Proposal Format (no new courses are required or proposed for the certificate)

Note: If new courses are required for the certificate, the standard Long Form for course and curriculum changes must be used for the certificate approval process.

TITLE: Graduate Certificate in Network Security, Graduate Certificate in Secure Software Design

ORIGINATING DEPARTMENT: _____Software and Information Systems_____

ADMINISTERING UNIT (if different): _____

First Term Certificate is to be offered ___Spring 2016_____

Primary Contact Name ____Sandra Krause_____

Graduate Program Director Name (if different)_____Heather Lipford_____

A: Summary (include a statement that the certificate is to be implemented using existing courses only.)

The Department of Software and Information Systems proposes 2 new graduate certificates in areas related to cyber security, namely network security and secure software development, to complement our existing certificate in Information Security and Privacy. These two certificates are to be added using existing courses only.

B: Catalog Copy

Graduate Certificate in Network Security

The Graduate Certificate in Network Security provides professionals with an opportunity to advance their knowledge and skills in cyber security for networked systems. The certificate requires fifteen (15) graduate credit-hours of coursework. The certificate may be pursued concurrently with a related graduate degree program at UNC Charlotte.

Program Requirements

The graduate certificate must meet both the University wide graduate certificate requirements as specified in the Graduate Catalogs and the certificate specific requirements of 15 credit hours of coursework. All requirements must be completed within four years of studies, starting from the time when the first course for the certificate is taken. Coursework taken for one graduate certificate may not be counted towards a second graduate certificate.

The Graduate Certificate in Network Security Curriculum requires the successful completion of 15 credit points and has the following components:

- Core (12 credit points)
- Security Elective (3 credit points)

The core courses are:

- ITIS 5250 Computer Forensics
- ITIS 6167 Network Security
- ITIS 6230 Information Infrastructure Protection
- ITCS 6160 Computer Communications and Networks

The elective can be from the following list of approved courses:

- ITIS 5221 Secure Programming and Penetration Testing
- ITIS 6150 Software Assurance
- ITIS 6200 Information Security and Privacy
- ITIS 6210 Access Control and Security Architecture
- ITIS 6220 Data Privacy
- ITIS 6240 Applied Cryptography
- ITIS 6250 Open Source Security Systems
- ITIS 6320 Cloud Data Storage
- ITIS 6362 Information Technology Ethics, Policy, and Security
- ITIS 6420 Usable Security and Privacy

Admission Requirements

This graduate certificate program is open to all applicants who hold a bachelor's degree from an accredited institution in a computing, mathematical, engineering or business discipline, with a minimum overall GPA of 2.8 and Junior/Senior GPA of 3.0, on a 4.0 scale. In addition, applicants are required to have substantial knowledge of data structures and object-oriented programming in C++, C# or Java.

The requirements on GPA may be waived if an applicant is currently enrolled and in good standing in a graduate degree program at UNC Charlotte.

Graduate Certificate in Secure Software Development

The Graduate Certificate in Secure Software Development provides professionals with an opportunity to advance their knowledge and skills in developing software applications that are secure. The certificate requires fifteen (15) graduate credit-hours of coursework. The certificate may be pursued concurrently with a related graduate degree program at UNC Charlotte.

Program Requirements

The graduate certificate must meet both the University wide graduate certificate requirements as specified in the Graduate Catalogs and the certificate specific requirements of 15 credit hours of coursework. All requirements must be completed within four years of studies, starting from the time when the first course for the certificate is taken. Coursework taken for one graduate certificate may not be counted towards a second graduate certificate.

The Graduate Certificate in Secure Software Development Curriculum requires the successful completion of 15 credit points and has the following components:

- Core (9 credit points)

- Security Elective (6 credit points)

The core courses are:

- ITIS 5221 Secure Programming and Penetration Testing
- ITIS 6150 Software Assurance
- ITIS 6420 Usable Security and Privacy

The electives can be selected from the following list of approved courses:

- ITIS 5250 Computer Forensics
- ITIS 5166 Network Based Application Development
- ITIS 5180 Mobile Application Development
- ITIS 6112 Software System Design and Implementation
- ITIS 6167 Network Security
- ITIS 6200 Information Security and Privacy
- ITIS 6210 Access Control and Security Architecture
- ITIS 6220 Data Privacy
- ITIS 6230 Information Infrastructure Protection
- ITIS 6240 Applied Cryptography
- ITIS 6250 Open Source Security Systems
- ITIS 6320 Cloud Data Storage
- ITIS 6342 Information Technology Project Management
- ITIS 6362 Information Technology Ethics, Policy, and Security
- ITCS 6114 Algorithm and Data Structures

Admission Requirements

This graduate certificate program is open to all applicants who hold a bachelor's degree from an accredited institution in a computing, mathematical, engineering or business discipline, with a minimum overall GPA of 2.8 and Junior/Senior GPA of 3.0, on a 4.0 scale. In addition, applicants are required to have substantial knowledge of data structures and object-oriented programming in C++, C# or Java.

The requirements on GPA may be waived if an applicant is currently enrolled and in good standing in a graduate degree program at UNC Charlotte.

1. Will the certificate program be delivered on campus, 100% online program, or a combination? Describe any distance education components in detail.

The certificate will be primarily delivered on campus, although we are developing several online and blended courses.

C: Justification

1. Need for program

Security is one of the key focus areas of the SIS Department. Our current M.S. in Information Technology degree offers a concentration in security. We are also developing an M.S. degree in security, and currently

offer one graduate certificate in general information security and privacy. There is a need to offer more focused certificates that specialize in particular aspects of security to better reflect the focused strengths of our extensive security programs – namely network security and secure software development, and to provide more detailed credentials to students who are interested in these two different aspects of security. The goal of these certificates is to encourage students who wish for specialized knowledge to pursue a more focused set of courses in security, and are perhaps not ready to commit or interested in a full M.S. degree. The certificates may also serve as a recruiting mechanism into the M.S. degree. Students who take two of the security certificates should also be able to meet the course requirements for an M.S. in security. We will be marketing these certificates in particular to regional businesses that have a strong cyber security workforce.

2. Impact statement
   a. What group of students would be served by this certificate?

      Primarily new graduate students in the College of Computing and Informatics

   b. What impact will this certificate have on existing curricula?

      None. All courses are currently offered regularly. As the number of students in the new certificate programs is small relative to the Master's programs, the impact on existing curricula is anticipated to be minimal.

   c. What is the projected annual enrollment for the first five years? Include "new" student enrollment counts and indicate if the program will primarily be pursued by students who are concurrently enrolled in a master's program or only enrolled in the certificate program.

      Combined enrollment for the two certificates:

	2015	2016	2017	2018	2019
New	10	15	20	25	30
Concurrent	5	10	15	15	15
Total	**15**	**25**	**35**	**40**	**45**

   d. Are any new resources required to implement the certificate? If "yes" what are they and how will these needs be met?

      No, all courses are currently offered.

3. Will a tuition increment be charged for this certificate? If "yes", how much?

   Yes. We are requesting the same tuition increment as for our M.S. in Cyber Security degree in preparation - $2000 for a full time student. We request this amount due to the heavy needs for advanced technology, and instruction in that technology, in the program.

D: Student Learning Outcomes (provide SLOs in template format)

See attachment.

E: For an educational program to be eligible for Title IV federal financial aid (unsubsidized student loans), it must lead to a degree, prepare students for further study, or lead to gainful employment. Because certificate programs do not necessarily lead to a degree, the U.S. Department of Education requires institutions to disclose certain information about the programs. If the proposed certificate is approved, it will be subject to annual Gainful Employment approval, disclosure, and most likely reporting requirements as established by the U.S. Department of Education.

F: How will the certificate be evaluated?

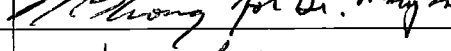
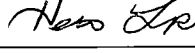
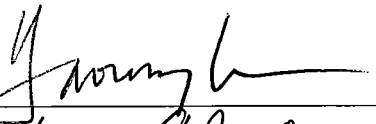
Criteria to be used to evaluate the program include, but are not limited to the following:

- Quality of applicants and entering students
- Progress toward the completion of the certificate
- Number of students that meet student learning outcomes
- Number of graduates from the program
- Successful placement of the majority of graduates in positions in industry or government
- Number of students advancing to a master's program

G: Letters of support or consultation as required. All units sponsoring and participating in the certificate should approve the proposal and provide letters of support.

H: Signatures and date (as appropriate). If the certificate is interdisciplinary, signatures from each participating unit are required.

1. Department Chair
2. Graduate Program Director
3. College Graduate Curriculum Committee Chair (if appropriate)
4. College Dean
5. Graduate Council Chair

Department Chair Mary Lou Maher		2/1/16
Graduate Program Director Heather Lipford		1/27/16
College Graduate Curriculum Committee Yaorong Ge		2/2/2016
College Dean		2/2/2016
Graduate Council Chair		2/3/16

Note: HLR is in lieu of our normal signature form

Procedure for certificate program approval

1. The originating unit files the proposal simultaneously with the appropriate college or colleges and with the Graduate Council. If any issues arise during the review with the college(s) or Graduate Council, the process will stop until the issue is resolved.

2. Approvals by the appropriate college committees and deans, the Graduate Council and the appropriate consultations (if required) are forwarded to the Dean of the Graduate School (DGS). The DGS, having determined that all appropriate consultations have been conducted and that the home college has approved the proposal with wording consistent to that approved by the Graduate Council, forwards the proposal to Academic Affairs to be placed on the FEC Consent Calendar.

3. The proposing unit and the DGS will work cooperatively to ensure timely consideration by by all involved.

4. Certificate programs will be approved for a five-year period. They are reviewed for renewal every five years using the Certificate Renewal Process approved by the Graduate Council (4/4/2006).

5. Certificates can be modified at any time through the same procedure as new programs, or can be ended at an earlier date at the request of the program or discretion of the Provost if they are no longer justified.

Network Security

Student Learning Outcome 1 (knowledge, skill or ability to be assessed)
NSec 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 withstands 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 2
(knowledge, skill or ability to be assessed)

Students will demonstrate understanding of core processes to ensure the security of large networked infrastructures.

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 6150 Information Infrastructure Protection** (required program course), students will learn the core processed that ensure infrastructure security, which includes knowledge of life cycle security, supply chain security, system certification and accreditation, network security administration, and information sharing. Evaluations will be based on core questions regarding these processes on midterm and/or final exams.

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.
ITIS 6230 is offered at least once per year. The instructor specifies a set of questions for mid term and/or final exams . 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 security processes evaluation.

Secure Software Development

Student Learning Outcome 2 (knowledge, skill or ability to be assessed)
Students will demonstrate ability to build a software application that resistant to 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 5221** Secure Programming and Penetration Testing (required program course), students are required to demonstrate understanding of basic techniques and use of tools to build software application that are resistant to attacks. They complete a project where they identify and resolve vulnerabilities in software using a variety of analysis and programming techniques.

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 5221 is offered, both in Fall and Spring semesters. The instructor specifies a set of assignments to help students apply concepts learned to build secure software systems. 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 secure software project evaluation.

Student Learning Outcome 4
(knowledge, skill or ability to be assessed)

Students will demonstrate understanding of core concepts of the secure software development process derived from best practices.

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.

ITIS 6150 Software Assurance (required program course), covers key concepts on secure software development process including secure software development life cycle, threat modeling, secure design, metrics, and maturity model. These will be evaluated by a set of core questions on the midterm and/or final exam.

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.

ITIS 6150 is offered once every academic year. The instructor specifies a set of questions related to the secure software development lifecycle develop and will be given on mid term and/or final exam. 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 secure software development concepts evaluation.