2014-2015 LONG SIGNATURE SHEET

UNC CHARLOTTE

Proposal Number: SIS 2-5-2016

Proposal Title: _New M.S. in Cybersecurity_____

Originating Department: __Software and Information Systems_____

TYPE OF PROPOSAL: UNDERGRADUATE_____ GRADUATE___X___ UNDERGRADUATE & GRADUATE____
(Separate proposals sent to UCCC and Grad. Council)

DATE RECEIVED	DATE CONSIDERED	DATE FORWARDED	ACTION	SIGNATURES
			Approved	**DEPARTMENT CHAIR** [print name here:] MARY LOU MAHER
			Approved	**COLLEGE CURRICULUM COMMITTEE CHAIR** [print name here:] YAORONG GE
			Approved	**COLLEGE FACULTY CHAIR (if applicable)** [print name here:] Yu Wang
			Approved	**COLLEGE DEAN** [print name here:] M.A. PEREZ-QUINONES
			Approved	**GENERAL EDUCATION** (if applicable; for General Education courses) [print name here:]
			Approved	**HONORS COLLEGE** (if applicable; for Honors courses & programs) [print name here:]
			Approved	**UNDERGRADUATE COURSE & CURRICULUM COMMITTEE CHAIR** (for undergraduate content)
2/5/16	3/1/16	3/23/16	*Approved*	**GRADUATE COUNCIL CHAIR** (for graduate content) Dennis Livesay
				FACULTY GOVERNANCE ASSISTANT (Faculty Council approval on Consent Calendar)
				FACULTY EXECUTIVE COMMITTEE (if decision is appealed)

Revised 05/06/14
OAA/mjw

UNC CHARLOTTE

LONG FORM
COURSE AND CURRICULUM PROPOSAL

---

*To:

From: Heather Lipford

Date: February 5, 2016

Re: new M.S. in Cybersecurity

The Long Form is used for major curriculum changes. Examples of major changes can include:

Undergraduate: Major changes include new undergraduate degrees, minors, concentrations, certificates, and changes to more than 50% of an existing program (Note: changing the name of an academic department does not automatically change the name(s) of the degree(s). The requests must be approved separately by the Board of Governors.)

Graduate: Major changes include new graduate courses, major changes to an existing graduate course or major changes to an existing graduate program

Submission of this Long Form indicates review and assessment of the proposed curriculum changes at the department and collegiate level either separately or as part of ongoing assessment efforts.

*Proposals for undergraduate courses and programs should be sent to the Undergraduate Course and Curriculum Committee Chair. Proposals related to both undergraduate and graduate courses, (e.g., courses co-listed at both levels) must be sent to both the Undergraduate Course and Curriculum Committee and the Graduate Council.

I. HEADING AND PROPOSAL NUMBER

A. HEADING. Place a three line double-spaced heading containing the following information at the top of the first page of the proposal and beginning at the left margin:

University of North Carolina at Charlotte

(Specify: New or Revised; Undergraduate or Graduate; or Undergraduate and Graduate)

Course and Curriculum Proposal from: (Name of Originating Unit)

B. PROPOSAL NUMBER. Place the proposal number in the upper right corner of page one of the proposal. The proposal number will consist of the abbreviation of the originating unit and the date the proposal was approved by the unit, e.g., BIO 7-24-02. If more than one proposal is passed on a specific date, assign alpha suffixes to distinguish them (e.g., BIO 7-24-02a and BIO 7-24-02b). Submit multiple courses as a single proposal when possible.

C. TITLE. Indicate a brief descriptive title for the proposal, e.g., "*Establishment of a Minor in Communication Studies.*"

II. CONTENT OF PROPOSALS

A. PROPOSAL SUMMARY.

1. **SUMMARY**. State clearly and concisely the actions proposed (e.g., "the Biology Department proposes to add four new elective courses to the undergraduate curriculum: BIO 2222, BIO 3456, BIO 2345, and BIO 3210).

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.

B. JUSTIFICATION.

1. Identify the need addressed by the proposal and explain how the proposed action meets the need.

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.

2. Discuss prerequisites/corequisites for course(s) including class-standing, admission to the major, GPA, or other factors that would affect a student's ability to register.

A student in the Master's program must maintain a minimum GPA of 3.0 for continued enrollment in the program

3. Demonstrate that course numbering is consistent with the level of academic advancement of students for whom it is intended.

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.

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. In general, how will this proposal improve the scope, quality and/or efficiency of programs and/or instruction?

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.

5. If course(s) has been offered previously under special topics numbers, give details of experience including number of times taught and enrollment figures.

C. **IMPACT.** Changes to courses and curricula often have impacts both within the proposing department as well as campus-wide. What effect will this proposal have on existing courses and curricula, students, and other departments/units? Submit an Impact Statement that fully addresses how you have assessed potential impacts and what the impacts of this proposal might be. Consider the following:

1. What group(s) of students will be served by this proposal? (Undergraduate and/or graduate; majors and/or non-majors, others? Explain). Describe how you determine which students will be served.

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.

2. What effect will this proposal have on existing courses and curricula?

a. When and how often will added course(s) be taught?

The program will use existing courses.

b. How will the content and/or frequency of offering of other courses be affected?

The department currently offers 13 courses in cyber security, requiring no additional courses to establish the degree.

c. What is the anticipated enrollment in course(s) added (for credit and auditors)?

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

d. How will enrollment in other courses be affected? How did you determine this?

Enrollment of international students in the existing the Master of Science 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.

Other courses for the MSIT should not be impacted. There is currently capacity in existing security courses for the program introduction, and additional sections will be added as the program grows.

e. Identify other areas of catalog copy that would be affected, including within other departments and colleges (e.g., curriculum outlines, requirements for the degree, prerequisites, articulation agreements, 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.

(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.

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.

The internship option requires 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.

III. Resources Required to Support Proposal.

When added resources are not required, indicate "none". For items which require "none" explain how this determination was made.

A. Personnel. Specify requirements for new faculty, part-time teaching, student assistants and/or increased load on present faculty. List by name qualified faculty members interested in teaching the course(s).

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

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. ~~These faculty will contribute to both the MS in cyber security and the PhD program in Computing and Information Systems.~~ remove - duplicate sentence

B. Physical Facility. Is adequate space available for this course?

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.

C. EQUIPMENT AND SUPPLIES: Has funding been allocated for any special equipment or supplies needed?

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.

This request will be funded by differential tuition.

D. COMPUTER. Specify any computer usage (beyond Moodle) required by students and/or faculty, and include an assessment of the adequacy of software/computing resources by available for the course(s).

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.

E. AUDIO-VISUAL. If there are requirements for audio-visual facilities beyond the standard classroom podiums, please list those here.

None.

F. OTHER RESOURCES. Specify and estimate cost of other new/added resources required, e.g., travel, communication, printing and binding.

See budget below.

G. SOURCE OF FUNDING. Indicate source(s) of funding for new/additional resources required to support this proposal.

PROPOSED BUDGET FOR 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	$ 90,000	$ 138,000	$ 180,000
Recruitment	$ 15,000	$ 10,000	$ 10,000	$ 10,000
Program Workshops/Seminars	$ -	$ 15,000	$ 15,000	$ 15,000
Technology	$ -	$ 27,500	$ 44,000	$ 65,000
TOTAL ADDITIONAL COSTS	**$ 100,000**	**$ 190,000**	**$ 276,000**	**$360,000**

1 Teaching Professor in year 1 and; In future years, new faculty and lab coordinators will be funded from tuition increment funds.

The tuition differential requested is $2000 per semester. The tuition differential will be used to maintain the high quality of the program, specifically to hire faculty, 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 recruitment efforts and because of student demand, 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 a Teaching

Assistant Professor; 15% will be allocated for recruitment costs including printing costs.

IV. CONSULTATION WITH THE LIBRARY AND OTHER DEPARTMENTS OR UNITS

A. LIBRARY CONSULTATION. Indicate written consultation with the Library Reference Staff at the departmental level to ensure that library holdings are adequate to support the proposal prior to its leaving the department. (Attach copy of ***Consultation on Library Holdings***).

Attached.

B. CONSULTATION WITH OTHER DEPARTMENTS OR UNITS. List departments/units consulted in writing regarding all elements outlined in IIC: Impact Statement, including dates consulted. Summarize results of consultation and attach correspondence. Provide information on voting and dissenting opinions (if applicable).

C. HONORS COUNCIL CONSULTATION. In the case of Honors courses or Honors programs indicate written consultation with the Honors Council (if applicable).

V. INITIATION, ATTACHMENTS AND CONSIDERATION OF THE PROPOSAL

A. ORIGINATING UNIT. Briefly summarize action on the proposal in the originating unit including information on voting and dissenting opinions.

Appendix C was considered and approved by the following groups:
Department of Software and Information Systems graduate committee
Department of Software and Information Systems
College of Computing and Informatics graduate committee
College of Computing and Informatics

B. CREDIT HOUR. (Mandatory if new and/or revised course in proposal)
Review statement and check box once completed:

☐ The appropriate faculty committee has reviewed the course outline/syllabus and has determined that the assignments are sufficient to meet the University definition of a credit hour.

C. ATTACHMENTS.

1. CONSULTATION: Attach relevant documentation of consultations with other units.

2. COURSE OUTLINE/SYLLABUS: For undergraduate courses attach course outline(s) including basic topics to be covered and suggested textbooks and reference materials with dates of publication. For Graduate Courses attach a course syllabus. Please see Boiler Plate for Syllabi for New/Revised Graduate Courses.

3. PROPOSED CATALOG COPY: Copy should be provided for all courses in the proposal. Include current subject prefixes and course numbers, full titles, credit hours, prerequisites and/or corequisites, concise descriptions, and an indication of when the courses are to be offered as to semesters and day/evening/weekend. Copy and paste the current catalog copy and use the Microsoft Word "track changes" feature (or use red text with "~~strikethrough~~" formatting for text to be deleted, and adding blue text with "underline" formatting for text to be added).

   a. For a new course or revisions to an existing course, check all the statements that apply:
   ____ This course will be cross listed with another course.
   ____ There are prerequisites for this course.
   ____ There are corequisites for this course.
   ____ This course is repeatable for credit.
   ____ This course will increase/decrease the number of credits hours currently offered by its program.
   ____ This proposal results in the deletion of an existing course(s) from the degree program and/or catalog.
   For all items checked above, applicable statements and content must be reflected in the proposed catalog copy.

   b. If overall proposal is for a new degree program that requires approval from General Administration, please contact the facultygovernance@uncc.edu for consultation on catalog copy.

Catalog copy attached.

4. ACADEMIC PLAN OF STUDY (**UNDERGRADUATE ONLY**): Does the proposed change impact an existing Academic Plan of Study?
☐ Yes. If yes, please provide updated Academic Plan of Study in template format.
☐ No.

5. STUDENT LEARNING OUTCOMES (UNDERGRADUATE & GRADUATE): Does this course or curricular change require a change in Student Learning Outcomes (SLOs) or assessment for the degree program?
☒ Yes. If yes, please provide updated SLOs in template format.
☐ No.

6. TEXTBOOK COSTS: It is the policy of the Board of Governors to reduce textbook costs for students whenever possible. Have

electronic textbooks, textbook rentals, or the buyback program been considered and adopted?

☐ Yes. Briefly explain below.

☒ No. Briefly explain below.

No new courses proposed. Textbooks considered as part of any previous course proposals.

Catalog copy

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.

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

Admissions Requirements

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) Applicants are required to demonstrate a satisfactory score on the aptitude portion of the Graduate Record Examination (GRE) or the Graduate Management Admission Test (GMAT).
4) All applicants are required to submit a statement of purpose as well as letters of recommendation.

Degree Requirements

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.

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.

Core Courses (12 credit hours)

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)

Concentration Courses (9 credit hours)

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.

Elective Courses (9 credit hours)

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.

Capstone Experience

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.

The internship option requires 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.

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**

UNCCHARLOTTE

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

Revised 05/06/14
OAA/mjw