SECTION 18

COLLEGE OF GRADUATE STUDIES

(ADMINISTERED BY THE OFFICE OF GRADUATE STUDIES)

Changes to Note

There were no curricular changes for the College of Graduate Studies for 2017-2018

University of South Florida
Office of Graduate Studies (College of Graduate Studies)
4202 E. Fowler Ave ALN226
Tampa, FL 33620

Web address: http://www.grad.usf.edu/
Phone: 813-974-2846
Fax: 813-974-5762

College Dean: Dwayne Smith, Ph.D.
Associate Dean: Ruth Bahr, Ph.D.

Mission Statement:
The University of South Florida Office of Graduate Studies serves as the University hub of leadership for graduate education producing global leaders, one scholar at a time.

College Information:
The College of Graduate Studies is housed in the Office of Graduate Studies and serves as the College for newly developed interdisciplinary programs. In the past programs have included the Applied Behavior Analysis (MA), Cancer Biology (Ph.D.), Entrepreneurship in Applied Technologies (MS), and Global Sustainability (MA), which are now housed in other colleges.

Degrees, Majors, Concentrations

Master of Science (M.S.)
Cybersecurity (CYS)
- Digital Forensics (CYC)
- Computer Security Fundamentals (CYF)
- Cyber Intelligence (CYI)
- Information Assurance (CIA)

CYBERSECURITY

Master of Science (M.S.) Degree

DEGREE INFORMATION

Priority Admission Application Deadlines:

Fall	February 15
Spring	October 15
Summer	February 15

International applicant deadlines:
http://www.grad.usf.edu/majors

Minimum Total Hours:	30*
Level:	Masters
CIP Code:	43.0303
Dept Code:	---
Major/College Codes:	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

MAJOR INFORMATION

The Master of Science in Cybersecurity is an interdisciplinary major that utilizes talent across the Colleges of Business, Engineering, Arts & Sciences, and Behavioral and Community Sciences. The major prepares students for leadership, managerial and domain-specific roles in Cybersecurity 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 major, the major is also expected to prepare students for 1) intelligence positions that require innovative, analytical, decision-making, and technical skills for providing cybersecurity 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) cybersecurity positions that require deep technical skills in the security domain.

Because this is a graduate-level major, to ensure that students possess the foundational knowledge for academic success, students admitted to this major 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. Note: For the Information Assurance Concentration it is recommended that students have a background in accounting information systems, database management, and systems analysis and design.

Major Research Areas:
Cyber, Cybersecurity, Cyber Security, Information Assurance, Secure Software, Information, Analytics, Intelligence, Computer, Network, IT, Software, Testing, Security, Analytic Communication, Data Communications, Cryptography, Information Security, Risk Management, Business Continuity, Disaster Recovery, Digital Forensics, National Security

ADMISSION INFORMATION

Must meet University requirements (see Graduate Admissions) as well as requirements for admission to the major, 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
- Current Resume or CV
- 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 graduate admissions committee may request a video or phone admission interview or additional documentation, if necessary.

CURRICULUM REQUIREMENTS

Total Minimum Hours: **30 credit hours**

Core Requirements – 12 hours
Concentrations – 15-18 hours
Practicum – 3 hours

Core Requirements - 12 hours

EEL 6935	3	Special Topics: Data Networks, Sys & Securities (Proposed EEL 6808; pending SCNS approval)
MAT 5932	3	Special Topics: Applied Cryptography
ISM 6328	3	Information Security and Risk Management
ISM 6930	3	Special Topics: Decision Processes for Business Continuity and Disaster Recovery

Concentrations - 15-18 hours
Students select from the following concentrations:

Digital Forensics - 15 hours
Area of emphasis on forensics following attacks on critical infrastructure systems.

CJE 6688	3	Cybercrime and Criminal Justice
CJE 6627	3	Digital Evidence Recognition and Collection
CJE 6624	3	Introduction to Digital Evidence
CJE 6625	3	Network Forensic Criminal Investigations
CJE 6626	3	Digital Forensic Criminal Investigations

Computer Security Fundamentals - 15 hours
Area of emphasis in operating secure critical infrastructure systems.

Students select from the following options to complete the 12 hour requirement:

EEL 6764	3	Principles of Computer Architecture
COP 6611	3	Operating Systems
COT 6405	3	Introduction to the Theory of Algorithms
CIS 6930	3	Special Topics: Computer Systems Security (New Course Number Pending)

For the remaining 3 hours 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	3	Professional and Technical Communication
LIS 6700	3	Information Strategy & Decision Making
LIS 6703	3	Core Concepts in Intelligence
LIS 6702	3	Advanced Intelligence Analytic Methods
LIS 6709	3	Cyber Intelligence
LIS 6670	3	Advanced Cyber intelligence

Information Assurance - 15 hours
Area of emphasis in securing critical information and systems. The concentration requires students to take four out of the following five courses as well as an additional elective course.

ISM 6124	3	Advanced Systems Analysis and Design
ISM 6218	3	Advanced Database Management
BUL 5842	3	Risk Management and Legal Compliance
ACG 6457	3	Accounting Systems Audit, Control and Security
ISM 6137	3	Statistical Data Mining

For the additional elective in the Information Assurance Concentration, students may take:

ISM 6145	3	Seminar on Software Testing
ISM 6316	3	Project Management
ACG 6688	3	Forensics Accounting and the Legal Environment

Or any other elective pre-approved by the Muma College of Business Information Assurance Concentration Director.

The information below applies to all concentrations in the major:

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 major 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 graduate 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 IT Graduate Practicum
- For Digital Forensics: CCJ 6905 Directed Independent Study
- For Cyber Intelligence: LIS 6946 Supervised Field Work

COURSES

See http://www.ugs.usf.edu/course-inventory/