Graduate Curriculum Approval Form
Changes to Degree Programs

Degree (i.e. M.A., Ph.D., etc.):
Name of Program (e.g. Biology)
Program CIP Code
Name of Concentration(s) (e.g. Botany)
Proposed Effective Term (e.g. Spring 2015)
Faculty Contact
Email

<table>
<thead>
<tr>
<th>APPROVALS</th>
<th>Name</th>
<th>Signature</th>
<th>Action</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dept. Chair</td>
<td>Balaji Padmanabhan</td>
<td></td>
<td>☒ Approve ☐ Not approved</td>
<td>9/23/14</td>
</tr>
<tr>
<td>School Committee Chair (if applicable)</td>
<td></td>
<td></td>
<td>☐ Approve ☐ Not approved</td>
<td></td>
</tr>
<tr>
<td>College Committee Chair</td>
<td>Dan Bradley</td>
<td></td>
<td>☒ Approve ☐ Not approved</td>
<td>9/24/14</td>
</tr>
<tr>
<td>College Dean/Associate Dean</td>
<td>Kaushal Chari</td>
<td></td>
<td>☒ Approve ☐ Not approved</td>
<td></td>
</tr>
<tr>
<td>Concurrence*</td>
<td>Dept: Chair:*</td>
<td></td>
<td>☐ Not Applicable ☐ Concur ☐ Doesn't concur ☐ Comments attached</td>
<td></td>
</tr>
<tr>
<td>Grad Council</td>
<td>Chair or designee</td>
<td></td>
<td>☐ Approve ☐ Not approved</td>
<td></td>
</tr>
<tr>
<td>Graduate Studies</td>
<td>GS Dean or designee</td>
<td></td>
<td>☐ Approve ☐ Disapprove</td>
<td></td>
</tr>
</tbody>
</table>

1. Summary of Changes – Select all that apply:
   - Change Admission Deadlines (no other changes)
   - Change Admissions to “fall admissions only” (no other changes)
   - Change Admission Requirements
   - Change Degree Program Requirements (including Concentration requirements)
   - Update Course Numbers in Program Listing (i.e. from Selected Topics to Permanent Numbers) (no other changes)
   - Other – please specify:

2. Briefly - Why are these changes necessary or desired?
The proposed changes allow students in the Information Assurance concentration of the MS in Cybersecurity additionally obtain the Graduate Certificate in “Compliance, Risk, and Anti Money Laundering.” This certificate was recently approved by the College of Business and targets a workforce need in the market for these students.

3. Attach the current Catalog Copy, with the requested revisions shown using Track Changes. If the only change is to the Admission Deadline revised Catalog Copy is not required – just specify the change below. All other changes require Catalog Copy.

Once College has approved, scan and email this Approval Form, and the revised Catalog Copy in Word to Graduate Studies by the deadline posted online http://www.grad.usf.edu/graduate-council.php. For questions, contact csb@usf.edu
CYBERSECURITY PROGRAM

Master of Science (M.S.) Degree

DEGREE INFORMATION

Program Admission Deadlines:

Domestic Students:
- **Fall**: February 15
- **Spring**: October 15
- **Summer**: February 15

International Students living outside the U.S. Deadline for immigration documents, etc.:
- **Fall**: February 15
- **Spring**: September 15
- **Summer**: February 15

Minimum Total Hours: 30*

Program Level: Masters

CIP Code: 43.0303

Dept Code: ---

Program (Major/College): CYS / GS

Effective: Fall 2014

Concentrations
- Digital Forensics (CYC)
- Computer Security Fundamentals (CYF)
- Cyber Intelligence (CYI)*
- Information Assurance (CIA)

*Cyber Intelligence requires 33 minimum total hours

CONTACT INFORMATION

College: Graduate Studies
Department: Institute for Secure and Innovative Computing
Contact Information: [www.grad.usf.edu](http://www.grad.usf.edu)

PROGRAM INFORMATION

The Master of Science in Cyber Security is an interdisciplinary program that utilizes talent across the Colleges of Business, Engineering, Arts & Sciences, and Behavioral and Community Sciences. The program prepares students for leadership, managerial and domain-specific roles in Cyber Security and for employment in managerial and operational positions that require quick analytical thinking, decision-making under uncertainty regarding critical resources, and domain-specific technical skills for managing secure operations. Specifically, based on the design of the concentrations and the core of this program, the program is also expected to prepare students for 1) intelligence positions that require innovative, analytical, decision-making, and technical skills for providing cyber security intelligence, 2) information assurance positions that require secure management of information and data transferred, used, stored, and processed in information systems, 3) law enforcement positions that are required to deal more and more with cyber-crimes, and 4) cyber security positions that require deep technical skills in the security domain.

Because this is a graduate-level program, to ensure that students possess the foundational knowledge for academic success, students admitted to this program are most likely to be successful if they have academic or work experience in the areas of C/C++ programming, computer networks, operating-system design, algorithms, data structures, and computer organization. An undergraduate degree in computer science, computer engineering, MIS, or IT is recommended for admission.

Accreditation:
Accredited by the Commission on Colleges of the Southern Association of College and Schools
Major Research Areas:

ADMISSION INFORMATION

Must meet University requirements (see Graduate Admissions) as well as requirements listed below

Undergraduate Degree: An applicant must have one of the following (a, b, or c):

a) A bachelor’s degree from a regionally accredited institution with a “B” average or better in all work attempted while registered as an undergraduate, degree-seeking student.
b) A bachelor’s degree with a “B” average or better from a regionally accredited institution and a previous graduate degree with a “B” average or better from a regionally accredited institution.
c) The equivalent bachelors and/or graduate degrees from a foreign institution.

English Language Proficiency: Applicants whose native language is not English or who have earned degrees from countries where English is not the official language must also demonstrate proficiency in English in one of the following ways:

- By providing scores of 79 or higher on the internet based Test of English as a Foreign Language (TOEFL iBT)
- By providing a score of 6.5 or higher on the International English Language Testing System (IELTS).
- By providing a score of 53 or higher on the Pearson Test of English Academic (PTE-A)
- By earning a score of 500 (153 or equivalent at 62nd percentile) on the GRE Verbal exam.
- By earning a baccalaureate or higher degree at a regionally accredited institution in the U.S.
- By earning a baccalaureate or equivalent degree at a foreign institution where English is the language of instruction (must be documented on the transcript or on an official Certificate of Medium of Instruction from the Institution).

Additional Requirements
 Applicants also must submit the following with their application:

- Official transcripts with confirmation that the applicant has received a bachelor’s degree from a regionally-accredited university
- A 250-500 word essay in which the student describes her or his academic and professional background, reasons for pursuing this degree, and professional goals pertaining to cybersecurity
- Two letters of recommendation, at least one of which should come from a faculty member familiar with the applicant’s academic performance and potential. If the applicant is unable to provide the letter from a former professor, with approval from the program’s admission coordinator, letters from other professional sources will be accepted
- Scores from the GRE General Test. Applicants with degrees from regionally-accredited U.S. universities, however, may request a waiver of the GRE requirement.

The program admissions committee may request a video or phone admission interview or additional documentation, if necessary.
DEGREE PROGRAM REQUIREMENTS

Total Minimum Hours: 30 credit hours

Core Requirements – 12 hours
Concentrations – 12-18 hours
Electives – 0-3 hours (depending on concentration)
Practicum – 3 hours

CORE REQUIREMENTS - 12 hours
- CNT 5004 Data Communications /Network 3
- CIS 5362 Cryptography 3
- ISM 6328 Basics of Information Security and Risk Management 3
- ISM 6930 Decision Processes for Business Continuity and Disaster Recovery 3

CONCENTRATIONS - 12-18 hours
Students select from the following concentrations:

Digital Forensics - 15 hours
Area of emphasis on forensics following attacks on critical infrastructure systems.
- CJE 6688 Cybercrime and Criminal Justice 3
- CJE 6623 Digital Evidence Recognition 3
- CJE 6624 Introduction to Digital Evidence 3
- CJE 6625 Network Forensic Criminal 3
- CJE 6626 Digital Forensic Criminal Investigations 3

Computer Security Fundamentals - 12 hours –Not Yet Available
Area of emphasis in operating secure critical infrastructure systems.
Students select from the following options to complete the 12 hour requirement:
- EEL 6764 Computer Architecture 3
- COP 6611 Operating Systems 3
- COT 6405 Graduate Algorithms 3
- CIS 6930 Special Topics: Computer Systems Security (New Course Number Pending) 3

For the remaining course for this concentration, students may select a course from the other concentrations.

Cyber Intelligence - 18 hours
Area of emphasis in methodologies for analyzing threats against critical systems
Note – this concentration requires a minimum of 33 total program hours.
- ENC 6261 Analytic Communication 3
- LIS 6700 Information Strategy & Decision Making 3
- LIS 6701 Core Concepts in Intelligence 3
- LIS 6702 Advanced Intelligence Analytic Methods 3
- LIS 6703 Cyber intelligence 3
- LIS 6704 Advanced Cyber intelligence 3

Information Assurance - 125 hours
Area of emphasis in designing and managing secure critical information and infrastructure systems.
The concentration requires students to take 4 out of the following five courses as well as an additional elective course.
- ISM 6145 Seminar on Software Testing 3
- ISM 6266 Software Architecture 3
- ISM 6124 Advanced Systems Analysis and Design 3
ISM 6316 Project Management 3
ISM 6218 Advanced Database Administration 3
BUL 5XXX Risk Management and Legal Compliance 3
ACG 6457 Accounting Systems Audit, Control and Security 3
ISM 6137 Statistical Data Mining 3

For the additional elective in the Information Assurance concentration, students may take ISM 6145 (Seminar on Software Testing), ISM 6316 (Project Management), ACG 6936 (Forensic Accounting and Legal Issues) or any other elective pre-approved by the College of Business.

Students in the Information Assurance concentration can also receive a Graduate Certificate in “Compliance, Risk, and Anti-Money Laundering” if their course selection includes BUL 5XXX, ACG 6936, ACG 6457 and ISM 6137 with a GPA of at least 3.0 in these four courses.

The information below applies to all concentrations in the program.

Additional Elective Courses - 3 hours
Students take one elective offered by the other concentrations within the degree program, or other graduate courses approved by faculty as meeting the requirements for the degree. Because the Cyber Intelligence Concentration requires credit 18 hours, student in that concentration do not take an elective. The additional elective course for the Information Assurance concentration can be taken as specified above in the description of the Information Assurance concentration.

Comprehensive Exam
During the semester in which the student is scheduled to graduate, the student will be required to submit an electronic portfolio demonstrating completion of core program competencies in cybersecurity and in the area of concentration. This competency-based portfolio will substitute for the written comprehensive exam because the portfolio permits the capstone assessment to align exactly with the degree program’s objectives. Each objective in the portfolio is reviewed and rated by program faculty for Content (demonstrating knowledge of accepted practices, procedures, and trends in the field) and Critical Thinking (ability the student’s ability to analyze a problem, organize a response, synthesize perspectives, and draw practical, testable conclusions)

Non-Thesis
Because the primary aim of the M.S. in Cybersecurity is to train highly skilled practitioners for the workforce, the Degree does not include a research thesis requirement.

Practicum - 3 hours
Satisfactory completion of a three (3) credit hour applied learning experience (practicum) is a core degree requirement for all students pursuing the M.S. in Cybersecurity. The practicum experience is arranged and managed through the coordinator for the student’s concentration area. The student will register for practicum credit in her concentration area’s home department. Until each department receives final approval for a “practicum” or “field work” course number, some departments will develop a learning plan with the student for the practicum and use the “Independent Study” course mechanism.

- For Information Assurance: ISM 6905 Independent Study
- For Computer Security Fundamentals: CAP 6940 Graduate Practicum
- For Digital Forensics: CCJ 6905 Directed Independent Study
- For Cyber Intelligence: LIS 6946 Supervised Field Work

REGISTRATION PROCESS

When do I register for courses?
After you receive your acceptance letter, your advisor will contact you to go over program details and course information. At that time, you will let your advisor know which courses you want to register for that term.

How do I register for courses?
Your advisor will handle your course registration for you.
You will NOT register through OASIS, the USF's student information system.

Do I get a registration confirmation?
Once you are registered for your courses, you will receive an email confirmation and can view your course registration through OASIS.

COURSES
See http://www.ugs.usf.edu/sab/sabs.cfm