

**New Program Proposal  
 Master of Science in Information Security  
 University of South Carolina Columbia**

**Summary**

The University of South Carolina Columbia requests approval to offer a program leading to the Master of Science in Information Security to be implemented in Spring 2017. The proposed program is to be offered through traditional instruction. The following chart outlines the stages of approval for the proposal; the Advisory Committee on Academic Programs (ACAP) and the Committee on Academic Affairs and Licensing voted to recommend approval of the proposal. The full program proposal and support documents are attached.

<b>Stages of Consideration</b>	<b>Date</b>	<b>Comments</b>
Program Proposal Received	7/1/16	Not Applicable
ACAP Consideration	9/29/16	Representatives from University of South Carolina Columbia discussed the need for the program. Members of the Advisory Committee on Academic Programs (ACAP) discussed the program, including an inquiry about the decision to offer the program as traditional face-to-face with less than 50% of the instruction online. USC representatives responded that this was a standard mode of delivery for the courses.  ACAP members voted to approve the program proposal.
Comments and suggestions from CHE staff sent to the institution	10/12/16	Staff requested the proposal be revised to: <ul style="list-style-type: none"> <li>▪ Provide program objectives in addition to the student learning outcomes in the Background Information section</li> <li>▪ Include in the Assessment of Need section the number of job positions that require a master’s degree. Also, this section states that the department has received “a large number of requests” for a master-level program; as discussed at the ACAP meeting, include information about sources of the requests and whether assessment of need data is available.</li> <li>▪ Provide available local and state employment data, including the number of positions available and projected employment growth</li> <li>▪ Explain why the curriculum includes 12 credit hours of elective graduate courses and whether there is a need for more specificity in this type of degree program at the graduate level</li> <li>▪ Verify specific admission criteria. The proposal states that the admission criteria will conform to those currently</li> </ul>

Stages of Consideration	Date	Comments
		<p>required by the USC Graduate School and the Department of Computer Science and Engineering.</p> <ul style="list-style-type: none"> <li>▪ Describe the academic support services associated with the program for reviewers who are unacquainted. The current edition states no additional academic support services are needed. Describe the student support services that will be available to students enrolled in the program.</li> <li>▪ Revise the response to the question about the physical facilities needed to support the program to describe the classroom and other space available for the program</li> <li>▪ Explain in the budget justification section how you calculated the tuition funding and provide the figures used for in-state and out-of-state tuition. Staff appreciated the in-state/out-of-state ratio provided.</li> <li>▪ State whether external feedback from employers, clients, or others is possible for program assessment or student learning assessment.</li> <li>▪ Include the discussion at ACAP about the reasons for offering the program through traditional instruction instead on online.</li> <li>▪ Include the discussion at ACAP about the transferability of courses from other institutions.</li> </ul>
Revised Program Proposal Received	10/20/16	The revised proposal satisfactorily addressed the requested revisions.
CAAL Consideration	11/10/16	<p>The representative from the University of South Carolina explained the need for the proposed program, citing nationwide workforce development and instructor-training in cyber security. Committee members asked what is the pathway to this degree program and if someone with a certificate could pursue the degree. The representative from USC stated students must have a bachelor’s degree in computer science to be admitted into the Master’s degree program.</p> <p>Commissioners also asked about the estimated headcount of twelve when total enrollment in current courses is over one hundred. Representatives from the institutions stated they were conservative in their estimates for enrollment in a Master’s degree program based on enrollment in undergraduate courses. Students enrolled in courses pursue multiple degree programs and all do not lead toward cyber security.</p> <p>Commissioners inquired about collaboration, articulation, and transferability of courses with other programs in the state. Representatives from The Citadel responded that their program was an undergraduate program and is veteran-focused. The</p>

Stages of Consideration	Date	Comments
		<p>Citadel is in support of the program at USC Columbia because the supply is far below the demand for graduates in information security. Institutional representatives stated that both USC Columbia and The Citadel are National Centers of Academic Excellence in Information Assurance and Cyber Defense Education, which is a distinction that helps to facilitate course transfer between institutions. Commissioners asked for additional information of the Memorandum of Understanding (MOU) between The Citadel and USC Columbia.</p> <p>Commissioners questioned representatives from USC Columbia about the possibility of a reduction in tuition since the program is projected to have 100% profit. Representatives from the institution noted there were a many issues involved with tuition and not all of the overage would revert to the specific program.</p>
Revised Program Proposal Received	12/7/16	<p>The institution provided the following responses to questions and topics from CAAL and staff:</p> <ul style="list-style-type: none"> <li>• Additional workforce data for South Carolina on page 7.</li> <li>• A link for the policy of transfer of graduate credit on page 11.</li> <li>• A statement about USC Columbia and The Citadel as the only higher education institutions in South Carolina to be accredited by the National Security Agency and the Department of Homeland Security as National Centers of Academic Excellence in Information Assurance and Cyber Defense Education. The institutions are engaged already in joint curriculum development and have signed a MOU to facilitate course transfer and share in information assurance (p.11).</li> <li>• A statement was included in the budget justification to address the excess revenues of the program (p.18)</li> </ul>

**Review**

Proposal consideration focused on the need for the program, program delivery online, estimated enrollment, collaboration with other institutions in the state, transferability of courses, and a possible reduction of tuition. University representatives responded satisfactorily to questions and concerns at the CAAL meeting and in the revised proposal.

**Recommendation**

The Committee on Academic Affairs and Licensing recommends that the Commission approve the program leading to the Master Science in Information Security to be implemented in Spring 2017.



### **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 program objectives for the MSIS are:

- To train cyber security professionals to meet the needs of business, industry, educational institutions and government agencies of the state of South Carolina.
- To increase research capability in information security for the benefit of the state and nation.
- To provide knowledge of the latest techniques in cyber security for computer professionals in the state and offer excellent opportunities for professional advancement.

The learning objectives are as follows. 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.

This is in alignment with the increasing number of cyber security job postings that require significant education and experience. According to Burning Glass report on the growth of cyber security jobs (<http://burning-glass.com/wp-content/uploads/Burning-Glass-Report-on->

Cybersecurity-Jobs.pdf<http://burning-glass.com/wp-content/uploads/Burning-Glass-Report-on-Cybersecurity-Jobs.pdf> ), 6% of job postings explicitly require a Masters degree while 78% specify at least a Bachelors with four or more years of experience. The expectations are that the postings requiring a Masters degree are likely to increase further, considering that to develop secure software one has to acquire knowledge and skills beyond the fundamentals of programming languages and algorithms that are part of a Bachelors program.

The department has also received more than ten requests (we have not kept track of the exact number) for a Master-level program in information security from students and working professionals in and around Charleston and Columbia. These all indicate local and regional interest in the proposed program. Moreover, the Industrial Advisory Board (IAB) of the department has suggested in the past that such a program would benefit the state of SC. When the proposed MSIS was presented to the IAB last year, all members strongly agreed on the need of such a 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 <a href="http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm">http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm</a>
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 <a href="https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC)%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf">https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC)%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf</a>

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>).

According to a recent Burning Glass report on the growth of cyber security jobs (<http://burning-glass.com/infographic-geography-cybersecurity-jobs-2015/>), there were 2,312 postings for cyber security related jobs in South Carolina in 2015, with a 134% growth over the next years. Cybersecurity jobs are expected to grow at twice the rate of growth for all IT jobs. The most recent survey of Cyber Seek company (<http://cyberseek.org/heatmap.html>) shows 348,975 cybersecurity job openings nationally, and 3,301 positions in South Carolina. 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 <a href="http://www.citadel.edu/root/mathcs-programs/cyber-security-graduate-certificate">http://www.citadel.edu/root/mathcs-programs/cyber-security-graduate-certificate</a>	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 Graduate Certificate in Cyber Security Studies	Coastal Carolina University <a href="https://www.coastal.edu/science/departments/cs/majorsandminors/graduateprogram/">https://www.coastal.edu/science/departments/cs/majorsandminors/graduateprogram/</a>  University of South Carolina <a href="https://cse.sc.edu/graduate/ias">https://cse.sc.edu/graduate/ias</a>	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. 4. The 12 credit hours of coursework is similar to the core requirements of the proposed M.S. in Information Security (MSIS) program.	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. 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							TOTAL
	517	522	590	715	727	813	824	
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**

To be admitted to MSIS, 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 (which is expected to be 160 or higher in quantitative and 145 or higher in verbal), two letters of recommendation, and GPA (3.0 or higher).

**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
- Justification: The number of elective course credits provides students the flexibility to gather the requisite knowledge about specific domains to which they intend to apply security principles. For instance, CSCE 520 is a good elective for students interested in securing databases and similarly CSCE 516 for those interested in Internet security.

### **Additional information**

- Up to 12 hours of graduate credit may be transferred from another institution, according to Graduate School policy. Detailed description of the policy is given at the USC Bulletin, [http://bulletin.sc.edu/content.php?catoid=52&navoid=1287#Transfer\\_of\\_Course\\_Credit](http://bulletin.sc.edu/content.php?catoid=52&navoid=1287#Transfer_of_Course_Credit)
- The University of South Carolina and The Citadel are the only higher education institutions in South Carolina that have been accredited 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. The two

institutions have already engaged in joint curriculum development and have a signed Memorandum of Understanding to facilitate course transfer and sharing in information assurance.

Total Credit Hours Required: 30

**Program delivery method**

While we offer some of the courses through APOGEE, more than half of the courses that are part of this program will be offered through traditional instruction, since they require significant face time with the instructors and advisors.

**Course Descriptions for New Courses**

No new courses are being proposed.

**Faculty**

<b>Faculty and Administrative Personnel</b>				
<b>Rank</b>	<b>Full- or Part- time</b>	<b>Courses Taught or To be Taught, Including Term, Course Number &amp; Title, Credit Hours</b>	<b>Academic Degrees and Coursework Relevant to Courses Taught, Including Institution and Major</b>	<b>Other Qualifications and Comments (i.e., explain role and/or changes in assignment)</b>
Associate Professor	FT	CSCE 522 — Information Security Principles (3) <i>Fall 2015</i> CSCE 548 — Building Secure Software (3) <i>Spring 2012</i> CSCE 727 — Information Warfare (3) <i>Spring 2016</i> CSCE 813 — Internet Security (3) CSCE 824 — Secure Database Systems (3) <i>Spring 2016</i>	Ph.D Information Technology	Lead instructor for courses CSCE 522, 548, 727, and 824 <ul style="list-style-type: none"> <li>• CSCE 522 will be offered in every Fall</li> <li>• CSCE 548 will be offered in every Spring and/or summer</li> <li>• CSCE 727 will be offered in every 4<sup>th</sup> semester</li> <li>• CSCE 824 will be offered in every 4<sup>th</sup> semester</li> </ul>
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) <i>Spring 2016</i>	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. <ul style="list-style-type: none"> <li>• CSCE 557 will be offered in every 4<sup>th</sup> semester</li> </ul>
Assistant Professor	FT	CSCE 548 — Building Secure Software (3) CSCE 747 — Software Testing and Quality Assurance (3) <i>Spring 2016</i> CSCE 846 — Software Reliability and Safety (3)	Ph.D., Computer Science	Lead instructor for CSCE 747 and CSCE 846. <ul style="list-style-type: none"> <li>• CSCE 747 will be offered in every Spring semester</li> <li>• CSCE 846 will be offered in every 4<sup>th</sup> semester</li> </ul>
Associate Professor	FT	CSCE 715 — Network Systems Security (3) <i>Spring 2015</i> CSCE 813 — Internet	Ph. D., Computer Science	Lead instructor for CSCE 715 and CSCE 813. <ul style="list-style-type: none"> <li>• CSCE 715 will be offered in every Fall</li> </ul>

		Security (3) <i>Fall 2015</i>		semester <ul style="list-style-type: none"> <li>CSCE 813 will be offered in every 4<sup>th</sup> semester</li> </ul>
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. <ul style="list-style-type: none"> <li>CSCE 719 will be offered in every 4<sup>th</sup> semester</li> </ul>
System Administrator	FT	CSCE 517 — Computer Crime and Forensics (3) <i>Summer 2015</i>	M.S., Computer Science and Engineering	Lead instructor for CSCE 517. <ul style="list-style-type: none"> <li>CSCE 517 will be offered in every summer semester</li> </ul>

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)

All graduate students, including MSIS students, will be supported by the graduate director and graduate program coordinator. Each student is advised by the graduate director prior to enrolling in courses each semester. The graduate program coordinator will act as a liaison to the Graduate School and assist the students in completing the necessary paperwork from matriculation to graduation. All these services are already available and 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 instructional equipment 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)



The Department of Computer Science and Engineering is located in a three-storied building with two floors of classrooms and instructional labs. It maintains four instructional labs populated with Windows and Linux machines. The department maintains its own web server and file servers, and the two college Windows labs run Xwin32 software to permit access to the Linux environment from those labs. Access from off-campus and through the college-wide wireless network is also routinely done by both students and faculty. The University of South Carolina maintains a high speed network inside the campus and is an Internet2 member. All these existing facilities will be available to MSIS students and no new facilities are needed.

Financial Support

Estimated New Costs by Year						
Category	1 <sup>st</sup>	2 <sup>nd</sup>	3 <sup>rd</sup>	4 <sup>th</sup>	5 <sup>th</sup>	Total
Program Administration  A 3% increase/year is calculated after the 1 <sup>st</sup> 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*						
<b>Total</b>	<b>101,927</b>	<b>104,925</b>	<b>108,013</b>	<b>111,193</b>	<b>114,469</b>	<b>540,527</b>
Sources of Financing						
Category	1 <sup>st</sup>	2 <sup>nd</sup>	3 <sup>rd</sup>	4 <sup>th</sup>	5 <sup>th</sup>	Total
Tuition Funding (21 credits/student /year, \$516 per hour for instate tuition and \$1,105.5 for others)	136,206	175,365	216,751	260,463	268,277	1,057,062
# of students enrolled	Instate: 4 Out-of-state: 4	Instate: 5 Out-of-state: 5	Instate: 6 Out-of-state: 6	Instate: 7 Out-of-state: 7	Instate: 7 Out-of-state: 7	
<b>Net Total (i.e., Sources of Financing Minus Estimated New Costs)</b>	<b>34,279</b>	<b>70,440</b>	<b>108,738</b>	<b>149,270</b>	<b>153,808</b>	<b>516,535</b>

\*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 in-state 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.

The revenues of the proposed program are expected to exceed costs. Not all University programs are equally revenue-positive. A key value of a University is its management of the complex resource balance among academic programs of all types, sizes, and degree levels, whereby essential smaller programs can be sustained because of successful programs.

### **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 3<sup>rd</sup> 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. To this end, we will survey the employers and our industrial advisory board members about the quality of our graduates. 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.