CYBER FORENSICS AND SECURITY, M.S.

The Master's Degree in Cyber Forensics and Security (M.S. CFS) provides students with advanced education and skills in digital forensics and cybersecurity. This advanced, practitioner-focused program is intended to prepare students for the fast-moving and ever--changing environment they will work in. Students will learn advanced skills and techniques to solve investigative and cybersecurity problems using science and technology. The program will prepare students to face sophisticated cybersecurity and investigative challenges and take a leadership role within their organization.

Prospective students will apply for the program at various stages of their careers. Some students will come straight into the program after completing their undergraduate degrees. Other students will be seeking to further their education after several years in the field. As such, there will be two paths into the program. Option A is for those students having recently graduated with an appropriate 4-year degree. Option B is for those applicants having significant work experience in the field. The details for each option are outlined below.

Option A

Option A is intended for applicants that are recent graduates and have less than three years work experience in digital forensics and/or information assurance.

1. **Baccalaureate Degree** - Students admitted to the program must have an appropriate baccalaureate degree from a regionally accredited U.S. institution, or U.S. equivalent.
2. **Grade Point Average** - Students admitted must have an undergraduate GPA of at least 2.8 on a 4.0 scale.
3. **GRE Score** - Applicants must take the GRE. The GRE will be evaluated in combination with the undergraduate GPA.
4. **Personal Statement** - In the Personal Statement, the applicant will describe their background and goals as they relate to the study of digital forensics and information assurance. Successful applicants will articulate how their background has prepared them for success in the program as well as how their goals align with the program's learning objectives.
5. **Letters of Recommendation** - Applicants must submit three letters of recommendation. The letters should attest to the applicant's knowledge, skills, character, and work ethic.

Option B

Option B is intended for applicants that have been out of school for more than three years and have three or more years of documented work experience in digital forensics and/or information assurance/ cybersecurity.

1. **Baccalaureate Degree** - Students admitted to the program must have a baccalaureate degree from a regionally accredited U.S. institution, or U.S. equivalent.
2. **Grade Point Average** - Students admitted must have an undergraduate GPA of at least 2.5 GPA on a 4.0 scale.
3. **Personal Statement** - In the Personal Statement, the applicant will describe their background and goals as they relate to the study of digital forensics and information assurance. Successful applicants will articulate how their background and work experience has prepared them for success in the program as well as how their goals align with the program's learning objectives.
4. **Letters of Recommendation** - Applicants must submit three letters of recommendation. The letters should attest to the applicant's knowledge, skills, character, and work ethic.
5. **Current CV /Resume** - An updated Resume or Curriculum Vitae that includes a detailed work history, education, training, certifications, awards, publications, professional memberships, etc.
6. **Professional Portfolio** -The portfolio must include examples of the applicant's work product and is intended to demonstrate their capacity to successfully complete graduate-level work in digital forensics and cybersecurity. The portfolio could include things such as:
    - Samples of professional writing (redacted reports, grants, SOPs, etc.)
    - Professional Publications (journals, books, articles, etc.)
    - Presentations (slide decks, conference proceedings, etc.)
    - Research

Program Requirements

The M.S. CFS requires 33 total hours of graduate-level coursework. Core courses comprise 27 of the 33-hour total. In addition, students are required to complete six hours of DFIA/CFS technical electives.

Code	Title	Credit Hours
Required Core		
CYBR 530	Cybersec Policies & Mgmt	3
CYBR 542	Cyber Operations	3
CFS 630	Cyber Threat Intelligence	3
CFS 640	Advanced Cyber Forensics	3
CFS 650	Adv Cyber Defense	3
CFS 660	Red Team	3
CFS 665	Cyber Sec IoT and ICS	3
CFS 670	Practicum	3
or CFS 675	Reserach in CFS	
CFS 690	Capstone	3
Technical Electives		**6**
Students must complete 6 credit hours from the following:		
CFS 505	OSINT Practicum I	
CFS 500	Intro to Digital Forensics	
CFS 520	Incident Response	
CFS 545	Mobile and Web Pen Testing	
CFS 548	Multimedia Forensics	
CFS 554	Adv Network Defense	
CFS 561	Applied Cyber Warfare	
CFS 562	Network Forensics	
CFS 564	Network and Cyber Crime	
CFS 567	Mobile Device Forensics	
Students may also choose electives from the following courses offered by the College of Engineering and Computer Sciences:		
CYBR 500	Computer Security Design	
CYBR 530	Cybersec Policies & Mgmt	
CYBR 542	Cyber Operations	

CYBR 615	Cyber Vulnerability Assess	
Total Credit Hours		**33**

Plan of Study

Course	Title	Credit Hours
First Year		
Fall		
CYBR 530	Cybersec Policies & Mgmt	3
DFIA/CFS Technical Elective		3
	Credit Hours	**6**
Spring		
CFS 640		3
CYBR 542	Cyber Operations	3
CFS 665	Cyber Sec IoT and ICS	3
	Credit Hours	**9**
Summer		
Summer I		
DFIA/CFS Technical Elective		3
Summer II		
CFS 670 or CFS 675	Practicum or Reserach in CFS	3
	Credit Hours	**6**
Second Year		
Fall		
CFS 650	Adv Cyber Defense	3
CFS 630	Cyber Threat Intelligence	3
	Credit Hours	**6**
Spring		
CFS 690	Capstone	3
CFS 660	Red Team	3
	Credit Hours	**6**
	Total Credit Hours	**33**