UNC CHARLOTTE
College of Computing and Informatics
Office of the Dean

9201 University City Boulevard, Charlotte, NC 28223-0001
t/ 704.687.8450 f/ 704.687.6979 www.cci.uncc.edu

Date: June 3, 2016

Courtney Thornton
AVP for Academic Programs
University of North Carolina

Ms. Thornton,

We thank the reviewers for their detailed comments regarding our Request to Establish the M.S. in Cyber Security. In this letter I respond to their comments and how we have modified our proposal in response.

We have added additional explanation to Appendix C regarding our laboratory requests:

While we will utilize existing online cybersecurity testbeds and simulations in courses as appropriate, we believe existing cloud infrastructures are not appropriate as the foundation for our proposed security labs as we must have extra protection built in to make sure students will not accidentally cause harm to others on the Internet, or generate network traffic that may appear to be suspicious. We believe the best way to achieve this is to create our own physical laboratories for these purposes, extending our current capabilities to meet the needs for additional graduate students.

As the reviewer noted, there are a variety of online resources available, many of these simulate certain kinds of security problems or environments. While we will certainly utilize these as appropriate in our courses, we still believe that the addition of two physical laboratories, expanding upon our current capabilities, will provide students with the kind of hands-on, real world experiences that are required in this subject area. Additionally, we have added a note about how we involve industrial participants in competitions, which serve to improve upon our laboratory exercises:

We will help to ensure the breadth and depth of projects and exercises utilizing these laboratories using a model of open competition. As tradition in our annual security symposium (organized since 2001), we have a "capture the flag" style competition with both industry and student participants. Materials developed every year for the competition will be utilized to improve and update our security laboratories. Feedback from industry participants helps keep these exercises up to date with the latest security developments.

We appreciate the concern over low enrollments due to having 3 concentrations. However, we should note that each of our courses already has sufficient enrollment to be offered at least yearly,

and our new program will only increase that enrollment. We believe it is important to allow students to specialize in our 2 security concentrations which are quite different (network security, and secure software development), and in addition, offer 1 concentration that is customizable and flexible to meet students' personal interests (the concentration in emerging technology).

The department does have a graduate certificate in "Information Security and Privacy", as well as 2 other security graduate certificates. Graduate certificates serve a different purpose to the Master's degree, attracting students who do not wish to pursue a full degree program, but who wish for specialized and focused training in security. Each of these graduate certificates is indeed a subset of courses from the proposed Master's in Cyber Security. We have kept the names of our graduate certificates different from the name of the Master's program so that students would not accidentally apply to a certificate (which has different admissions requirements) if they meant to apply for a Master's degree, and vice versa.

Sincerely,

Yi Deng, Ph.D.
Dean and Professor

UNC CHARLOTTE

Office of the Chancellor

9201 University City Boulevard, Charlotte, NC 28223-0001
t/ 704.687.5700 f/ 704.687.1700 www.uncc.edu

January 27, 2016

Dr. Chris Brown
Vice President for Research and Graduate Education
University of North Carolina
Post Office Box 2688
Chapel Hill, North Carolina 27515-2688

Dear Dr. Brown:

Enclosed is UNC Charlotte's request for authorization to establish a M.S. in Cyber Security. Building on the existing cyber security education and research programs at UNC Charlotte that have been recognized by the National Security Agency and the National Science Foundation, this new program will prepare graduates to work in the high-demand field of cyber security and privacy across a wide array of industries including business, healthcare, banking and energy.

Thank you for your consideration of this request. Provost Joan Lorden or I would be pleased to respond to any questions that you may have.

Cordially,

Philip L. Dubois
Chancellor

cc: Joan F. Lorden, Provost and Vice Chancellor for Academic Affairs
Yi Deng, Dean, College of Computing and Informatics
Courtney Thornton, Associate Vice President for Research and Graduate Education
Cody Thompson, Coordinator for Academic Planning

APPENDIX C

UNIVERSITY OF NORTH CAROLINA

REQUEST FOR AUTHORIZATION TO ESTABLISH A NEW DEGREE PROGRAM

INSTRUCTIONS: Each proposal should include a 2-3 page executive summary. The signature of the Chancellor is required. Please submit one hard copy and an electronic copy of the proposal to the Office of the Senior Vice President of Academic Affairs at UNC General Administration.

Date: ___June 3, 2016_____

Constituent Institution: The University of North Carolina at Charlotte

CIP Discipline Specialty Title: Computer & Information Sciences

CIP Discipline Specialty Number: ___11.1003 Level: B _____ M _X_ Res. Doc. _____ Prof. Doc. _____

Exact Title of the Proposed Program: Cyber Security

Exact Degree Abbreviation (e.g., B.S., B.A., M.A., M.S., Ed.D., Ph.D.): M.S.

Does the proposed program constitute a substantive change as defined by SACS? Yes

> The current SACS Substantive Change Policy Statement may be viewed at:
> *http://www.sacscoc.org/pdf/081705/Substantive%20Change%20policy.pdf*

If yes, please briefly explain.

> As required by the Policy Statement on Substantive Change for Accredited Institutions of the Commission on Colleges, the University of North Carolina at Charlotte (UNC Charlotte) is required to submit a letter of notification prior to implementation for new degree programs. Notification of this new degree program will be provided to SACS after approval by the University of North Carolina Board of Governors and prior to implementation.

Proposed date to enroll first students in degree program: January 2017

Are there plans to offer 50% or more of program credit hours to students off-campus or online? No

If yes, complete the form to be used to request establishment of a distance education program and submit it along with this request.

Note: If a degree program has not been approved by the Board of Governors, its approval for alternative, online, or distance delivery must wait until BOG program approval is received. (400.1.1[R], page 3)

Provide a summary of the status of this proposal in your campus review processes.

a. List the campus bodies that reviewed and commented on this Appendix C proposal before submission to UNC General Administration. What were there determinations? Include any votes, if applicable.

This proposal has been reviewed by the following campus bodies. All these bodies have approved the proposal unanimously.

- The graduate curriculum committee of the Department of Software and Information Systems
- The Department of Software and Information Systems
- The graduate committee of the College of Computing and Informatics
- The graduate council of UNC Charlotte

b. Summarize any issues, concerns or opposition raised throughout the campus process and comment periods. Describe revisions made to address areas of concern.

No major issues were raised during the consultation process.

Executive Summary

The Department of Software and Information Systems, in the College of Computing and Informatics at the University of North Carolina at Charlotte, requests authorization to establish a Master of Science degree in Cyber Security. This program complements the Master of Science in Information Technology degree currently offered by the department, enhancing our ability to educate students in state of the art knowledge and skills that are essential to safeguard the nation's information and computing assets. The specific objectives of the program include a fundamental understanding of common security vulnerabilities of computing and networked systems and methods to attack those systems; the ability to analyze and evaluate the security and privacy risks in information systems and networks; and the ability to design and implement information systems with security controls to minimize security and privacy risks.

President Obama has declared that the "cyber threat is one of the most serious economic and national security challenges we face as a nation" and that, "America's economic prosperity in the 21st century will depend on cyber-security." As a result of these challenges, the field of cyber security is experiencing rapid growth, with the demand for skilled professionals outpacing availability. Cyber security is projected to grow fastest among all major STEM occupations, with jobs across a variety of sectors, such as technology, healthcare, financial services, and government. Cyber security postings in the Charlotte region reflect this growth, with 147% growth from 2010-2014. The proposed Master of Science degree in Cyber security will provide the in-depth training and knowledge required for many of these positions. There are no similar graduate degree programs in the State of North Carolina.

The Department of Software and Information Systems has been building capacity in cyber security education and research for the past 15 years. The department has been recognized by the National Security Agency (NSA) and the National Science Foundation (NSF) as a Center of Excellence in Information Assurance Education and Research for the past decade. Faculty from the department include internationally recognized experts in cyber security whose research results are widely cited by peers and have also been adopted as international standards for data security. The department has also been a participant in NSF/Department of Defense Cyber Security Scholarship for Service programs during the past decade years, and has graduated over 60 master's students who have all been hired by federal government agencies.

The proposed Master of Science degree in Cyber Security expands upon the department's current programs by providing even greater depth in the area of security. The current MS in Information Technology trains students in advanced software design and development and computing technologies, and offers a concentration in cyber security consisting of three courses. The department also offers a graduate certificate in information security, which is comprised of five courses. The proposed MS in Cyber Security involves at least nine courses in cyber security, including a culminating project experience. This increased depth will attract students who desire careers in cyber security, and will provide focused and deep training and skills in analyzing and protecting computing and information systems from security risks and vulnerabilities. The proposed degree is composed of a common core of four courses, with three concentrations reflecting depth in a specific area within cyber security including network security and secure software development. Students will also have the option to pursue advanced research with a Master's thesis. The department currently offers 13 courses in cyber security, requiring no additional courses to establish the degree. We expect that as enrollment grows, we will continue to expand and improve the courses and course offerings.

I. Description of the Program

A. Describe the proposed degree program (i.e., its nature, scope, and intended audience).

The Department of Software and Information Systems (SIS), in the College of Computing and Informatics at UNC Charlotte proposes to add a new Master of Science in Cyber Security program. The program will be open to both full time students and part-time professionals. The program targets both recent graduates of computing bachelor's programs, as well as current computing professionals. We are particularly interested in attracting computing professionals in the region who are interested in deepening their education in cyber security to pursue a career in security.

B. List the educational objectives of the program.

The Master of Science in Cyber Security is designed to equip students with the latest knowledge and skills in cyber security and privacy. Graduates of the program will be employable by both businesses and governments that have important information assets to be protected from increasingly sophisticated cyber-attacks.

Specific educational objectives of the program include:

- A fundamental understanding of:
  - common vulnerabilities of computing and networked systems,
  - cyber-attacking methods,
  - human and organizational aspects of cyber security,
  - methods for compromising privacy, and
  - risk assessment of cyber-attacks.
- Able to apply security techniques to analyze and evaluate the security risk of information systems and networks.
- Able to design information systems and networks with security controls to minimize security risks.

The program requires students take four core courses, three concentration courses, and three elective courses. The core courses are designed to prepare students with fundamental knowledge and skills in cyber security and privacy protection that are essential to all cyber security professionals. The concentration courses give students an opportunity to specialize in network security, secure software development, or emerging technologies. Elective courses give students an opportunity to further broaden their knowledge and skills in areas that are of particular interest to them. Together these three components will equip students with necessary skill sets in specific areas in cyber security and privacy where they wish to pursue their professional careers.

C. Describe the relationship of the program to other programs currently offered at the proposing institution, including the common use of:

1. Courses
2. Faculty
3. Facilities, and
4. Other resources

The Master of Science in Cyber Security will complement the Master of Science in Information Technology program offered at UNC Charlotte. Although the Master of Science in Information Technology offers a concentration in information security and

privacy, students in that program generally take four courses in information security and privacy which makes it difficult for students to have a deep understanding of rapidly expanding knowledge and skills in cyber security. The new program will require students to take at least nine courses in cyber security and privacy so that they are well equipped with state of the art skills in the area that is essential in safe-guarding information assets.

Enrollment of international students in the existing the Master of Science in Information Technology program has been growing at a pace far greater than that of domestic students. On the other hand, domestic students have historically shown more interest in information security. The new Master's program in cyber security will be able to attract more native North Carolina students into the graduate program, resulting in a more diverse and balanced graduate student body with interests in employment in the state.

The program will use existing courses. Courses for the new program will be open to students in other graduate programs from the College and the University including the existing Master of Science in Information Technology program. They will be taught by the same faculty that teach courses for other graduate programs offered by the Department. Facilities and library resources will also be shared.

II. Justification for the Program – Narrative Statement

A. Describe the proposed program as it relates to:

1. Institutional mission

The proposed Master of Science in Cyber Security closely aligns with the UNC Charlotte mission as North Carolina's urban research university. It strongly supports the University's focus on community engagement, graduate education, and the economic and social needs of the greater Charlotte region. Cyber security has been identified as a critical need in the major industries of the Charlotte region, including healthcare[1][2], energy[3][4], and financial services[5]. The program also aligns with the missions of the Department of Software and Information Systems (SIS) and College of Computing and Informatics (CCI). The Master's program is built upon a strong record of faculty achievement in the areas of cyber security and privacy.

The University is committed to growing graduate programs in areas of national, state, and regional need. The proposed program will help address an increasingly strong demand for employees with information and network security knowledge and skills. Further, it aligns well with growing national security needs in safeguarding the nation against emerging threats emanating from the cyber space. President Obama has declared that the "cyber threat is one of the most serious economic and national security challenges we face as a nation" and that, "America's economic prosperity in the 21st century will

[1] http://www.information-age.com/technology/security/123460052/why-healthcare-industry-badly-needs-cyber-security-health-check

[2] http://www.techrepublic.com/article/cybersecurity-professionals-the-healthcare-industry-needs-you/

[3] https://securityintelligence.com/should-the-energy-production-industry-consider-cybersecurity/

[4] http://energy.gov/oe/services/cybersecurity

[5] http://www.thinkadvisor.com/2014/11/25/top-10-cybersecurity-trends-for-financial-services

depend on cyber-security." According to Steve Rosenbush, the Deputy Editor of the CIO journal belonging to the Wall Street Journal, the demand for cyber security experts is growing at 3.5 times the pace of the overall IT job market, and 12 times the overall job market. Because of the sensitivity of responsibilities in cyber security, many of these jobs cannot be out-sourced. At the same time, economic drivers in the Charlotte region such as the power and financial service industries have been frequent targets of cyber-attacks. The proposed degree addresses the need for a skilled cyber security workforce. The program is designed to ensure that students are well equipped for employment in a wide variety of industries including financial services, energy, retail/supply chain and health care where data and infrastructure security and safety are of paramount importance.

2. Strategic plan

The proposed program aligns with the College and Department strategic plans to expand and grow the number of students completing degrees in cyber security. The proposed Master of Science in Cyber Security will complement the Master of Science in Information Technology program offered at UNC Charlotte. Although the Master of Science in Information Technology offers a concentration in information security and privacy, students in that program generally take four courses in information security and privacy, which makes it difficult for students to acquire a deep understanding of the rapidly expanding knowledge and skills in cyber security. The new program will require students to take at least nine courses in cyber security and privacy to better equip them with state of the art knowledge and skills in the areas that are essential in safe-guarding information assets.

The proposed program aligns with the College and Department strategic plan to increase diversity in the graduate student body, and to specifically attract more students from the Charlotte region. Enrollment of international students in the existing the Master of Science in Information Technology program has been growing at a pace far greater than that of domestic students (see Section 3 for details). On the other hand, domestic students have historically shown more interest in information security. The new Master of Science in Cyber Security will attract more domestic students into the graduate programs of the College of Computing and Informatics, resulting in a more diverse and balanced graduate student body.

3. Student demand. Provide any update to the documented evidence of student demand presented in Appendix A.

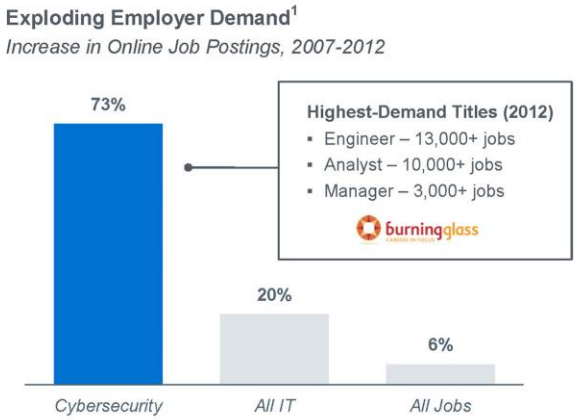
The proposed program will help address an increasingly strong demand for employees with information and network security knowledge and skills. Further it aligns very well with growing national security needs in safeguarding the nation against emerging threats emanating from the cyber space. At the regional level, economic driving forces in the Charlotte region such as power and financial service industries have been a primary target of cyber-attacks. The proposed Master's degree addresses this need in a timely manner. The program is designed to ensure that graduates are all well equipped for employment in a wide variety of industries ranging from financial services, energy and retail/supply chain to health care where security and privacy is of paramount importance.

The department surveyed IT professionals attending the Charlotte Security Symposium to determine their interest in the new MS in Cyber Security in October 2015 (survey is attached, see Attachment E). The survey was distributed on paper during the opening session to approximately 400 attendees, and 71 returned the survey. When asked if they would recommend the MS in Cyber Security to a colleague or employee, 95% said

they were likely to do so. When asked if they would enroll in the MS in Cyber Security, 73% said they were likely to enroll.

4. Societal demand and employability of graduates. Provide any update to the documented evidence of societal demand and employment opportunities presented in Appendix A.

At the 2015 Cybersecurity Symposium in Charlotte, the group technology manager for Wells Fargo & Company cyber security defense and monitoring group told the audience that there is a shortage of talent in cybersecurity[6]. The Education Advisory Board echoes this sentiment, stating, "Cyber security is one field where the demand is far outpacing the number of skilled professionals available," with a 73% growth in cyber security jobs from 2007 to 2012.



Source: https://www.eab.com/research-and-insights/continuing-and-online-education-forum/studies/2014/hyperstackable-emerging-careers

According to the US Department of Labor Bureau of Labor Statistics, employment in information security jobs is "projected to grow 37 percent from 2012 to 2022, much faster than the average for all occupations. Demand for information security analysts is expected to be very high" (retrieved from NCWorks.gov on June 2, 2014[7]). Of this 37% employment growth for the information security profession between 2012 and 2022, the Bureau of Labor Statistics estimates 27,400 new jobs will need to be filled in the industry.

"Occupational Outlook Quarterly" projects in its Spring 2014 issue that demand for information security analysts (i.e. cyber security professionals) will grow the fastest among all major STEM occupations. Demand for information security analysts is expected to be very high as these analysts will be needed to come up with innovative solutions to prevent hackers from stealing critical information or creating havoc on computer networks.

[6] http://www.bizjournals.com/charlotte/blog/bank_notes/2015/10/wells-fargo-exec-there-is-a-shortage-of-talent-in.html

[7]https://www.ncworks.gov/vosnet/lmi/occ/occsummary.aspx?enc=tVxpoeFornWSIu9Am4p9B7Ht3tFejby8t8OLBPJZB2Nl6LC5AJykT47NC/3UNpGHx2+IJ+xxV70K9H9qUWa5hNN+kqZ7TSC23EczjuSsinI

Occupation	Employment growth, projected 2012–22 (percent)	Employment		Median annual wage, May 2013
		2012	Projected 2022	
Information security analysts[2]	37%	75,100	102,500	$88,590
Operations research analysts	27	73,200	92,700	74,630
Statisticians	27	27,600	34,900	79,290
Biomedical engineers	27	19,400	24,600	88,670
Actuaries[3]	26	24,300	30,600	94,340
Petroleum engineers	26	38,500	48,400	132,320
Computer systems analysts	25	520,600	648,400	81,190
Software developers, applications	23	613,000	752,900	92,660
Mathematicians	23	3,500	4,300	102,440
Software developers, systems software	20	405,000	487,800	101,410
Computer user support specialists[4]	20	547,700	658,500	46,620

Source: Occupational Outlook Quarterly (www.bls.gov/ooq), Spring 2014

B. Provide any update to the discussion of similar degree programs and opportunities for collaboration presented in Appendix A. Discuss here the feasibility of a joint or collaborative degree program with one or more UNC institutions.

There is no update on the discussion of similar degree programs and opportunities for collaboration presented in Appendix A.

The SIS Department has had a long collaborative relationship with North Carolina A&T, the largest historically black university in the nation, in cyber security education. For a number of years, the department and the Computer Science Department at North Carolina A&T were a joint recipient of cyber security education scholarship grants from the National Science Foundation (NSF) and the Department of Defense (DoD). We anticipate that the collaborative relationship can be further extended to the Master of Science in Cyber Security.

C. Enrollment (baccalaureate programs should include only upper division majors, that is, juniors and seniors).

Please indicate the anticipated first year and fourth year steady-state enrollment (head count) for the proposed program.

Year 1: Full Time ___20__ Part-time _10_____ Total __35_____

Year 4: Full-time ___80___ Part-time ___20_____ Total __100___

III. Program Requirements and Curriculum

A. Program Planning

1. List the names of institutions with similar offerings regarded as high quality programs by the developers of the proposed program.

Masters Programs in Cyber Security Student Enrollment, Fall 2013	
University	**Enrollment**
University of Maryland M.S. in Cyber Security	1340
DePaul M.S. in Computer, Information & Network Security	174
Northeastern University M.S. in Information Assurance	140
Boston University M.S. in Computer Information Systems (Security)	137
NYU-Poly M.S. in Cybersecurity	111
George Mason University Masters In Information Security & Assurance	76
Johns Hopkins M.S. in Security Informatics	57
George Washington University M.S. in Cybersecurity in Computer Science	29

2. List institutions visited or consulted in developing this proposal. Also discuss or append any consultants' reports or committee findings generated in planning the proposed program.

In addition to the above eight universities, the Office of Institutional Research at UNC Charlotte called Stevens Institute, Wright University, University of Southern California, New Jersey Institute of Technology, Indiana University, Iowa State University, Illinois Institute of Technology and University of Houston. Recent data on graduate degrees or certificates in areas related to cyber security were collected where possible. Analysis of this data indicates that there is a growing demand for cyber security professionals across the nation. The data were also used as reference points in producing our (conservative) estimates of enrollments for this proposed program for the first few years.

B. Admission. List the following:

1. Admissions requirements for proposed program (indicate minimum requirements and general requirements).

Students entering the Master of Science in Cyber Security program are required to have completed a baccalaureate degree from an accredited institution of higher learning and have acquired substantial experience in studying, applying, or developing information and computing technology. Such experience may be developed by completing an undergraduate major in a discipline related to information technology, including but not limited to: business information systems, computer engineering, computer science, data communication, information management, information technology, mathematical and physical sciences, and software engineering. For applicants who have an undergraduate major not directly related to computing, the experience may be acquired through work, professional training, or further education such as graduate certificates or post baccalaureate studies

For admission to the Master's degree program, applicants must meet both Graduate School and program specific requirements, including submission of official test scores from the Graduate Record Examination (GRE) or the Graduate Management Admission Test (GMAT). Full details on Graduate School requirements, including requirements regarding test scores, can be found in the most recent version of the Graduate Catalog. Admission requirements specific to the program include:

1) Applicants must have completed undergraduate or equivalent coursework in (a) data structures, (b) object-oriented programming in C++, C#, or java, (c) databases, (d) computer networks and (e) web application development, all with a minimum GPAs of 3.0 on a 4.0 scale. Applicants who have substantial work experience in applying or developing computing and information technology may be able to substitute their work experience for the above specific requirements, subject to review by the Program Coordinator.
2) All applicants must have an undergraduate GPA or equivalent of at least 3.0 on a scale of 1.0 to 4.0, and a Junior/Senior GPA of at least 3.0.
3) All applicants are required to submit a statement of purpose as well as letters of recommendation.

2. Documents to be submitted for admission (listing or attach sample).

Required documents to be submitted for admission include copies of transcripts, GRE scores, references and a statement of purpose.

C. Degree requirements. List the following:

1. Total hours required. State requirements for Major, Minor, General Education, etc.

Students are required to complete 30 credit hours for the Master's degree, of which (a) 12 are for 4 common core courses, (b) 9 are for depth in a particular area of cyber security, and (c) 9 are for electives in security and computing and information technology.

30 credit hours for the degree		
12 credit hours (=4 courses) for common core	9 credit hours (=3 courses) for concentration	9 credit hours (=3 courses) for electives

(a) Students are required to complete the following four common core courses (12 credit hours):

- ITIS 5250 Computer Forensics (3 credit hours)
- ITIS 6167 Network Security (3 credit hours)
- ITIS 6200 Principles of Information Security and Privacy (3 credit hours)
- ITIS 6240 Applied Cryptography (3 credit hours)

(b) Students are required to complete one of the following concentrations (9 credit hours). Students pursuing a MS thesis will use 6 credit hours towards their concentration in place of coursework.

Network Security Concentration:

- ITIS 6230 Information Infrastructure Protection (3 credit hours)
- ITCS 6166 Computer Communications and Networks (3 credit hours)
- Three credit hours of security elective

Secure Software Development Concentration:

- ITIS 5221 Secure Programming and Penetration Testing (3 credit hours)
- ITIS 6150 Software Assurance (3 credit hours)
- ITCS 6114 Algorithms and Data structures (may be substituted by a security elective based on an approved undergraduate CS algorithm course)

Security for Emerging Technology

- Nine credit hours of courses to achieve a clearly defined security theme. Must be under the direction of a member of CCI graduate faculty with program approval.

  For example: a theme of Cloud Data Security
  - ITIS 6220 Data Privacy (3 credit hours)
  - ITIS 6230 Information Infrastructure Protection (3 credit hours)
  - ITIS 6320 Cloud Data Storage (3 credit hours)

(c) Students are required to complete two additional courses as security electives from the following list.

- ITIS 5221 Secure Programming and Penetration Testing (3 credit hours)
- ITIS 6150 Software Assurance (3 credit hours)
- ITIS 6210 Access Control and Security Architecture (3 credit hours)
- ITIS 6220 Data Privacy (3 credit hours)
- ITIS 6230 Information Infrastructure Protection (3 credit hours)
- IT IS 6250 Open Source Security Systems (3 credit hours)

- ITIS 6320 Cloud Data Storage (3 credit hours)
- ITIS 6362 Information Technology Ethics, Policy, and Security (3 credit hours)
- ITIS 6420 Usable Security and Privacy (3 credit hours)
- ITIS 6880 Independent study for a security topic (may be repeated but only 3 credit hours can count towards the degree).
- ITIS 6999 SFS Research (may be repeated but only 3 credit hours can count towards the degree)

CCI Elective
Students may complete any additional course offered by the College of Computing and Informatics for their remaining elective.

Three of the nine credit hours for electives may be substituted by an approved IT Internship, which also serves as a capstone project.

2. Other requirements (e.g. residence, comprehensive exams, thesis, dissertation, clinical or field experience, "second major," etc.).

Students have three options to complete the 30-credit hour program:

1. Coursework + Master's Thesis: 24 hours of course work plus 6 hours of Master's research thesis project,
2. Coursework + Internship: 27 hours of course work plus 3 credit hours of an approved IT Internship, or
3. Coursework + capstone report: 30 hours of course work and a capstone report.

The thesis option requires the formation of a program committee. The thesis option requires students to perform research under the supervision of an academic advisor, submit a written thesis and orally defend their work before their program committee. Students must enroll in 2 semesters of ITIS 6991 Information Technology Thesis (3 credit hours).

The internship option requires enrollment in ITIS 6198 IT Internship Project (3 credit hours) Completion of this courserequires approval by the program director of an internship location and preceptor, and the submission of a written internship report.

All students selecting the capstone report option are required to complete 30 credits of coursework and successfully complete a report describing a project experience in cyber security to fulfill the requirements of a culminating experience for the Master's degree. The report will be submitted to and approved by the Graduate Coordinator.

For graduate programs only, please also list the following:

3. Proportion of courses open only to graduate students to be required in program

At least 15 semester hours of the 30 required semester hours must be in courses numbered 6000 or above. Courses numbered 6000 and above are only open to graduate students.

4. Grades required

   A student in the Master's program must maintain a minimum GPA of 3.0 for continued enrollment in the program. Accumulation of three C grades will result in the suspension of the student's enrollment in the program. Accumulation of one unsatisfactory (U) grade will result in the suspension of the student's enrollment in the program.

5. Amount of transfer credit accepted

   At most six credits of approved course work taken at another institution or from another program prior to admission to the Master's program. Only courses in which the student earned a grade of B or better may be transferred.

6. Language and/or research requirements

   Students who choose the Master's Thesis option will complete a thesis and a thesis defense. There is no language requirement.

7. Any time limits for completion

   Time limits are described in the UNC Charlotte Graduate Catalog: "University policy requires that no course listed on a Master's student's candidacy form be older than six years at the time of graduation. This policy is in place because of the University's interest in a degree being current when it is awarded. Courses that exceed this time limit must be revalidated or retaken, whichever the graduate program decides is necessary, if they are to count in a degree program."

D. For all programs, list existing courses by title and number and indicate (*) those that are required. Include an explanation of numbering system. List (under a heading marked "new") and describe new courses proposed.

The following 4 existing courses form the common core for the Master's program:

- ITIS 5250 Computer Forensics (3 credit hours) *
- ITIS 6167 Network Security (3 credit hours) *
- ITIS 6200 Principles of Information Security and Privacy (3 credit hours) *
- ITIS 6240 Applied Cryptography (3 credit hours) *

In addition, the department offers the following courses in cyber security:

- ITIS 5221 Secure Programming and Penetration Testing (3 credit hours)
- ITIS 6150 Software Assurance (3 credit hours)
- ITIS 6210 Access Control and Security Architecture (3 credit hours)
- ITIS 6220 Data Privacy (3 credit hours)
- ITIS 6230 Information Infrastructure Protection (3 credit hours)
- IT IS 6250 Open Source Security Systems (3 credit hours)
- ITIS 6320 Cloud Data Storage (3 credit hours)
- ITIS 6362 Information Technology Ethics, Policy, and Security (3 credit hours)
- ITIS 6420 Usable Security and Privacy (3 credit hours)

All the 6000 level courses are for graduate students only; 5000 level courses are cross-listed as upper level undergraduate courses.

IV. Faculty

A. (For undergraduate and Master's programs) List the names, ranks and home department of faculty members who will be directly involved in the proposed program. The official roster forms approved by SACS may be submitted. For Master's programs, state or attach the criteria that faculty must meet in order to be eligible to teach graduate level courses at your institution.

At UNC Charlotte, faculty teaching graduate level courses must have the terminal degree awarded in their field, or demonstrated equivalent education or experience. For cyber security this means a Ph.D. in a computing or a security oriented field. There are a significant number of existing faculty members from the UNC Charlotte Department of Software and Information Systems who will be directly involved and serve as the main faculty body in the proposed program. These faculty members offer cutting edge knowledge and expertise in cyber security. In addition, industry practitioners with appropriate credentials, including those from Bank of America, Wells Fargo, IBM, TIAA-CREF, Vanguard and other corporations in the region, will be invited to serve as adjunct faculty for the program on an as-needed basis. The table below shows the list of current faculty members who will teach the cyber security courses for the proposed Master's program. The faculty roster is attached as Appendix F.

Faculty Name	**Title**	**Department**
Dr. Ehab Al-Shaer	Professor	SIS
Dr. Bill Chu	Professor	SIS
Dr. Heather Lipford	Associate Professor	SIS
Dr. Mohamed Shehab	Associate Professor	SIS
Dr. Meera Sridhar	Assistant Professor	SIS
Dr. Weichao Wang	Associate Professor	SIS
Dr. Yongge Wang	Associate Professor	SIS

B. (For doctoral programs) List the names, ranks, and home department of each faculty member who will be directly involved in the proposed program. The official roster forms approved by SACS may be submitted. Provide complete information on each faculty member's education, teaching and research experience, research funding, publications, and experience directing student research including the number of theses and dissertations directed.

C. Estimate the need for new faculty for the proposed program over the first four years. If the teaching responsibilities for the proposed program will be absorbed in part or in whole by the present faculty, explain how this will be done without weakening existing programs.

We plan to request one new faculty position in cyber security in the first year of the new MS and up to three new faculty over the first four years of the program, depending on program growth. These faculty will contribute to both the MS in cyber security and the PhD program in Computing and Information Systems. Currently the Department has the following demographics:

- 16 tenure-track faculty and three non-tenure-track faculty
- Two administrative support positions
- 330 BA students
- 223 MSIT students for Fall 2015
- 55 PhD students

The request for new faculty positions will be based on enrollment in the MS and expansion of our research capacity in cyber security. Additional faculty will ensure that our existing MSIT programs and this proposed new Master of Science in Cyber Security are delivered at the highest quality.

D. Explain how the program will affect faculty activity, including course load, public service activity, and scholarly research.

The program will not have significant impact on faculty's course load, service and scholarly research. There is currently capacity for additional enrollment in existing cyber security courses to support the introduction of the program. As the program grows, we will add additional sections and course offerings to accommodate increases in enrollment. We do not anticipate the program will impact enrollment in the current MSIT degree offered by the department, other than a few students who would have pursued the current degree with a concentration in security and will instead enroll in the new program.

V. Library

A. Provide a statement as to the adequacy of present library holdings for the proposed program to support the instructional and research needs of this program.

See Attachment C. Current monograph and journal holdings are adequate to support the proposed program.

B. State how the library will be improved to meet new program requirements for the next four years. The explanation should discuss the need for books, periodicals, reference material, primary source material, etc. What additional library support must be added to areas supporting the proposed program?

Existing library resources are adequate for the program.

C. Discuss the use of other institutional libraries.

The library's participation in an interlibrary loan consortium provides another means of effectively supporting research and instructional needs.

VI. Facilities and Equipment

A. Describe facilities available for the proposed program.

The College of Computing and Informatics has three large computer labs dedicated to teaching. It has an additional lab for teaching hands-on teaching and learning in computer networking. The same lab also has the capacity of being isolated for the purpose of carrying out cyber security related exercises and experiments by students. Details of existing laboratory facilities are below.

Available Laboratories and Facilities for the Proposed Master's Program	
College of Computing and Informatics	
Name	**Description**
Teaching Laboratories:	
CCI General Purpose Computer Lab	General teaching lab equipped with desk top computers available to all college students, 1945 sq. ft., Woodward Hall.
Introduction to Computer Science Lab	Hands-on teaching lab for introduction to computer science courses, ~1000 sq. ft., Woodward Hall
Computer Teaching Labs	Three (3) teaching labs equipped with Apple Mac desktops for teaching and class projects, in the Bioinformatics Building. Over 3000 sq. ft.
Cyber Corps Lab	Computer security laboratory, 400 sq. ft.
Information and Infrastructure Security Lab	28 workstations and 80 networking devices dedicated for Cyber security lab assignments. The lab is isolated from the Internet so penetration testing and other experiments can be conducted.
Computer Forensics Lab	20 iMac workstations equipped with a variety of forensic software.

In addition to these teaching labs, all faculty members have active research programs and have computing equipment for research, part of which may be used by students in the new program who will work with faculty on specific research projects. Finally, the university has an extensive collection of high performance computing facilities some of which may be employed for the purpose of teaching classes for students in the new program.

B. Describe the effect of this new program on existing facilities and indicate whether they will be adequate, both at the commencement of the program and during the next decade.

A one-time investment in establishing two cyber security laboratories, one in Network Security and the other in Malware Analysis, will be needed. The amount needed is $60,000 ($30,000 for each laboratory), including support for equipment, networking and required software. The primary reasons for the request are as follows:

- A quality cyber security program must provide students with adequate opportunities for hands-on experience.
- Due to the nature of cyber security, most of the projects to be carried out by students must be conducted in an isolated computing environment so that impact of accidents is controlled and confined. Currently the department has an infrastructure laboratory that is extensively used by undergraduate classes. It will be inadequate to cater for the needs of the proposed Master's program.
- While we will utilize existing online cybersecurity testbeds and simulations in courses as appropriate, we believe existing cloud infrastructures are not appropriate as the foundation for our proposed security labs as we must have extra protection built in to make sure students will not accidentally cause harm to others on the Internet, or generate network traffic that may appear to be suspicious. We believe the best way to achieve this is to create our own physical laboratories for these purposes, extending our current capabilities to meet the needs for additional graduate students.
- We will help to ensure the breadth and depth of projects and exercises utilizing these laboratories using a model of open competition. As tradition in our annual security symposium (organized since 2001), we have a "capture the flag" style competition with both industry and student participants. Materials developed every year for the competition will be utilized to improve and update our security laboratories. Feedback from industry participants helps keep these exercises up to date with the latest security developments.

C. Describe information technology and services available for the proposed program

In addition to the IT facilities mentioned above, the University has an expanding information technology infrastructure covering communication, web servers, Moodle teaching servers, and cloud storage available campus-wide. All these facilities will support the new program to ensure its success.

D. Describe the effect of this new program on existing information technology and services and indicate whether they will be adequate, both at the commencement of the program and during the next decade.

It is anticipated that existing central Information Technology Services (ITS) resources are adequate for the new program, and the effect of the new program on the technology and services is minimal. The unique resources required by the program are housed and maintained in the College of Computing and Informatics. With the exception of the two labs needed, the resources are robust and can support the program for its commencement and into the future.

VII. Administration

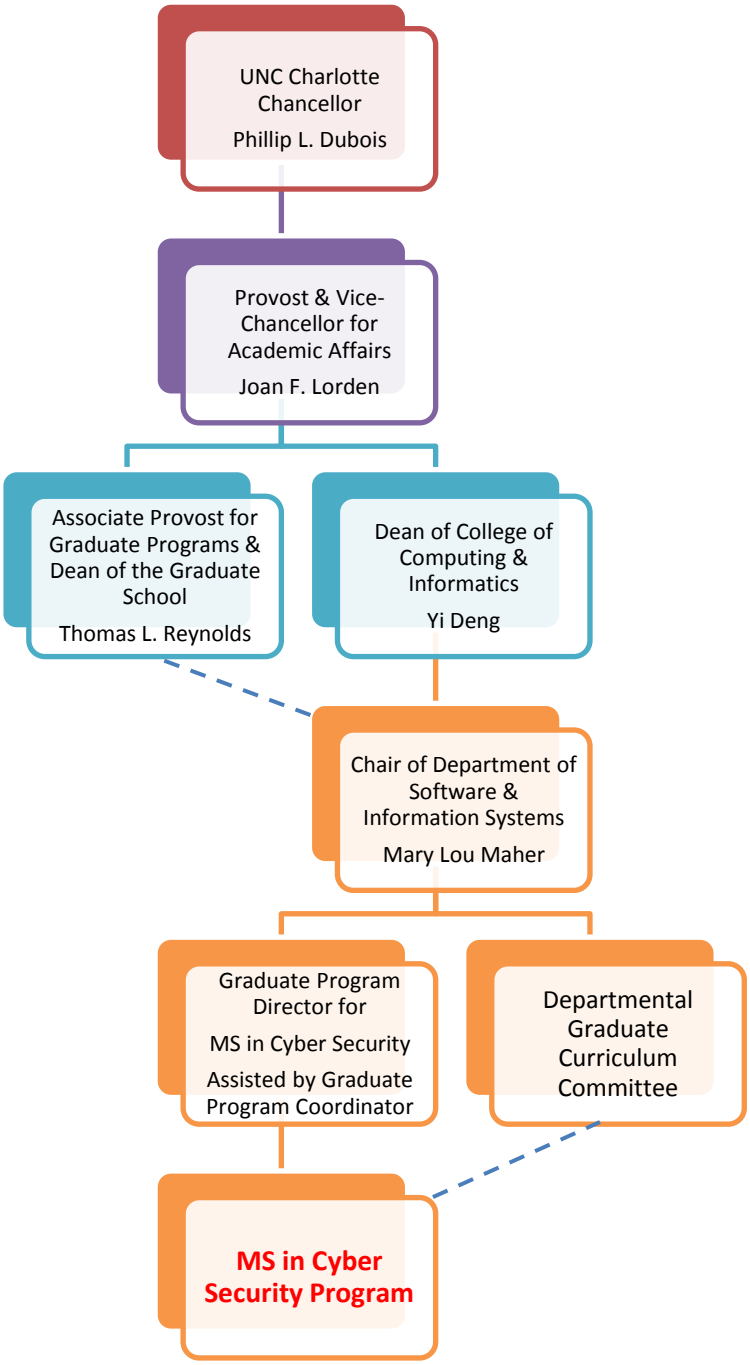
Describe how the proposed program will be administered, giving the responsibilities of each department, division, school, or college. Explain any inter-departmental or inter-unit administrative plans. Include an organizational chart showing the "location" of the proposed new program.

The proposed program will be administered within the Department of Software and Information Systems in the College of Computing and Informatics. The College has a Graduate Program Coordinator that assists all graduate programs in the College with recruiting, enrollment management, and coordinating activities of the program. The Department Chair has ultimate responsibility for the programs within the Department, reporting to the Dean of the College, who in turn reports to the Provost. Each graduate program has a Program Director who administers the program in liaison with the CCI Graduate Program Coordinator and reports to the Department Chair.

At the University of North Carolina at Charlotte, the Dean of the Graduate School is the administrative officer with primary responsibility for the supervision of graduate programs. The Dean is responsible for the executive and administrative affairs of the Graduate School in accordance with policies determined by the UNC Charlotte Graduate Council, the Graduate faculty, and the Faculty Council. The Graduate School is responsible for monitoring the quality of graduate programs, the final admission of graduate students, appointments to the Graduate faculty, and the enhancement of research activities essential to the conduct of graduate programs. The Graduate Dean's main duties include the following:

- Admission of students
- Appointment of dissertation and thesis committees
- Approval of programs of study
- Admission of students to candidacy
- Final approval of theses and dissertations

The following chart depicts the organizational "location" of the proposed Master's program.



VIII. Accreditation and Licensure

A. Where appropriate, describe how all licensure or professional accreditation standards will be met, including required practica, internships, and supervised clinical experiences.

UNC Charlotte is accredited by the Commission on Colleges of the Southern Association of Colleges and Schools (SACS) to award baccalaureate, master's, and doctoral degrees.

B. Indicate the names of all accrediting agencies normally concerned with programs similar to the one proposed. Describe plans to request professional accreditation.

N/A.

C. If the new degree program meets the SACS definition for a substantive change, what campus actions need to be completed by what date in order to ensure that the substantive change is reported to SACS on time?

The Department will draft a substantive change prospectus per SACS requirements. The draft will be submitted to the Executive Director of the Office of Assessment and Accreditation, who will work with the Provost and Chancellor to submit the prospectus at least six months prior to the start of the new Master's degree program.

D. If recipients of the proposed degree will require licensure to practice, explain how program curricula and title are aligned with requirements to "sit" for the licensure exam.

No licensure to practice is required.

IX. Supporting Fields

Discuss the number and quality of lower-level and cognate programs for supporting the proposed degree program. Are other subject-matter fields at the proposing institution necessary or valuable in support of the proposed program? Is there needed improvement or expansion of these fields? To what extent will such improvement or expansion be necessary for the proposed program?

None is needed.

X. Additional Information

Include any additional information deemed pertinent to the review of this new degree program proposal.

No additional information is included.

XI. Budget

A. Complete and insert the Excel budget template provided showing incremental continuing and one-time costs required each year of the first four years of the program. Supplement the template with a budget narrative for each year.

SUMMARY OF ESTIMATED ADDITIONAL COSTS FOR PROPOSED PROGRAM

INSTITUTION	UNC Charlotte	DATE	
Program (CIP, Name, Level)	Master of Science in Cyber Security		
Degree(s) to be Granted	MS	Program Year	Year 1 (2016-2017)
Differential tuition requested per student per academic yr	$4,000		
Projected annual FTE students	25		
Projected annual differential tuition	$100,000		
Percent differential tuition for financial aid			
Differential tuition remainder	100000		

ADDITIONAL FUNDS REQUIRED - BY SOURCE

	Reallocation of Present Institutional Resources	Projected Differential Tuition	Enrollment Increase Funds	Other New Allocations (Identify)	Total
EPA/SPA Regular Salaries					
PT Program Coordinator	$ 32,000.00	$ -	$ -	$ -	$ 32,000.00
EPA Academic Salaries					
FT Teaching Assistant Professor	$ -	$ 35,000.00	$ -	$ -	$ 35,000.00
Social Security	$ 2,448.00	$ 2,678.00	$ -	$ -	$ 5,126.00
State Retirement	$ -	$ 4,498.00	$ -	$ -	$ 4,498.00
Medical Insurance	$ 1,264.00	$ 2,736.00	$ -	$ -	$ 4,000.00
Graduate Stipends					
4.5 @ $9,600/year	$ -	$ 43,200.00	$ -	$ -	$ 43,200.00
Supplies and Materials					
(Identify)	$ -	$ -	$ -	$ -	$ -
Current Services					
(Identify)	$ -	$ -	$ -	$ -	$ -
Travel	$ 6,000.00	$ -	$ -	$ -	$ 6,000.00
Communications	$ 1,000.00	$ -	$ -	$ -	$ 1,000.00

Printing and Binding	$ 1,000.00	$ -	$ -	$ -	$ 1,000.00
Advertising	$ 3,000.00	$ -	$ -	$ -	$ 3,000.00
Fixed Charges					
(Identify)	$ -	$ -	$ -	$ -	$ -
Capital Outlay (Equipment)					
Laboratory Technology	$ -	$ 11,888.00	$ -	$ 48,112.00	$ 60,000.00
Libraries	$ 2,000.00	$ -	$ -	$ -	$ 2,000.00
TOTAL ADDITIONAL COSTS	**$ 48,712.00**	**$ 100,000.00**	**$ -**	**$ 48,112.00**	**$ 196,824.00**

Narrative: Recruiting for a full-time Teaching Assistant Professor will begin the first semester of the program. Year 1 tuition differential will support this position, with benefits, for the second semester. The tuition differential funding will also support approximately 4.5 graduate assistantships at $9,600/year for a total of $43,200. Reallocation of current resouces will support a part-time Program Coordinator with a salary of $32,000 ($64,000-Full salary in Year 3) and travel, communications, printing, advertising, etc. Year 1 also includes a $60,000 one-time investment for the establishment of two cyber security laboratories, which will be supported by the tuition differential and other allocations TBD.

SUMMARY OF ESTIMATED ADDITIONAL COSTS FOR PROPOSED PROGRAM

INSTITUTION	UNC Charlotte	DATE	
Program (CIP, Name, Level)	Master of Science in Cyber Security		
Degree(s) to be Granted	MS	Program Year	Year 2 (2017-2018)
Differential tuition requested per student per academic yr	$4,000		
Projected annual FTE students	47.5		
Projected annual differential tuition	$190,000		
Percent differential tuition for financial aid			
Differential tuition remainder	190000		

ADDITIONAL FUNDS REQUIRED - BY SOURCE

	Reallocation of Present Institutional Resources	Projected Differential Tuition	Enrollment Increase Funds	Other New Allocations (Identify)	Total
EPA/SPA Regular Salaries					
PT Program Coordinator	$ -	$ -	$ 32,000.00	$ -	$ 32,000.00
EPA Academic Salaries					
FT Teaching Assistant Professor	$ -	$ 70,000.00	$ -	$ -	$ 70,000.00
Social Security	$ -	$ 5,355.00	$ 2,448.00	$ -	$ 7,803.00
State Retirement	$ -	$ 8,995.00	$ -	$ -	$ 8,995.00
Medical Insurance	$ -	$ 5,581.00	$ 1,264.00	$ -	$ 6,845.00
Graduate Stipends					
9 @ $9,600/year	$ -	$ 86,400.00	$ -	$ -	$ 86,400.00
Supplies and Materials					
Classroom Technology	$ -	$ 11,600.00	$ 8,000.00	$ -	$ 19,600.00
Program Workshop/Seminars	$ -	$ -	$ 5,000.00	$ -	$ 5,000.00
Recruiting Supplies	$ -	$ -	$ 1,000.00	$ -	$ 1,000.00
Current Services					
Program Workshop/Seminars	$ -	$ -	$ 10,000.00	$ -	$ 10,000.00

Travel	$ -	$ 6,000.00	$ -	$ -	$ 6,000.00
Communications	$ -	$ -	$ 1,000.00	$ -	$ 1,000.00
Printing and Binding	$ -	$ -	$ 1,000.00	$ -	$ 1,000.00
Advertising	$ -	$ 2,069.00	$ -	$ -	$ 2,069.00
Fixed Charges					
(Identify)	$ -	$ -	$ -	$ -	$ -
Capital Outlay (Equipment)					
Classroom Technology	$ -	$ -	$ 19,500.00	$ -	$ 19,500.00
Libraries	$ -	$ -	$ 2,000.00	$ -	$ 2,000.00
TOTAL ADDITIONAL COSTS	**$ -**	**$ 196,000.00**	**$ 83,212.00**	**$ -**	**$279,212.00**

Narrative: Year 2 tuition differential will support the Teaching Assistant Professor for the full year at a salary of $70,000. It will also cover approximately 9 graduate assistantships at $9,600/year. The remainder of tuition differential funding will support classroom technology/supplies, travel and advertising. Enrollment increase funds will support a PT Program Coordinator, recruitment costs of $15,000, classroom technology expenditures of $27,500 and program workshops/seminars of $15,000.

SUMMARY OF ESTIMATED ADDITIONAL COSTS FOR PROPOSED PROGRAM

INSTITUTION	UNC Charlotte	DATE	
Program (CIP, Name, Level)	Master of Science in Cyber Security		
Degree(s) to be Granted	MS	Program Year	Year 3 (2018-2019)
Differential tuition requested per student per academic yr	$4,000		
Projected annual FTE students	69		
Projected annual differential tuition	$276,000		
Percent differential tuition for financial aid			
Differential tuition remainder	276000		

ADDITIONAL FUNDS REQUIRED - BY SOURCE

	Reallocation of Present Institutional Resources	Projected Differential Tuition	Enrollment Increase Funds	Other New Allocations (Identify)	Total
EPA/SPA Regular Salaries					
FT Program Coordinator	$ -	$ -	$ 64,000.00	$ -	$ 64,000.00
EPA Academic Salaries					
FT Teaching Assistant Professor	$ -	$ 72,000.00	$ -	$ -	$ 72,000.00
Assistant Professor	$ -	$ 45,000.00	$ -	$ -	$ 45,000.00
Social Security	$ -	$ 8,951.00	$ 4,896.00	$ -	$ 13,847.00
State Retirement	$ -	$ 15,035.00	$ 8,224.00	$ -	$ 23,259.00
Medical Insurance	$ -	$ 8,482.00	$ 5,692.00	$ -	$ 14,174.00
Graduate Stipends					
9.5 @ $9,600/year	$ -	$ 91,200.00	$ -	$ -	$ 91,200.00
Supplies and Materials					
Technology	$ 12,000.00	$ -	$ -	$ -	$ 12,000.00
Program Workshops/Seminars	$ 3,168.00	$ 1,832.00	$ -	$ -	$ 5,000.00
Recruiting Supplies	$ 1,500.00	$ -	$ -	$ -	$ 1,500.00
Current Services					

Program Workshops/Seminars	$ 10,000.00	$ -	$ -	$ -	$ 10,000.00
Travel	$ 5,000.00	$ -	$ -	$ -	$ 5,000.00
Communications	$ 1,000.00	$ -	$ -	$ -	$ 1,000.00
Printing and Binding	$ -	$ 1,500.00	$ -	$ -	$ 1,500.00
Advertising	$ 2,000.00	$ -	$ -	$ -	$ 2,000.00
Fixed Charges					
(Identify)	$ -	$ -	$ -	$ -	$ -
Capital Outlay (Equipment)					
Classroom Technology	$ -	$ 32,000.00	$ -	$ -	$ 32,000.00
Libraries	$ -	$ -	$ 2,000.00	$ -	$ 2,000.00
TOTAL ADDITIONAL COSTS	**$ 34,668.00**	**$ 276,000.00**	**$84,812.00**	**$ -**	**$395,480.00**

Narrative: Hiring for an Assistant Professor will take place in Year 3. The Assistant Professor will start in the second semester, with a salary of $45,000 (full salary of $90,000 in Year 4). The tuition differential will will fund both the Teaching Assistant Professor and Assistant Professor positions. Graduate stipends of $91,200 (9.5 @ $9,600/year) will be funded through these funds. The remainder of the tuition increment will cover the costs of printing and classroom technology, etc. The college will fund a portion of costs for progam workshops/seminars, technology, travel, and other supplies. Estimated enrollment increase funds will support a full time Program Director with a salary of $64,000 with benefits.

SUMMARY OF ESTIMATED ADDITIONAL COSTS FOR PROPOSED PROGRAM

INSTITUTION	UNC Charlotte	DATE	
Program (CIP, Name, Level)	Master of Science in Cyber Security		
Degree(s) to be Granted	MS	Program Year	Year 4 (2019-2020)
Differential tuition requested per student per academic yr	$4,000		
Projected annual FTE students	90		
Projected annual differential tuition	$360,000		
Percent differential tuition for financial aid			
Differential tuition remainder	360000		

ADDITIONAL FUNDS REQUIRED - BY SOURCE

	Reallocation of Present Institutional Resources	Projected Differential Tuition	Enrollment Increase Funds	Other New Allocations (Identify)	Total
EPA/SPA Regular Salaries					
FT Program Coordinator	$ -	$ -	$ 64,000.00	$ -	$ 64,000.00
EPA Academic Salaries					
FT Teaching Assistant Professor	$ -	$ 75,000.00	$ -	$ -	$ 75,000.00
Assistant Professor	$ -	$ 90,000.00	$ -	$ -	$ 90,000.00
Social Security	$ -	$ 12,623.00	$ 4,896.00	$ -	$ 17,519.00
State Retirement	$ -	$ 21,203.00	$ 8,224.00	$ -	$ 29,427.00
Medical Insurance	$ -	$ 11,612.00	$ 5,805.00	$ -	$ 17,417.00
Graduate Stipends					
10 @ $9,600/year	$ -	$ 96,000.00	$ -	$ -	$ 96,000.00
Supplies and Materials					
Program Workshops/Seminars	$ -	$ 5,000.00	$ -	$ -	$ 5,000.00
Recruiting Supplies	$ -	$ 2,000.00	$ -	$ -	$ 2,000.00
Current Services					
Program Workshops/Seminars	$ -	$ 10,000.00	$ -	$ -	$ 10,000.00

Travel	$ -	$ 5,000.00	$ -	$ -	$ 5,000.00
Communications	$ -	$ 2,000.00	$ -	$ -	$ 2,000.00
Printing and Binding	$ -	$ 2,000.00	$ -	$ -	$ 2,000.00
Advertising	$ -	$ 1,000.00	$ -	$ -	$ 1,000.00
Fixed Charges					
(Identify)	$ -	$ -	$ -	$ -	$ -
Capital Outlay (Equipment)					
Classroom Technology	$ 38,438.00	$ 26,562.00	$ -	$ -	$ 65,000.00
Libraries	$ -	$ -	$ 2,000.00	$ -	$ 2,000.00
TOTAL ADDITIONAL COSTS	**$ 38,438.00**	**$ 360,000.00**	**$ 84,925.00**	**$ -**	**$483,363.00**

Narrative: Year 4 will support both full-time Teaching Assistant Professor and Assistant Professor positions, along with $96,000 (10 @ $9,600/year) in graduate stipends. The remaining tuition differential will cover costs for program workshop/seminars, recruiting, and a portion of classroom technology. The college will support $38,438 in classroom technology and with the estimated enrollment increase funds the FT Program Coordinator will be paid.

B. Based on the campus' estimate of available existing resources or expected non-state financial resources that will support the proposed program (e.g., federal support, private sources, tuition revenue, etc), will the campus:

1. Seek enrollment increase funds or other additional state appropriations (both one-time and recurring) to implement and sustain the proposed program? If so, please elaborate.

We will seek enrollment increase funds to support the program beginning in Year 2. As the program grows, these funds will be used support the program coordinator and specialized materials for the program. We do not anticipate federal support for the MS degree, however, an increase in tenure track faculty that teach in the MS degree will result in an increase in federal support for research in cyber security. No additional funds from the State are sought.

2. Require differential tuition supplements or program-specific fees? If so, please elaborate.

a. State the amount of tuition differential or program-specific fees that will be requested.

The tuition differential requested is $2000 per semester. We request this differential to support the specialized laboratory and software technologies

required for this program. Tuition differential will also support graduate stipends and additional teaching faculty.

b. Describe specifically how the campus will spend the revenues generated.

See budget narrative

c. Does the campus request the tuition differential or program-specific fees be approved by the Board of Governors prior to the next Tuition and Fee cycle?

Yes.

C. If enrollment increase funding, differential tuition, or other state appropriations noted in the budget templates are not forthcoming, can the program still be implemented and sustained and, if so, how will that be accomplished? Please elaborate and provide documentation of campus commitments where appropriate.

Because the courses needed for the program are already being offered, the program can be sustained, but not at the anticipated enrollment. Additional sections of core courses will be needed.

XII. Evaluation Plans

All new degree program proposals must include an evaluation plan which includes:

A. Criteria to be used to evaluate the quality and effectiveness of the program, including academic program student learning outcomes.

Proposed Student Learning Outcomes – see Attachment B for more detail

- SLO1 Students will demonstrate knowledge of core information security concepts.
- SLO2 Students will demonstrate ability to build a system that is secure against network based attacks.
- SLO3 Students will demonstrate knowledge of key cryptographic algorithms.
- SLO4 Students will demonstrate effective written and oral communication in the domain of cyber security.

Other external criteria used to evaluate the program include, but are not limited to the following:

- Quality of applicants and entering students
- Progress toward degree
- Number of students that meet student learning outcomes
- Number of graduates from the program
- Successful placement of the graduates in positions in industry or government
- Successful placement of graduates not immediately seeking employment in advanced degree (Ph.D.) programs

B. Measures (metrics) to be used to evaluate the program (include enrollments, number of graduates, and student success).

- The program is expected to reach a steady-state enrollment of about 100 students within four years, with about 20% being part time.
- Full time students are expected to complete the program in 1.5 years, and part-time students in 2.5 years.

- The program will be deemed successful if students receive competitive job offers from industry and government agencies, or proceed to enroll in a PhD program for further studies.
- The Student Learning Outcomes Assessment Plan will be used to evaluate the four student learning objectives.

C. The plan and schedule to evaluate the proposed new degree program prior to the completion of its fourth year of operation.

The SIS Department will employ its existing robust continuous improvement assessment process to this proposed program. Annual evaluation prior to the fourth year will consist of a review of achievements related to student recruitment, admissions and retention, as well as evaluations by students of course delivery, advising and placement. Data on time to graduation will be collected and analyzed on a yearly basis. In addition, feedback from alumni and employers will be surveyed regularly to refine and improve the program.

Data collected will also be used as part of the input to the yearly evaluation for the Student Learning Outcomes Assessment Plan which is part of the Institutional Effectiveness report.

XIII. Reporting Requirements

Institutions will be expected to report on new program productivity as a part of the biennial low productivity program review process.

XIV. Attachments

Attach the final approved Appendix A as the first attachment following this document.

This proposal to establish a new degree program has been reviewed and approved by the appropriate campus committees and authorities.

Chancellor: _____**Date**:_____

Attachment A. Request to Plan (Approved)

UNC CHARLOTTE

Office of the Chancellor

9201 University City Boulevard, Charlotte, NC 28223-0001
t/ 704.687.5700 f/ 704.687.1700 www.uncc.edu

August 7, 2015

Dr. Chris Brown
Vice President for Research and Graduate Education
University of North Carolina
Post Office Box 2688
Chapel Hill, North Carolina 27515-2688

Dear Dr. Brown:

Enclosed is UNC Charlotte's request for authorization to plan a M.S. in Cyber Security. The proposed program would prepare graduates to work in the high-demand field of cyber security and privacy in a variety of industries including business, healthcare, government, and the banking and energy industries. The program would build upon the internationally recognized faculty that UNC Charlotte has in this field.

Thank you for your consideration of this request. Provost Joan Lorden or I would be pleased to respond to any questions that you may have.

Cordially,

Philip L. Dubois
Chancellor

cc: Joan F. Lorden, Provost and Vice Chancellor for Academic Affairs
Yi Deng, Dean, College of Computing and Informatics
Courtney Thornton, Associate Vice President for Research and Graduate Education
Cody Thompson, Coordinator for Academic Planning

UNC CHARLOTTE

Office of Academic Affairs

9201 University City Blvd, Charlotte, NC 28223-0001
t/ 704.687.5717 f/ 704.687.1457 www.uncc.edu

August 10, 2015

Dr. Chris Brown
Vice President for Research and Graduate Education
University of North Carolina
Post Office Box 2688
Chapel Hill, North Carolina 27515-2688

Dear Dr. Brown:

Enclosed is UNC Charlotte's Appendix A: Request for Authorization to Plan a M.S. in Cyber Security. The proposal provides a summary budget which includes enrollment increase funding. UNC Charlotte is committed to funding the expenses for the degree as described by reallocating funds, if needed.

Thank you for your consideration of this request.

Sincerely,

Joan F. Lorden

Joan F. Lorden
Provost and Vice Chancellor for Academic Affairs

cc: Courtney Thornton, Associate Vice President for Research and Graduate Education
Cody Thompson, Coordinator for Academic Planning

APPENDIX A

UNIVERSITY OF NORTH CAROLINA

REQUEST FOR AUTHORIZATION TO PLAN A NEW DEGREE PROGRAM

THE PURPOSE OF ACADEMIC PROGRAM PLANNING: Planning a new academic degree program provides an opportunity for an institution to make the case for need and demand and for its ability to offer a quality program. The notification and planning activity to follow do not guarantee that authorization to establish will be granted.

Date: September 14, 2015

Constituent Institution: The University of North Carolina at Charlotte

CIP Discipline Specialty Title: Computer & Information Sciences

CIP Discipline Specialty Number: ___11.1003__ Level: B _____ M _X_ Res. Doc. _____ Prof. Doc. _____

Exact Title of the Proposed Program: Cyber Security

Exact Degree Abbreviation (e.g., B.S., B.A., M.A., M.S., Ed.D., Ph.D.): M.S.

Does the proposed program constitute a substantive change as defined by SACS? Yes _X__ No _____

The current SACS Substantive Change Policy Statement may be viewed at:
http://www.sacscoc.org/pdf/081705/Substantive%20Change%20policy.pdf

If yes, please briefly explain.

As required by the Policy Statement on Substantive Change for Accredited Institutions of the Commission on Colleges, the University of North Carolina at Charlotte (UNC Charlotte) is required to submit a letter of notification prior to implementation for new degree programs. Notification of this new degree program will be provided to SACS after approval by the University of North Carolina Board of Governors and prior to implementation.

Proposed date to enroll first students in degree program: *Month* August *Year* 2016

1. Provide a summary of the status of this proposal in your campus review processes.

   a. List the campus bodies that reviewed and commented on this Appendix A proposal before submission to UNC General Administration. What were their determinations? Include any votes, if applicable.

   This proposal has been reviewed by the following campus bodies. All these bodies have approved the proposal unanimously.
   - The graduate curriculum committee of the Department of Software and Information Systems
   - The Department of Software and Information Systems
   - The graduate committee of the College of Computing and Informatics

b. Summarize any issues, concerns or opposition raised throughout the campus process and comment periods. Describe revisions made to address areas of concern.

No major issues were raised during the consultation process.

2. Describe the proposed new degree program. The description should include:

a. A brief description of the program and a statement of educational objectives;

The Master of Science in Cyber Security is designed to equip students with the latest knowledge and skills in Cyber Security and privacy. Graduates of the program will be employable by both businesses and governments that have important information assets to be protected from increasingly sophisticated cyber-attacks.

Specific educational objectives of the program include:

- A fundamental understanding of:
  - common vulnerabilities of computing and networked systems,
  - cyber-attacking methods,
  - human and organizational aspects of Cyber Security,
  - methods for compromising privacy, and
  - risk assessment of cyber-attacks.
- Able to apply security techniques to analyze and evaluate the security risk of information systems and networks.
- Able to design information systems and networks with security controls to minimize security risks.

The program requires students take four core courses and six elective courses, including the selection of a concentration and a culminating experience. The core courses are designed to prepare students with fundamental knowledge and skills in Cyber Security and privacy protection that are essential to all Cyber Security professionals. The elective courses give students an opportunity to further broaden their knowledge and skills in areas that are of particular interest to them. The selection of a concentration allows students to choose to learn more depth in a particular area of Cyber Security such as information security, network security, or secure software development. For the culminating experience, the student may choose an industry internship or a master's thesis. Together these components will equip students with necessary skill sets in specific areas in Cyber Security and privacy where they wish to pursue their professional careers.

UNC Charlotte has offered a 12 credit graduate certificate in information security for over ten years. The proposed program requires 30 credit hours of graduate level Cyber Security courses to provide much more technical depth content than is provided in the graduate certificate. Furthermore, the selection of a Cyber Security concentration area allows specialization in an area in which UNC Charlotte has been certified by the National Security Agency and the U.S. Department of Homeland Security as a Center of Academic Excellence. The proposed program also differs from the graduate certificate in that it allows the students to choose to do a master's thesis or an industry internship. The master's thesis option offers an opportunity for students to solve a unique problem under the direction of an experienced research faculty and is often a stepping-stone towards pursuing a career in advanced research. The internship option provides students with guided industry experience in Cyber Security.

b. The relationship of the proposed new program to the institutional mission;

The proposed Master of Science in Cyber Security closely aligns with the UNC Charlotte mission as North Carolina's urban research university. It strongly supports the university's focus on community engagement, graduate education, and the economic and social needs of the greater Charlotte region. The program also aligns with the missions of the Department of Software and information Systems (SIS) and College of Computing and Informatics (CCI). The master's program is built upon a strong record of faculty achievement in the areas of Cyber Security and privacy.

The University is committed to growing graduate programs in areas of national, state, and regional need. The proposed program will help address an increasingly strong demand for employees with information and network security knowledge and skills. Further, it aligns well with growing national security needs in safeguarding the nation against emerging threats emanating from the cyber space. President Obama has declared that the "cyber threat is one of the most serious economic and national security challenges we face as a nation" and that, "America's economic prosperity in the 21st century will depend on cyber-security." According to Steve Rosenbush, the Deputy Editor of the CIO journal belonging to the Wall Street Journal, the demand for Cyber Security experts is growing at 3.5 times the pace of the overall IT job market, and 12 times the overall job market. Because of the sensitivity of responsibilities in Cyber Security, many of these jobs cannot be out-sourced. At the same time, economic drivers in the Charlotte region such as the power and financial service industries have been frequent targets of cyber-attacks. The proposed degree addresses the need for a skilled Cyber Security workforce. The program is designed to ensure that students are well equipped for employment in a wide variety of industries including financial services, energy, retail/supply chain and health care where data and infrastructure security and safety are of paramount importance.

c. The relationship of the proposed new program to existing programs at the institution and to the institution's strategic plan; and

The Master of Science in Cyber Security will complement the Master of Science in Information Technology (MSIT) program offered at UNC Charlotte. Although the Master of Science in Information Technology offers a concentration in information security and privacy, students in that program can take a maximum of only 12 credit hours in information security and privacy, which makes it difficult for students to acquire a deep understanding of the rapidly expanding knowledge and skills in Cyber Security. The new program will require students to take up to 30 credit hours in Cyber Security and privacy, as well as a culminating experience relevant to Cyber Security. The proposed program will better equip students with state of the art knowledge and skills in the areas that are essential in safe-guarding information assets.

Enrollment of international students in the existing MSIT program has been growing at a pace far greater than that of domestic students (see Section 3 for details). On the other hand, domestic students have historically shown more interest in information security. The new Master of Science in Cyber Security will attract more domestic students into the graduate programs of the College of Computing and Informatics, resulting in a more diverse and balanced graduate student body.

The proposed program will also strengthen our MSIT program. We do not plan to eliminate our current information security concentration in the MSIT program because it provides more flexibility for students to pursue a broader education in information technology. The proposed program will attract more students to our graduate programs

in Cyber Security and create a larger community interested in this topic. In fall 2015, 10% of the MSIT students enrolled choose the information security concentration (18 out of 176).

The students in the PhD program in Computing and Information Systems have also expressed interested in Cyber Security that will benefit from the proposed program. In addition, the courses in the proposed master's degree will serve our PhD program as most of these courses are cross-listed as 8000-level courses. The new program will increase the number of students in these cross-listed courses. The number of PhD students working in the area of Cyber Security has been increased substantially (more than ~50%) in our department in the past five years.

We chose to create the proposed program as a MS program instead of as a Professional Science Master's because it provides flexibility for students to choose either a research focus, by selecting the master's thesis option, or a professional focus, by choosing an internship. In this critical area of Cyber Security, producing students with either advanced knowledge in the form of research or industry experience is critical to safe-guarding information assets.

d. Special features or conditions that make the institution a desirable, unique, or cost effective place to initiate such a degree program.

UNC Charlotte is situated in the region's largest city. Charlotte is ranked as the 17th largest U.S. city and is a financial, energy, healthcare, distribution and transportation center for the region. The business research company Hoover's lists 3,464 companies with $1 million or more in revenues located in the city of Charlotte and Mecklenburg county. Two hundred and seventy-four Fortune 500 companies have facilities in Charlotte, with eight headquartered here, including Bank of America, Lowe's, Nucor, Duke Energy, Family Dollar Stores, Goodrich, Sonic Automotive, and SPX. Charlotte is also home to the third largest public healthcare system in the country, Carolinas Healthcare System. The business community provides strong support for the Cyber Security program, as evidenced by attendance at regular information security events hosted by UNC Charlotte, including the annual information security symposium. This symposium is now in its 15th year and draws over 500 in attendance.

As the only public doctoral research university in the Charlotte region, UNC Charlotte is well positioned to offer this program. The Department of Software and Information Systems has been recognized by the National Security Agency (NSA) and the National Science Foundation (NSF) as a center of excellence in information and assurance education and research during the past decade. Faculty from the department include internationally recognized experts in Cyber Security whose research results are widely cited by peers and have also been adopted as international standards for data security. The Department has been a participant in NSF/Department of Defense Cyber Security Scholarship programs during the past 14 years, and have graduated over 60 master's students who have all been hired by federal government agencies.

3. Provide documentation of student demand. Discuss the extent to which students will be drawn from a pool of students not previously served by the institution. Evidence of student demand should reflect likely applicant pools (local, regional, statewide, national, or global) and could include:

a. Surveys of potential enrollees (such as students or alumni of feeder programs, community college enrollees, etc.).

In lieu of surveys of potential enrollees, we have obtained letters from major corporations in the Charlotte region (see attached) that indicate both a demand for students graduating with a specialization in Cyber Security and an interest in having their employees gain additional knowledge and skills in Cyber Security.

b. Enrollment data from existing minor, concentration or certificate programs on your campus.

National enrollment trend indicators for computer science have begun to show increases in the last decade. Freshmen interest in computing majors (HERI, http://www.heri.ucla.edu/tfsPublications.php) is increasing, as is actual enrollment in computing programs, which has increased by approximately 13% since 2011-12 (Taulbee, http://cra.org/resources/taulbee/).

The existing Master of Science in Information Technology (MSIT) at UNC Charlotte is designed to equip students with advanced skills and knowledge in the planning, design, implementation, testing and evaluation, deployment, maintenance, and management of applications and systems that embody information and communication technologies for their proper functioning. These skills form the necessary foundations for solving practical problems that arise in business, industrial, governmental, and other organizations, as well as for pursuing doctoral studies in information technologies. The current areas of concentration in the MSIT are: Advanced Data and Knowledge Discovery, Design, Emerging Technologies, Human-Computer Interaction, Information Security and Privacy, Information Technology Management, Software Systems Design and Engineering, and Web Development. The number of students enrolled in the MSIT has grown from 50-60 in Fall 2013 to 170-180 (a 300% increase). In Fall 2015, 10% of students enrolled in the MSIT program chose the Information Security and Privacy concentration (18 out of 176). More data will be presented in Section 4.g showing the strong market demand for IT workers with Cyber Security skills.

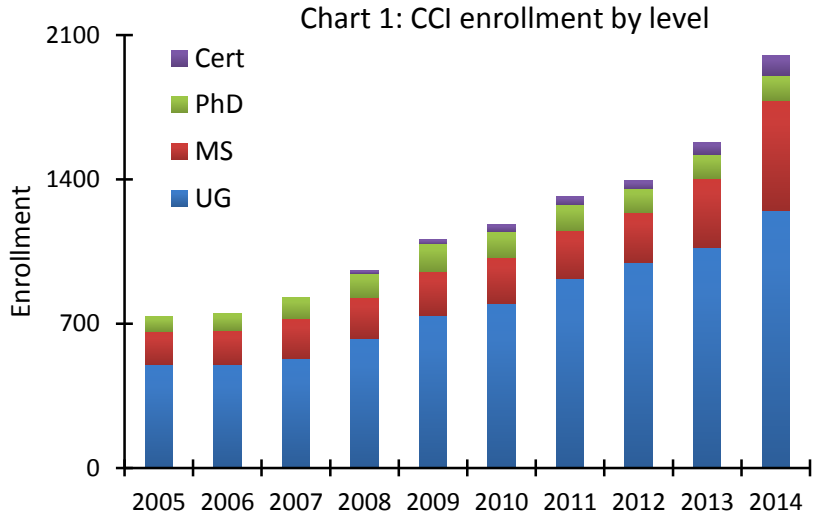
The SIS department currently offers the following Graduate Certificates:

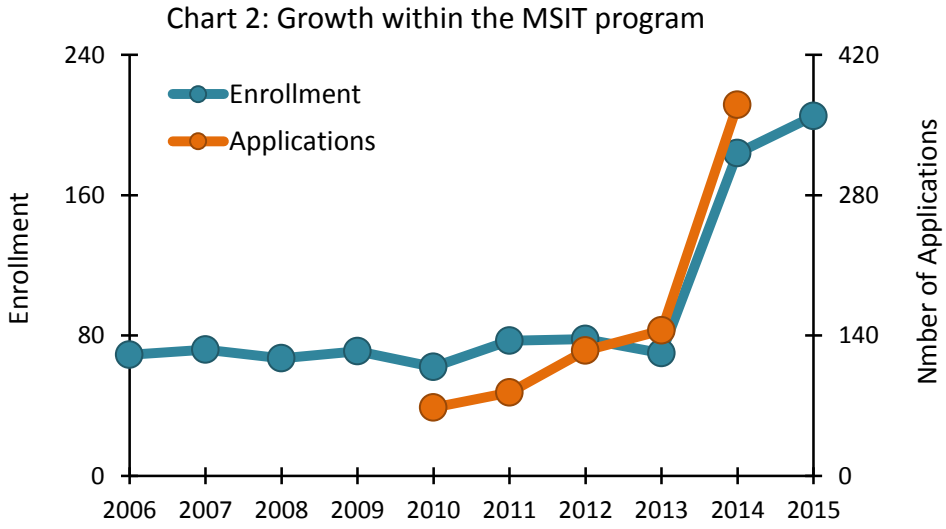
Graduate Certificate in Health Information Technology: This graduate certificate program is jointly offered by the College of Computing and Informatics and the College of Health and Human Services. The program provides healthcare professionals with an opportunity to advance their level of competence in the management of healthcare information as well as the secure and reliable exchange of the information among consumers, healthcare providers and other stakeholders in the industry.

Graduate Certificate in Information Security and Privacy: This graduate certificate provides professionals with an opportunity to advance their level of competence in the understanding, management, and applications of Cyber Security and privacy technology. We do not plan to eliminate our current graduate certificate in Information Security and Privacy because it provides more flexibility for students to pursue a broader IT education. The proposed program is designed to provide an in depth focus on Cyber Security.

Graduate Certificate in Management of Information Technology: This graduate certificate provides professionals with an opportunity to advance their level of competence in the management and applications of computing and information technology through formal training.

The SIS department is one of three departments within the College of Computing and Informatics (CCI) at UNC Charlotte. The College offers a variety of degree programs at all levels, including two doctoral programs, two MS programs, and partners with others on three Professional Science Master's programs. All of our programs have experiences dramatic growth in demand over the past decade, with our total enrollment nearly tripling in that time (see *Chart 1*). Moreover, growth within and applicant interest for the SIS department's existing MSIT program strongly parallels the College's overall growth (see *Chart 2*).





c. Enrollment data from similar programs in UNC, the state, or country.

In the UNC system, no university currently offers a master's degree in Cyber Security. Of the 55 existing master's programs within 300 miles of Charlotte that currently specify a degree that includes information security, only one in the southeast region is a campus-based degree specifically about information security: Master of Arts in Homeland Security, Keiser University, Ft. Lauderdale, FL. [Source: Petersons.com, retrieved June 2, 2015; search criteria = MS information security].

4. Provide evidence of societal demand and employability of graduates from as many of the following sources as feasible unless a good reason exists why such evidence cannot be obtained and similar evidence is presented from sources not listed here.

a. Labor market information (www.ncworks.gov) – Current and projected industry and occupational data by region and statewide from the NC Department of Commerce. Available data include (but are not limited to):

(1) Area, occupation, and industry profiles.

(2) NC occupational and employment projections.

(3) Job postings.

(4) Economic and demographic indicators.

b. National occupational and industry projections (http://www.bls.gov/data/) – National, regional and state outlook for occupations, also including wage data.

c. Wages and employment of graduates in North Carolina – Percentage of graduates of UNC programs employed in North Carolina and wages paid to graduates of UNC programs employed in North Carolina.

d. Wages and employment of graduates nationally when these data becomes available (see http://www.doleta.gov/performance/pfdocs/wris2_status_state_optin.pdf) – Wages paid to graduates of UNC programs employed nationally (North Carolina partnership in WRIS2 forthcoming).

e. Job-posting analyses.

f. Projections from professional associations or industry reports.

g. Data concerning employment and wages for graduates of a particular program area from the UNC alumni survey when this survey and data become available.

Cyber security requires special skills beyond what is generally covered in a baccalaureate degree. For example, to understand network security one must first understand networking well. Similarly, to understand software security one must have sufficient appreciation of software development and engineering. Given typical credit hour limits for a four-year degree program it is difficult to provide adequate coverage of Cyber Security topics in a four-year undergraduate degree program. It is therefore essential to offer Cyber Security at the master's level.

According to the US Department of Labor Bureau of Labor Statistics, employment in information security jobs is "projected to grow 37 percent from 2012 to 2022, much faster than the average for all occupations. It is estimated that this growth will result in 27,400 new jobs needed to fill the

industry. Demand for information security analysts in North Carolina is expected to be very high" (retrieved from NCWorks.gov on September 13, 2014).

Occupational Outlook Quarterly projected in its Spring 2014 issue that demand for information security analysts (i.e. Cyber Security professionals) will grow the fastest among all major STEM occupations, at 37% on average between 2012-2022. Demand for information security analysts is expected to be very high as these analysts will be needed to come up with innovative solutions to prevent hackers from stealing critical information or creating havoc on computer networks.

Occupation	Employment growth, projected 2012–22 (percent)	Employment		Median annual wage, May 2013
		2012	Projected 2022	
Information security analysts[2]	37%	75,100	102,500	$88,590
Operations research analysts	27	73,200	92,700	74,630
Statisticians	27	27,600	34,900	79,290
Biomedical engineers	27	19,400	24,600	88,670
Actuaries[3]	26	24,300	30,600	94,340
Petroleum engineers	26	38,500	48,400	132,320
Computer systems analysts	25	520,600	648,400	81,190
Software developers, applications	23	613,000	752,900	92,660
Mathematicians	23	3,500	4,300	102,440
Software developers, systems software	20	405,000	487,800	101,410
Computer user support specialists[4]	20	547,700	658,500	46,620

Source: Occupational Outlook Quarterly (http://www.bls.gov/careeroutlook/), Spring 2014

According to *Cisco 2014 Annual Security Report*, currently there is a global shortage of over one million Cyber Security professionals, with the majority of the demand being located in developed economies including the U.S.

The City of Charlotte has reported in their letter of support for this program that *Burning Glass Technologies* research shows that North Carolina experienced 127% growth in Cyber Security job postings between 2010 and 2014, with Charlotte experiencing 147% growth in the same period. This outstrips the 91% growth rate cited for Cyber Security job postings nationwide.

A recent report entitled *Understanding the Changing Market for Professional Master's Programs* from the Educational Advisory Board identified Cyber Security as one of three specialized areas that will have the fastest growth in master's enrollments in the next decade.

Demand for UNC Charlotte graduates with Cyber Security training has been very strong. For example, we have trained and placed over 150 MS graduates with concentration in Cyber Security for federal, state and local government. In fact, the demand for Cyber Security skills is so great in the public sector, the federal government offers generous scholarships for students to study Cyber Security in return to work in the public section upon graduation. The Department of Software and Information Systems has had a Scholarship for Service program funded by the Federal government for over 10 years to attract more students to study in the area of Cyber Security (http://sfs.uncc.edu/).

5. List all other public and private institutions of higher education in North Carolina currently operating programs similar to the proposed new degree program, including their mode of delivery.

Currently no university in North Carolina offers a master's program specifically in Cyber Security and Privacy. There are Graduate Certificates and MS degrees that have a concentration in Cyber Security, but North Carolina is underserved in providing a master's degree that is specifically in Cyber Security. Given the regional economy's reliance on financial service and energy as critical infrastructure, the proposed program will fill this gap.

a. Show a four-year history of enrollments and degrees awarded in similar programs offered at other UNC institutions (using the format below for each institution with a similar program); describe what was learned in consultation with each program regarding their experience with student demand and job placement. Indicate how their experiences influenced your enrollment projections.

Institution:
_____

Program Title:
_____

	(year)	(year)	(year)	(year)
Enrollment				
Degrees-awarded				

b. Identify opportunities for collaboration with institutions offering related degrees and discuss what steps have been or will be taken to actively pursue those opportunities where appropriate and advantageous.

c. Present evidence that establishment of this program would not create unnecessary program duplication.

6. Are there plans to offer all or a portion of this program to students off-campus or online?

Yes

If so,

a. Briefly describe these plans, including sites and method(s) of delivering instruction.

A limited number of courses will be available online to complement the on-campus instruction course offerings. The program will be offered on the UNC Charlotte Main Campus with a plan to offer some courses at the Center City Building in the future.

b. Indicate any similar programs being offered off-campus or online in North Carolina by other institutions (public or private).

No other institution in North Carolina is offering a similar program.

c. What is the estimated percentage of courses in the degree program that will be offered/available off-campus or online: 10-20%

d. Estimate the number of off-campus or online students that would be enrolled in the first and fourth years of the program:

First Year Full-Time 0 *Part-Time* 0

Fourth Year Full-Time 10 *Part-Time* 10

Note: If a degree program has not been approved by the Board of Governors, its approval for alternative, online, or distance delivery is conditioned upon BOG program approval. (400.1.1[R], page 3)

7. Estimate the total number of students that would be enrolled in the program during the first year of operation: *Full-Time* 20 *Part-Time* 10

Estimate the total number of students that would be enrolled in the program during the fourth year of operation: *Full-Time* 80 *Part-Time* 20

These numbers take into consideration that this is a two-year program and reflect the projected new and graduating student numbers. We estimate that 80% of the new students will enroll full-time based on our current enrollment demographics in graduate programs in the College of Computing and Informatics. We are also encouraging undergraduates to complete a master's degree with an early entry program which encourages students to enroll in the master's degree full time when they complete the Bachelor's degree (http://graduateschool.uncc.edu/future-students/programs/early-entry-graduate-programs).

8. Will the proposed program require development of any new courses: No

UNC Charlotte has been building education and research capabilities in Cyber Security over the past 15 years. We currently offer 12 graduate level courses (36 credit hours) related to Cyber Security. We expect to further improve and increase our course offerings over time, however, the proposed program does not require the development of new courses to get started. In response to demands from the proposed program and the interests of our industry partners, we expect more security courses will be offered each semester thus providing more electives for all graduate students at UNC Charlotte including those enrolled in the MSIT program.

9. Will any of the resources listed below be required to deliver this program? (If yes, please briefly explain in the space below each item, state the estimated new dollars required at steady state after four years, and state the source of the new funding and resources required.)

a. New Faculty: Yes

We plan to request one new faculty position in Cyber Security in the first year of the new MS and up to three new faculty over the first four years of the program, depending on program growth. These faculty will contribute to both the MS in Cyber Security and the expansion of the PhD program in Computing and Information Systems. Currently the Department has the following demographics in 2015:

- 16 tenure-track faculty and three non-tenure-track faculty
- Two administrative support positions
- 330 BA students
- 200+ MSIT students for Fall 2015

- 55 PhD students

The request for new faculty positions will be based on enrollment in the MS and expansion of our research capacity in Cyber Security. Additional faculty will ensure that our existing MSIT programs and this proposed new Master of Science in Cyber Security are delivered at the highest quality.

b. Additional Library Resources: No

c. Additional Facilities and Equipment: Yes

One-time investment in establishing two Cyber Security laboratories, one in Network Security and the other in Malware Analysis, is requested. The amount needed is $60,000 ($30,000 for each laboratory), including support for equipment, networking and required software. The primary reasons for the request are as follows:

- A quality Cyber Security program must provide students with adequate opportunities for hands-on experience.
- Due to the nature of Cyber Security, most of the projects to be carried out students must be conducted in an isolated computing environment so that impact of accidents is controlled and confined.
- Currently the Department has only an infrastructure laboratory that is extensively used by undergraduate classes. It will be inadequate for cater for the needs of the proposed master's program.

d. Additional Other Program Support: No
(for example, additional administrative staff, new master's program graduate student assistantships, etc.)

10. Does the program require enrollment growth funding in order to be implemented and sustained? If so, can the campus implement and sustain the program should enrollment growth funding be unavailable? Letters of commitment should be provided.

Yes, enrollment growth funding will be required to support the additional faculty and facility needs. A letter of support from the Provost is attached.

Does the program require a tuition differential or program specific fee in order to be implemented and sustained?
Yes.

a. If yes, state the amount of tuition differential or fee being considered, and give a brief justification.

The tuition differential being considered is $2000 per semester. The requested tuition differential will be used to maintain the high quality of the program, specifically for the following purposes:

New tuition dollars will be used to provide seminars and workshops, strengthen student recruitment, purchase specialized technology, and provide student financial assistance. The MS in Cyber Security program is estimated to enroll 20 full time and 10 part time students the first year of the program. Through aggressive recruitment efforts, it is expected that the student base will increase by 21-22 students in subsequent years. Based on this enrollment, the program will generate approximately

$100,000 in the first year from the increment. In the first year, 25% of the total tuition increment will be allocated to graduate assistantships; 60% percent will support .5 FTE of an Assistant Professor (the CCI will provide 50% salary support for the Assistant Professorship in the first year of the program); 15% will be allocated for recruitment costs including printing costs. The subsequent years will be budgeted as follows:

Need Based Graduate Assistantships (25%):

A portion of the tuition funds will be used to increase the number of assistantships in CCI. These Graduate Assistantships and the financial support they provide are essential in attracting the best available graduate students to the program. Assistantships offer an invaluable opportunity for graduate assistants to work with renowned faculty and allow faculty members to better leverage their teaching and research efforts through these talented students. The plan is to focus on students with financial need in the Charlotte region and on U.S. domestic students, raising the percentage of U.S. students in our program. This support will also be used to increase the enrollment of underrepresented populations.

Assistant Professor (50%):

An assistant professor will be hired in the 1st year of the MS program who is specialized in the area of Cyber Security; specifically, this faculty member will teach in the area of malware analysis. In subsequent years, new faculty and lab coordinators will be requested to address areas of high enrollment and research potential.

Recruitment and Technology (25%)

Ongoing recruitment costs will be capped at $10,000 each year. Recruitment costs include recruitment materials, campaigns, national travel to college fairs and industry engagements, supplies, and advertising costs. Starting in year three, salary support for a graduate program coordinator is budgeted to support recruitment efforts specific to the Cyber Security program.

Cyber Security is a technology-intensive field. Graduate students need a high level of technological interaction in the classroom. Hands on experience and realistic classroom exercises and simulations are required to provide students with the relevant exposure that potential employers are seeking. Standard network configurations, software, workstations and laptops are often inadequate for classroom assignments using the latest methods and larger scale data. High performance computing, software and data storage resources will need to be bolstered to support classroom instruction in order to prepare MS Cyber Security students for this type technology.

The remaining portion of the proposed tuition adjustment will be used to sponsor student learning enhancement in the form of seminars, workshops, and networking events with high-profile academic and industry leaders. The format of these events may include experts brought in to address particular courses

among other possible formats and will be designed to give students an opportunity to meet and learn from professionals in the Cyber Security arena. Additionally, these events will provide excellent opportunities for students to learn about job opportunities and to network with industry employers.

SUMMARY OF ESTIMATED ADDITIONAL COSTS FOR PROPOSED PROGRAM

INSTITUTION	***UNC Charlotte***
Degree(s) to be Granted	***M.S. Cyber Security***
Differential tuition requested per student per academic year	***$4,000***

PROJECTED ENROLLMENT

	Year 1	Year 2	Year 3	Year 4
Projected Full Time Student (1.0 FTE)	20	40	60	80
Projected Part Time Students (0.5 FTE)	10	15	18	20
Projected annual FTE students	25	47.5	69	90
Projected annual differential tuition	**$ 100,000**	**$ 190,000**	**$ 276,000**	**$360,000**

PROPOSED BUDGET OF DIFFERENTIAL TUITION

	Year 1	Year 2	Year 3	Year 4
Need-Based Graduate Assistantships/ Scholarships	$ 25,000	$ 47,500	$ 69,000	$ 90,000
Full Time Teaching/Assistant Professor*	$ 60,000	$ 95,000	$ 138,000	$ 180,000
Recruitment	$ 15,000	$ 10,000	$ 10,000	$ 10,000
Program Workshops/Seminars	$ -	$ 10,000	$ 15,000	$ 15,000
Technology	$ -	$ 27,500	$ 44,000	$ 65,000
TOTAL ADDITIONAL COSTS	**$ 100,000**	**$ 190,000**	**$ 276,000**	**$360,000**

.5 FTE in year 1; 1.0 FTE with 3% escalation in future years; $95,000 salary base + fringe

b. Can the campus implement and sustain the program if the tuition differential or program fee is not approved? Letters of commitment should be provided.

See attached letter from the Office of Academic Affairs.

12. For doctoral programs only:

a. Describe the research and scholarly infrastructure in place (including faculty) to support the proposed program.

b. Describe the method of financing the proposed new program (including extramural research funding and other sources) and indicate the extent to which additional state funding may be required.

c. State the number, amount, and source of proposed graduate student stipends and related tuition benefits that will be required to initiate the program.

13. List the names, titles, e-mail addresses and telephone numbers of the person(s) responsible for planning the proposed program.

- Dr. Mary Lou Maher, Chair, Department of Software and Information Systems, College of Computing and Informatics, M.Maher@uncc.edu, 704 687 6065

This request for authorization to plan a new program has been reviewed and approved by the appropriate campus committees and authorities.

Chancellor: _____ **Date**:_____

CHARLOTTE.
INNOVATION & TECHNOLOGY

September 4, 2015

Yi Deng, Ph.D.
Dean and Professor
UNC Charlotte, College of Computing and Informatics
9201 University City Boulevard
Charlotte, North Carolina 28223

Dear Dr. Deng,

We in the City of Charlotte strongly support the proposed new Master of Science in Cybersecurity degree by the College of Computing and Informatics at UNC Charlotte, which will train advanced professionals in the area of cybersecurity and privacy. There is a rapidly expanding demand for such advanced cybersecurity professionals and a widening shortage of talent supply in this critical area both regionally and nationally. Burning Glass Technologies has researched that North Carolina experienced 127% growth in cybersecurity job postings between 2010 and 2014, with Charlotte experiencing 147% growth in the same time period. This far outstrips the 91% growth rate cited for cybersecurity job postings nationwide and clearly illustrates the need for a strong local source for cybersecurity talent.

The proposed new degree program will not only expand the much needed new talent supply for the region and beyond, but will also create opportunities for organizations like ours to upgrade the knowledge and skills of our employees in the fast changing area of information security. In the next few years, we expect to expand our cybersecurity team by 50% after having expanded at least 25% for the past two years consecutively. We look forward to working with UNC Charlotte to expand talent supply and training in this area critical to our industries and economy in the region and nationwide.

Best regards,

Jeffrey W. Stovall

Jeffrey W. Stovall
Chief Information Officer
Innovation & Technology Department
City of Charlotte, North Carolina

301 South Tryon Street
Charlotte, NC 28262

Mr. Yi Deng, Ph.D.
Dean and Professor
UNC Charlotte, College of Computing and Informatics

Dear Mr. Yi Deng,

"We strongly support the proposed new MS in Cybersecurity degree by the College of Computing and Informatics at UNC Charlotte, which will train advanced professionals in the area of cybersecurity and privacy. There is a rapidly expanding demand for such advanced cybersecurity professionals and widening shortage of talent supply in this critical area both regionally and nationally. This proposed new degree will not only expand the much needed new talent supply for the region and beyond, but also create opportunities for companies like ours to access top, current talent in the fast changing area of cybersecurity. We are investing substantial resources and expanding our team in the area of cybersecurity and expect that trend to continue in the coming years. We look forward to working with UNC Charlotte to expand talent supply and training is this area critical to our industry and economy in the region and in the nation."

Rich Baich

Chief Information Security Officer
Corporate Risk

Wells Fargo & Company l 301 S Tryon St. l Charlotte, NC 28282
MAC D1130-204
Tel 704-715-8018 l Cell 704-763-6301 l Fax 704-383-8129

rich.baich@wellsfargo.com

Attachment B. Student Learning Outcomes

Student Learning Outcome 1 (knowledge, skill or ability to be assessed)
MSSec students will demonstrate knowledge of core information security concepts.
Changes to the Student Learning Outcomes Assessment Plan: If any changes were made to the assessment plan (which includes the Student Learning Outcome, Effectiveness Measure, Methodology and Performance Outcome) for this student learning outcome since your last report was submitted, briefly summarize the changes made and the rationale for the changes.
Effectiveness Measure: Identify the data collection instrument, e.g., exam, project, paper, etc. that will be used to gauge acquisition of this student learning outcome and explain how it assesses the desired knowledge, skill or ability. A copy of the data collection instrument and any scoring rubrics associated with this student learning outcome are to be submitted electronically to the designated folder on the designated shared drive.
In **ITIS 6200 Principles of Information Security and Privacy** (required program course) students are required to demonstrate knowledge of core information security concepts in a subset of questions in the course mid-term and/or final examination. Information security concepts will be judged in the areas of security attacks, security mechanisms, security policy, security threats, and secure systems. Exams will include questions similar to the ITIS 6200 Information Security Exam Question Examples included with the SLO documentation.
Methodology: Describe when, where and how the assessment of this student learning outcome will be administered and evaluated. Describe the process the department will use to collect, analyze and disseminate the assessment data to program faculty and to decide the changes/improvements to make on the basis of the assessment data.
Information security conceptual knowledge will be evaluated by the course instructor each semester that ITIS 6200 is taught. Typically, one section of ITIS 6200 is offered each Fall and Spring semester. The course instructor will specify a set of core information security concepts questions on the mid-term and/or final examination that correspond to the skill areas described above in the Effectiveness Measure. ITIS 6200 instructors will grade student responses according to a rubric that scores student performance on a scale of 1 to 5 across the multiple skill areas described above in the Effectiveness Measure. After collecting data, the instructors will report results, comments and suggestions for improvements to the Program Director. The Program Director will provide additional analysis and comments as needed and will forward all results and suggestions to the Departmental Graduate Committee for discussion and analysis. The Committee will evaluate results, identify areas for improvement, and suggest changes to achieve minimum performance targets by submitting a report to the Department Chair, the Program Director, and the College's Associate Dean for Administration, copying each affected instructor. The Program Director will coordinate with instructors to ensure that deficient areas are corrected and suggested changes are implemented. The Program Director will be responsible for generating the Final Assessment Report and gaining approval for the Report from the Department Chair and the College's Associate Dean for Administration.
Performance Outcome: Identify the percentage of students assessed that should be able to demonstrate proficiency in this student learning outcome and the level of proficiency expected. *Example: 80% of the students assessed will achieve a score of "acceptable" or higher on the Oral Presentation Scoring Rubric. (*Note: a copy of the scoring rubric, complete with cell descriptors for each level of performance, is to be submitted electronically to the designated folder on the designated shared drive.)
At least 80% of students will score 3 or better (on a 5 point scale) on the information security concepts evaluation.

Student Learning Outcome 2 (knowledge, skill or ability to be assessed)
MS Sec students will demonstrate ability to build a system that is secure against network based attacks.
Changes to the Student Learning Outcomes Assessment Plan: If any changes were made to the assessment plan (which includes the Student Learning Outcome, Effectiveness Measure, Methodology and Performance Outcome) for this student learning outcome since your last report was submitted, briefly summarize the changes made and the rationale for the changes.
None.
Effectiveness Measure: Identify the data collection instrument, e.g., exam, project, paper, etc. that will be used to gauge acquisition of this student learning outcome and explain how it assesses the desired knowledge, skill or ability. A copy of the data collection instrument and any scoring rubrics associated with this student learning outcome are to be submitted electronically to the designated folder on the designated shared drive.
In **ITIS 6167 Network Security** (required program course), students build a secure network based system that withstand network attacks as part of a semester-long development project. The projects require students to analyze various possible network based attacks, and to identify and define system requirements appropriate to secure the system. Project guidelines are given to the students, and then student project proposals are reviewed and approved by the instructor before students begin work. Course instructors provide details and interactive feedback on project development verbally throughout the semester, both in class and at project group meetings.
Methodology: Describe when, where and how the assessment of this student learning outcome will be administered and evaluated. Describe the process the department will use to collect, analyze and disseminate the assessment data to program faculty and to decide the changes/improvements to make on the basis of the assessment data.
The projects are graded by the course instructor each semester ITIS 6167 offered both in Fall and Spring semesters. The instructor specifies a set of assignments to develop a secure network based system. A rubric will be used to score student performance on a scale of 1 to 5 across the multiple skill areas described above in the Effectiveness Measure. After collecting data, the instructors will report results, comments and suggestions for improvements to the Program Director. The Program Director will provide additional analysis and comments as needed and will forward all results and suggestions to the Departmental Graduate Committee for discussion and analysis. The Committee will evaluate results, identify areas for improvement, and suggest changes to achieve minimum performance targets by submitting a report to the Department Chair, the Program Director, and the College's Associate Dean for Administration, copying each affected instructor. The Program Director will coordinate with instructors to ensure that deficient areas are corrected and suggested changes are implemented. The Program Director will be responsible for generating the Final Assessment Report and gaining approval for the Report from the Department Chair and the College's Associate Dean for Administration.
Performance Outcome: Identify the percentage of students assessed that should be able to demonstrate proficiency in this student learning outcome and the level of proficiency expected. *Example: 80% of the students assessed will achieve a score of "acceptable" or higher on the Oral Presentation Scoring Rubric. (*Note: a copy of the scoring rubric, complete with cell descriptors for each level of performance, is to be submitted electronically to the designated folder on the designated shared drive.)
At least 80% of students will score 3 or better (on a 5 point scale) on the network security effectiveness rubric.

Student Learning Outcome 3 (knowledge, skill or ability to be assessed)
MS Sec students will demonstrate knowledge of key cryptographic algorithms.
Changes to the Student Learning Outcomes Assessment Plan: If any changes were made to the assessment plan (which includes the Student Learning Outcome, Effectiveness Measure, Methodology and Performance Outcome) for this student learning outcome since your last report was submitted, briefly summarize the changes made and the rationale for the changes.
None.
Effectiveness Measure: Identify the data collection instrument, e.g., exam, project, paper, etc. that will be used to gauge acquisition of this student learning outcome and explain how it assesses the desired knowledge, skill or ability. A copy of the data collection instrument and any scoring rubrics associated with this student learning outcome are to be submitted electronically to the designated folder on the designated shared drive.
In **ITIS 6240 Applied Cryptography** (required program course) students are required to demonstrate knowledge of key cryptographic algorithms in the course midterm and/of final examination. These algorithms include symmetric encryption and decryption algorithms, public key encryption and decryption algorithms, cryptographic hashing algorithms, digital signature algorithms, random number generation algorithms, and crypto analysis methods.
Methodology: Describe when, where and how the assessment of this student learning outcome will be administered and evaluated. Describe the process the department will use to collect, analyze and disseminate the assessment data to program faculty and to decide the changes/improvements to make on the basis of the assessment data.
Cryptography conceptual knowledge will be evaluated by the course instructor each semester that ITIS 6240 is taught. Typically, one section of ITIS 6240 is offered once a year. The course instructor will specify a set of core cryptography concepts questions on the mid-term and/or final examination that correspond to the skill areas described above in the Effectiveness Measure. ITIS 6240 instructors will grade student responses according to a rubric that scores student performance on a scale of 1 to 5 across the multiple skill areas described above in the Effectiveness Measure. After collecting data, the instructors will report results, comments and suggestions for improvements to the Program Director. The Program Director will provide additional analysis and comments as needed and will forward all results and suggestions to the Departmental Graduate Committee for discussion and analysis. The Committee will evaluate results, identify areas for improvement, and suggest changes to achieve minimum performance targets by submitting a report to the Department Chair, the Program Director, and the College's Associate Dean for Administration, copying each affected instructor. The Program Director will coordinate with instructors to ensure that deficient areas are corrected and suggested changes are implemented. The Program Director will be responsible for generating the Final Assessment Report and gaining approval for the Report from the Department Chair and the College's Associate Dean for Administration.
Performance Outcome: Identify the percentage of students assessed that should be able to demonstrate proficiency in this student learning outcome and the level of proficiency expected. *Example: 80% of the students assessed will achieve a score of "acceptable" or higher on the Oral Presentation Scoring Rubric. (*Note: a copy of the scoring rubric, complete with cell descriptors for each level of performance, is to be submitted electronically to the designated folder on the designated shared drive.)
At least 80% of students will score 3 or better (on a 5 point scale) on the cryptographic algorithms evaluation.

Student Learning Outcome 4 (knowledge, skill or ability to be assessed)
MSSec students will demonstrate effective written and oral communication in the domain of cyber security.
Changes to the Student Learning Outcomes Assessment Plan: If any changes were made to the assessment plan (which includes the Student Learning Outcome, Effectiveness Measure, Methodology and Performance Outcome) for this student learning outcome since your last report was submitted, briefly summarize the changes made and the rationale for the changes.
None.
Effectiveness Measure: Identify the data collection instrument, e.g., exam, project, paper, etc. that will be used to gauge acquisition of this student learning outcome and explain how it assesses the desired knowledge, skill or ability. A copy of the data collection instrument and any scoring rubrics associated with this student learning outcome are to be submitted electronically to the designated folder on the designated shared drive.
In **ITIS 5250 Computer Forensics** (required program course) students deliver at least one written and one oral report of a forensics investigation. The presentation requires students to demonstrate an ability to use effective oral communication to report on the outcomes of a forensics investigation. Oral communication will be judged in the areas of body language, eye contact, pacing, poise, vocalization, use of visual aids, technical content, and answering questions. Course instructors provide feedback on the report, including the oral component, throughout the semester.
Methodology: Describe when, where and how the assessment of this student learning outcome will be administered and evaluated. Describe the process the department will use to collect, analyze and disseminate the assessment data to program faculty and to decide the changes/improvements to make on the basis of the assessment data.
Oral communication is graded by the course instructor each semester that ITIS 5250 is taught, typically offered each semester. How well the students construct and deliver the oral presentation(s) will be specifically evaluated as a component of one assignment grade. A rubric will be used to score student performance on a scale of 1 to 5 across the multiple skill areas described above in the Effectiveness Measure. After collecting data, the instructors will report results, comments and suggestions for improvements to the Program Director. The Program Director will provide additional analysis and comments as needed and will forward all results and suggestions to the Departmental Graduate Committee for discussion and analysis. The Committee will evaluate results, identify areas for improvement, and suggest changes to achieve minimum performance targets by submitting a report to the Department Chair, the Program Director, and the College's Associate Dean for Administration, copying each affected instructor. The Program Director will coordinate with instructors to ensure that deficient areas are corrected and suggested changes are implemented. The Program Director will be responsible for generating the Final Assessment Report and gaining approval for the Report from the Department Chair and the College's Associate Dean for Administration.
Performance Outcome: Identify the percentage of students assessed that should be able to demonstrate proficiency in this student learning outcome and the level of proficiency expected. *Example: 80% of the students assessed will achieve a score of "acceptable" or higher on the Oral Presentation Scoring Rubric. (*Note: a copy of the scoring rubric, complete with cell descriptors for each level of performance, is to be submitted electronically to the designated folder on the designated shared drive.)
At least 80% of students will score 3 or better (on a 5 point scale) on the communication evaluation.

Attachment C. Library Consultation

UNC CHARLOTTE

J. Murrey Atkins Library

Consultation on Library Holdings

To: Dr. Yuliang Zheng

From: Dr. Melanie Sorrell

Date: 1/7/2015

Subject: Master of Science in Cyber Security

Summary of Librarian's Evaluation of Holdings:

Evaluator: Dr. Melanie Sorrell Date: 1/7/2015

Check One:

1. Holdings are superior _____
2. Holdings are adequate __x__
3. Holdings are adequate only if Dept. purchases additional items. _____
4. Holdings are inadequate _____

Comments:
This is a proposal for a new graduate level degree program, which includes either a capstone project or a thesis option. Library holdings should be adequate to support student research for this program (see list of items held by subject heading below). Students will have access to relevant databases including INSPEC, Web of Science, Compendex, ACM Digital Library, IEEE Xplore Digital Library, PubMed, and the Wiley Online Library.

LC Subject Heading	Total items held
Computer Security	1,642 monographs
Data privacy	190 monographs
Computers – Moral and ethical aspects	42 monographs
Cloud computing – security measures	22 monographs
Computers – Access control	414 monographs
Computer software – Testing	139 monographs
ACM Transactions on Information and System Security	Journal title
IEEE Security & Privacy	Journal title

Melanie Sorrell

_____

Evaluator's Signature

1/7/2015

_____

Date

Attachment D. Letters of Support

1. Information Assurance Advisory
2. DataChambers
3. Oracle
4. Time Warner Cable
5. Womble Carlyle Sandridge & Rice

Information Assurance Advisory, LLC
301 McCullough Drive, 4th Floor, Charlotte, NC 28262-3310
Phone: 704-236-2385 Fax: 704-909-2701
www.iaadvisory.com

February 12, 2015

Dean Yi Deng
College of Computing and Informatics
University of North Carolina at Charlotte
9201 University City Boulevard
Charlotte, NC 28223-0001

Re: New UNC Charlotte Master of Science in Cyber Security Degree

As Managing Director of Information Assurance Advisory, LLC, I am writing to express support for UNC Charlotte's proposal to establish a Master of Science in Cyber Security degree. One only needs to read the news headlines over the past year to understand the need for more knowledgeable and skilled cyber security professionals. This new program will serve as an important source of cyber security talent; especially for many organizations in Charlotte, the surrounding areas and beyond.

Information Assurance Advisory, LLC has collaborated with the College of Information and Informatics for more than six years. Through collaboration on cybersecurity research initiatives, the College of Computing and Informatics has established it has a superb cadre of knowledgeable faculty and is developing many quality graduates from UNC Charlotte with critical cybersecurity knowledge.

The Council on Cybersecurity recently explained an existing dilemma; namely, "There is an unprecedented demand for highly-skilled practioners capable of building security into new and existing networks, assessing security on a real-time basis as new vulnerabilities are identified and disclosed, and acting as front-line cyber defenders across various industries and government agencies. Meanwhile, the number of entrants into the IT workforce has not kept up with demand, leaving a significant gap in capacity to adequately protect these networks from attack."

Information Assurance Advisory, LLC supports UNC Charlotte, and appreciates the College of Computing and Informatics' effort in establishing a Master of Science in Cyber Security degree. The new master's degree program will not only provide highly sought-after cyber security professionals for companies in the region but also will be responsive to the growing need to protect the economic and homeland security segments of the state and country.

Sincerely,

Roger M. Callahan
Managing Director

Data Chambers
by NORTH STATE

February 10, 2015

Dean Yi Deng
College of Computing and Informatics
University of North Carolina at Charlotte
9201 University City Boulevard
Charlotte, NC 28223-0001

Re: New Master of Science in Cyber Security Degree

On behalf DataChambers, I am writing to express support for UNC Charlotte's proposal to establish a Master of Science in Cyber Security degree. This program will serve as an important source of cyber security talents for DataChambers as our offices grow in the Charlotte region. It will also serve, very well, other companies in the Charlotte region and beyond.

DataChambers has been collaborating with the College of Information and Informatics in the past few years by attending and financially supporting the Cyber Security Symposium, promoting a Big Data Hackathon, an event to be held on campus in the Portal Building, and our Charlotte region General Manager, a UNCC Graduate, sits on the Alumni Board of Directors of the University. As we grow our offices in Charlotte we will always evaluate local talent such as graduates from UNC Charlotte. Through the collaboration my colleagues at DataChambers have been very impressed by the quality of graduates from UNC Charlotte, and from the College of Computing and Informatics in particular.

As a company that has a focus around data security and providing our clients safe and consistent access to their data, having a better understanding of all facets of cyber security are an important aspect in the success of our business. Each day companies are threatened in one way or another by cyber security attacks. The best way to defend against these attacks is to gain the highest level of understanding of where the attacks are materializing, the target source of the attacks and then how to put policies and technologies in place to defend against those threats.

DataChambers supports UNC Charlotte and appreciates the College of Computing and Informatics' effort in establishing a Master of Science in Cyber Security degree. The new master's degree program will not only provide highly sought-after cyber security professionals for companies in the region including DataChambers, but also help protect the economic future of the state.

Sincerely,

Nicholas L. Kottyan
President & Chief Executive Officer

3310 Old Lexington Rd. Winston-Salem, NC 27107 Telephone- 336-499-6000 Fax 336-499-6060
www.datachambers.com

ORACLE
COMMUNICATIONS

Oracle
Communications Global
Business Unit

5200 Paramount Pkwy
Morrisville, NC 27560

phone +1919.205.6001
fax +1919.205.6986
oracle.com

Dean Yi Deng
College of Computing and Informatics
University of North Carolina at Charlotte
9201 University City Boulevard
Charlotte, NC 28223-0001

Re: New Master of Science in Cyber Security Degree

On behalf of Oracle's Global Communications Business Unit, I am writing to express our enthusiastic support for UNC Charlotte's proposal to establish a Master of Science in Cyber Security degree. This program will serve as an important and reliable source of Cyber Security talents for the industry from an institution we trust to produce candidates of a very high caliber.

Oracle has been collaborating with the College of Information and Informatics since 2012 as a Tera Partner providing scholarships, recruiting for our rigorous Co-Op program in Telecommunications, and participating in many enrichment activities for students. Most recently, I spoke at an informational session with the 49th Security Division, a student organization dedicated to Cyber Security. Not only do we enjoy the privilege of interacting directly with the students, one of our Vice Presidents, Chris Benson, sits on the Dean's Advisory Board. As our participation and collaboration evolves, we continue to be impressed and excited by the candidates UNC Charlotte and the College of Information and Informatics provides us.

Cyber Security is rapidly becoming one of the most challenging aspect of our jobs. Our products exist in premier telecommunications networks around the world. This makes our responsibility to keep them secure, internationally relevant. It's no secret that the software community was plagued by critical bugs in 2014, notably Heartbleed and Shellshock. These security vulnerabilities cost numerous companies money, time, and other resources that would have been much better spent in research and development. The threat of hackers exploiting software weaknesses cannot be ignored. It only makes sense that as attacks are more frequent and more informed, we must make a greater transition from being reactionary to being preventative. That transition requires ethical hackers and cyber security professionals that have an extensive understanding of all aspects of security. After reviewing the proposed curriculum for the Master's program, I deeply believe this will create incredibly valuable cyber security professionals whose impact will extend far past Charlotte and into the global market.

Oracle supports UNC Charlotte and admires the College of Computing and Informatics' effort in establishing a Master of Science in Cyber Security degree. We look forward to the wealth of benefits we will receive—along with our entire industry—once this program is established.

Warmest regards,

Bob Garrell

7910 Crescent Executive Drive
Charlotte, NC 28217
Tel 704-731-3000

TIME WARNER CABLE

Dean Yi Deng
College of Computing and Informatics
University of North Carolina at Charlotte
9201 University City Boulevard
Charlotte, NC 28223-0001

Re: New Master of Science in Cyber Security Degree

On behalf of Time Warner Cable, I am writing to express support for UNC Charlotte's proposal to establish a Master of Science in Cyber Security degree. This program will serve as an important source of cyber security talents for Time Warner Cable in a timely manner. It will also serve very well other companies in and outside the Charlotte region.

Time Warner Cable has been collaborating with the College of Information and Informatics in the past six years by accepting student interns and collaborating on the Information Security Symposium. We have hired three graduates from UNC Charlotte in the past four years alone. Through the collaboration my colleagues at Time Warner Cable have been very impressed by the quality of graduates from UNC Charlotte, and from the College of Computing and Informatics in particular.

With the number of security breaches resulting in an increase of attention on regulation from the government and within various industries, the need to ensure that a company has competent security resources to identify and manage security risks across the enterprise is significant. As one of the largest broadband providers within the country, Time Warner Cable has a large infrastructure and customer base that requires continuous review and response capabilities to ensure that Time Warner Cable provides a set of trusted services to its customers and a safe work environment for its employees.

Time Warner Cable supports UNC Charlotte, and appreciates the College of Computing and Informatics' effort in establishing a Master of Science in Cyber Security degree. The new master's degree program will not only provide highly sought-after cyber security professionals for companies in the region including Time Warner Cable, but also help protect the economic future of the state.

Sincerely,

Prentis C Brooks III
Director, Cyber Security
Time Warner Cable

WOMBLE CARLYLE SANDRIDGE & RICE
A LIMITED LIABILITY PARTNERSHIP

One Wells Fargo Center
301 South College Street
Suite 3500
Charlotte, NC 28202-6037

Telephone: (704) 331-4900
Fax: (704) 331-4955
www.wcsr.com

Theodore F. Claypoole
Direct Dial: (704) 331-4910
Direct Fax: (704) 338-7816
E-mail: tclaypoole@wcsr.com

February 11, 2015

Dean Yi Deng
College of Computing and Informatics
University of North Carolina at Charlotte
9201 University City Boulevard
Charlotte, NC 28223-0001

Re: New Master of Science in Cyber Security Degree

Dear Dean Deng:

On behalf of Womble Carlyle, I am writing to express support for UNC Charlotte's proposal to establish a Master of Science in Cyber Security degree. This program will serve as an important source of cyber security talents for professional organizations and their clients. It will also serve very well other companies in the charlotte region and beyond.

Womble Carlyle has been collaborating with the College of Information and Informatics in the past 16 years, sponsoring and participating in data security progams. Through the collaboration my colleagues at Womble Carlyle have been very impressed by the quality of graduates from UNC Charlotte, and from the College of Computing and Informatics in particular.

Cyber security is vital to the legal and accounting sector as we hold privileged information and secrets from our clients. Our business is based on trust and confidence, which cannot exist without appropriate security.

Womble Carlyle supports UNC Charlotte, and appreciates the College of Computing and Informatics' effort in establishing a Master of Science in Cyber Security degree. The new master's degree program will not only provide highly sought-after cyber security professionals for companies in the region, but also help protect the economic future of the state.

Best regards,

WOMBLE CARLYLE SANDRIDGE & RICE
A Limited Liability Partnership

Theodore F. Claypoole

Attachment E. Survey of Information Technology Professionals

UNC CHARLOTTE

COLLEGE OF COMPUTING AND INFORMATICS

Department Software Information Systems
9201 University City Boulevard, Charlotte, NC 28223-0001
t/ 704.687.8658 www.sis.uncc.edu

MS in Cyber Security

CCI is planning a new Master of Science in Cyber Security to equip students with the latest knowledge and skills in Cyber Security and Privacy. The students in our program are expected to be employed or will be employable by both businesses and governments that have important information assets to be protected from increasingly sophisticated cyber-attacks. A brief outline of the MS is below.

(a) Students are required to complete the following four common core courses (12 credit hours):
ITIS 6200 Principles of Information Security and Privacy (3 credit hours)
ITIS 5250 Computer Forensics (3 credit hours)
ITIS 6167 Network Security (3 credit hours)
ITIS 6240 Applied Cryptography (3 credit hours)

(b) Students are required to complete three courses (9 credit hours) selected from the following:
IT IS 5220 Vulnerability Assessment and System Assurance (3 credit hours)
ITIS 5221 Secure Programming and Penetration Testing (3 credit hours)
ITIS 6150 Software Assurance (3 credit hours)
ITIS 6210 Access Control and Security Architecture (3 credit hours)
ITIS 6220 Data Privacy (3 credit hours)
ITIS 6230 Information Infrastructure Protection (3 credit hours)
IT IS 6250 Open Source Security Systems (3 credit hours)
ITIS 6320 Cloud Data Storage (3 credit hours)
ITIS 6362 Information Technology Ethics, Policy, and Security (3 credit hours)
ITIS 6420 Usable Security and Privacy (3 credit hours)

(c) Students are required to complete three additional courses (9 credit hours) offered by the College of Computing and Informatics as electives.

(d) As a capstone experience, each student will complete an internship, a Maser's Thesis, or a graduate report.

Please help us understand the demand for our graduate programs related to cyber security by answering a few questions.

- How likely is it that you would recommend the MS Cyber Security to your employees or colleagues?
  Extremely likely
  Very likely
  Moderately likely
  Slightly likely
  Not at all likely

- How likely is it that would you enrol in the MS Cyber Security?
  Extremely likely
  Very likely
  Moderately likely
  Slightly likely
  Not at all likely

- How likely are employees/colleagues/yourself to attend a part time program with classes scheduled in the evenings and weekends?
  Extremely likely
  Very likely
  Moderately likely
  Slightly likely
  Not at all likely

- How likely are employees/colleagues/yourself to attend full time (3 courses per semester) with classes scheduled in the evenings and weekends?
  Extremely likely
  Very likely
  Moderately likely
  Slightly likely
  Not at all likely

- Which topics in Cyber Security are included in our program that you think are essential?

- Are there topics in Cyber Security that you would like to see in our program?

CCI is also planning to offer Graduate Certificates for students that do not wish to commit to a Masters degree. If a student completes 2 Certificates, s/he may apply these to a Masters degree.

Topic Areas for Graduate Certificates

1. Information Security and Privacy
2. Management of Information Technology
3. Database Management and Discovery
4. Human Computer Interaction
5. Network Security
6. Software Security
7. Emerging Technologies

- If the above Certificates were available how likely is it that would you recommend at least one of them to your employees?

  Extremely likely
  Very likely
  Moderately likely
  Slightly likely
  Not at all likely

- List the topics most relevant to your company.

Attachment F. **Faculty Roster Form**

Faculty Roster Form
Qualifications of Full-Time and Part-Time Faculty

Name of Institution: University of North Carolina at Charlotte

Name of Primary Department, Academic Program, or Discipline: College of Computing & Informatics

Academic Term(s) Included: Spring 2016 **Date Form Completed: 2/01/16**

1	2	3	4
NAME (F, P[1])	**COURSES TAUGHT Including Term, Course Number & Title, Credit Hours (D, UN, UT, G[23])**	**ACADEMIC DEGREES& COURSEWORK Relevant to Courses Taught, Including Institution & Major List specific graduate coursework, if needed**	**OTHER QUALIFICATIONS & COMMENTS Related to Courses Taught**
Ehab Al-Shaer (F)	ITIS6230 Info Infrastructure Protection, 3 (G)	PHD (Computer Science), Old Dominion University MS (Computer Science), Northeastern University BS (Computer Engineering), King Fahad Univ Petro/Mrnl	
Bill Chu (F)	ITIS3200 Intro to Info Security & Priv, (UT) 3 ITIS3650 Senior Project, (UT) ITIS4221/ ITIS5221 Secure Prog Penetr Testing, 3 (G) ITIS6999 SFS Research, 3 (G)	PHD (Computer Science), University of MD-College Park MS (Computer Science), University of MD-College Park BS (Electrical and Electronics Egr), University of MD-College Park	
Heather Lipford (F)	ITIS4420/ ITIS6420 Usable Security and Privacy, 3 (G)	PHD (Computer Science), Georgia Institute of Tech BS (Computer Science), Michigan State University	

[1] F, P: Full-time or Part-time
[2] D, UN, UT, G: Developmental, Undergraduate Nontransferable, Undergraduate Transferable, Graduate

Mohamed Shehab (F)	ITCS4180/ ITCS5180/ ITIS4180/ ITIS5180 Mobile Application Development, 3 (G)	PHD (Computer Engineering), Purdue Univ-West Lafayette BS (Electrical and Electronics Egr), United Arab Emirates Univ	
Meera Sridhar (F)	ITIS6150/ ITIS8150 Software Assurance, 3 (G)	PHD (Computer Science), Texas At Dallas,U of MS (Computer Science), Carnegie Mellon University BS (Computer Science), Carnegie Mellon University	
Weichao Wang (F)	ITIS6200/ ITIS8200 Prin Info Security & Privacy, 3 (G)	PHD (Computer Science), Purdue Univ-West Lafayette MS (Computer Science), Purdue Univ-West Lafayette MS (Computer Science), Tsinghua University BS (Computer Science), Tsinghua University	
Yongge Wang (F)	ITIS6320/ ITIS8320 Cloud Data Storage, 3 (G)	PHD (Mathematics and Computer Sci), Universitat Heidelberg MS (Mathematics), Nankai University	