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): **--- / GS**

Concentrations
Cyber Crime (---)
Cyber Fundamentals (---)
Cyber Intelligence (---)
Information Assurance (---)

CONTACT INFORMATION

College: Graduate Studies
Department: **Institute for Secure and Innovative Computing**
Contact Information: 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.

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

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 listed below

Program Admission Requirements
The USF admission committee will consider the strength of each applicant based on the entire completed application.

- Bachelor's degree from a regionally accredited institution required
- Official Transcripts
- GMAT (preferred), GRE or MCAT scores
- Relevant professional work experience
- Recommendation letters
- A statement of purpose
- Community or volunteer service
- Any other information that helps ensure the potential success of the applicant in the program.
- Applicants whose native language is not English or who have not earned a degree in the United States must also submit TOEFL scores earned within two (2) years of the desired term of entry. A minimum total score of 79 on the Internet-based test, 213 on the computer-based test, or 550 on the paper-based test is required. Students' personal characteristics that add to the diversity of the class may also be considered.
- Pre-requisite – students entering the program are required to have one semester equivalent of programming and operating system coursework, among other technical skills that will be determined by the faculty

DEGREE PROGRAM REQUIREMENTS

Total Minimum Hours: **30 credit 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 hours**
Students select from the following concentrations:

Cyber Crime
Area of emphasis on forensics following attacks on critical infrastructure systems.

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

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

Cyber Fundamentals
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
CIS 6930	Special topics: Computer Networks, Fundamental principles and analysis	3
CIS 6930	Special topics: Security & Privacy	3

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

Cyber Intelligence

Area of emphasis in methodologies for complex information processing for critical systems

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

LIS 5937	Visual Information Analytics	3
ENC 6261	Analytic Communication	3
CCJ 6074	Advanced Intelligence Analytic Methods	3
INR 5365	Core Concepts in Intelligence	3
DSC 6600	Cyber intelligence	3
LIS 6758	Information Strategy & Decision Making	3

Information Assurance

Area of emphasis in designing and managing secure critical infrastructure systems.

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

ISM 6145	Seminar on Software Testing	3
ISM 6125	Software Architecture	3
ISM 6124	Advanced Systems Analysis and Design	3
ISM 6316	Project Management	3
ISM 6218	Advanced Database Administration	3

Electives **3 hours**

Students take any electives offered by the other concentrations within the degree program, or other courses approved by faculty as meeting the requirements for the degree.

Comprehensive Exam

During the semester in which the student is scheduled to graduate, she will be required to submit an electronic portfolio demonstrating completion of core program competencies in cybersecurity and in her 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)

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 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 her practicum and use the "Independent Study" course mechanism.

- For Information Assurance: ISM 6905 Independent Study
- For Cyberfundamentals: CAP 6940 Graduate Practicum
- For Cybercrime: CCJ 6905 Directed Independent Study
- For Cyber Intelligence: LIS 6946 Supervised Field Work

COURSES

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