7	268,277 Instate: 7 Out-of-state: 7	1,057,062
Net Total (i.e., Sources of Financing Minus Estimated New Costs)	**34,279**	**70,440**	**108,738**	**149,270**	**153,808**	**516,535**

*Provide an explanation for these costs and sources of financing in the budget justification.

Budget Justification

Provide a brief explanation for the other new costs and any special sources of financing (state funding, reallocation of existing funds, federal funding, or other funding) identified in the Financial Support table. (1000 characters)

Note: Institutions need to complete this budget justification *only* if any other new costs, state funding, reallocation of existing funds, federal funding, or other funding are included in the Financial Support table.

There are no other new costs, state funding, reallocation of existing funds, federal funding, or other funding included in the financial support table. The revenue from tuition is estimated at $516 per credit hour for instate tuition and $1,105.5 for out-of-state tuition. The total tuition revenue was calculated based on the credit hours shown under the projected enrollment.

Evaluation and Assessment

Programmatic Assessment: Provide an outline of how the proposed program will be evaluated, including any plans to track employment. Identify assessment tools or software used in the evaluation. Explain how assessment data will be used. (3000 characters)

The assessment of the proposed MSIS will be performed by the assessment of the learning outcomes (see the following table) and the assessment of the program's success.

We will periodically measure the success of the MSIS program to ensure continuous quality improvement and that the program meets the changing demands. Initially, we plan to perform yearly assessment on the program, followed by a full assessment of the program and the learning outcomes in the 3rd year. We plan full assessment every 5 years afterwards.

The assessment of the program will be based on the 1) rate of recruitment, 2) rate of retentions, 3) satisfactory offering of the core and elective courses, 4) M.S. Theses and professional publications, and 5) the placement of the graduates.

Recruitment: We anticipate a steadily increasing enrollment during the first five years. We will compare enrollment demographics (e.g., field of undergraduate studies, transfer information, GRE score, etc.) of the MSIS students and the other M.S. programs in the department.

Retention: We will collect and analyze data about the rate of successful completion of the program. We will also collect data for identifying the characteristics of students who dropped out of the program. We aim to use these characteristics to provide intervention and reduce the number of students who transfer out or drop out of the program.

Course offering: The department already offers sufficient courses to enable completion of the MSIS program in a timely manner. We will monitor the schedule and ensure that a full time student will be able to complete the program within 2 years.

Job placement: We will track the job placement of the MSIS graduates. We will analyze the data on the employment of MSIS graduates immediately after graduation and many years after graduation. We will gather information about the position title, rank, size of the organization, and primary responsibilities. It is anticipated, that near graduation employment will be primarily in the technical areas of information security. However, after 5 years, graduates are expected to move into leadership positions.

Student Learning Assessment

Learning outcomes of the proposed M.S. in Information Security are assessed through assignments, projects, tests, and presentations of the courses that cover the educational topics. In the following table, we list the expected learning outcomes and the core course that covers the corresponding topics. The core courses will provide the baseline assessment of student learning outcomes. Additional assessments will be available from elective courses.

Expected Student Learning Outcomes	Methods of/Criteria for Assessment
Perform information security risk assessment, identify potential threats, and develop threat mitigation strategies	Core courses: CSCE 522, CSCE 548, CSCE 715 Homework, tests, projects, and oral presentations
Describe individual privacy rights, related laws and regulations, and the use of information assurance technologies to support the enforcement of these rights	Core courses: CSCE 522 Homework, tests
Describe the responsibilities of all levels of users related to the threats against information systems	Core courses: CSCE 522 Tests, oral presentations
Describe security design principles and identify security mechanisms to implement desired security principles	Core courses: CSCE 522 and CSCE 715 Homework, tests, and projects
Identify malicious activities and attacks, and recommend appropriate response capabilities	Core courses: CSCE 522, CSCE 548, CSCE 715 Homework, tests, projects, and oral presentations
Implement security defense technologies	Core courses: CSCE 522, CSCE 548, CSCE 715 Homework, test, project, and oral presentations
Perform audit procedures, evaluate the strengths and weaknesses of the security mechanisms, and develop contingency plans	Core courses: CSCE 522 Homework, test
Communicate information security concepts to individuals with diverse levels of computing skills	Core courses: CSCE 522, CSCE 548 Homework, oral presentation

Will the proposed program seek program-specific accreditation?

☐Yes

☒No

If yes, provide the institution's plans to seek accreditation, including the expected timeline for accreditation. (500 characters)

Will the proposed program lead to licensure or certification?

☐Yes

☒No

If yes, explain how the program will prepare students for licensure or certification. (500 characters)

Teacher or School Professional Preparation Programs

Is the proposed program a teacher or school professional preparation program?

☐Yes

☒No

If yes, complete the following components.

Area of Certification

Please attach a document addressing the South Carolina Department of Education Requirements and SPA or Other National Specialized and/or Professional Association Standards.