DIGITAL FORENSICS (DFSC)

DFSC 5310. Princple& Policy-Info Assuranc. 3 Hours.
An investigation into the development of security planning and policy formation, risk management, security education, training and awareness programs. This course examines physical and electronic approaches to data protection and derives appropriate assessment strategies for determining the assurance quality of target systems.

DFSC 5315. Network and Cyber Security. 3 Hours.
This course provides the framework and procedures for securing computer systems and data networks. Topics include the methodologies for the design of security systems, establishing security protocols, and the identification of best practices in administration, testing, and response protocols for secure communications systems.

DFSC 5316. File System Forensics. 3 Hours.
This course focuses on the important concepts associated with the structures, encoding, boot process and storage technologies of modern computers, and the implications of those concepts regarding the analysis of volumes and file systems for forensics purposes.

DFSC 5317. Digital Security. 3 Hours.
This course introduces the student to basic security needs. The course will include, but not be limited to examination of individual vs. government privacy issues, federal encryption standards, the different layers of security currently available, cryptography, and strategies for evaluation and selection of security methods.

DFSC 5318. Cyber Law. 3 Hours.
The focus will be on how the law impacts digital security in diverse ways. Discussion will emphasize the concept of criminal intent, the digital victim and address jurisdictional issues and provide an overview of legal terms and issues with which the security manager must address.

DFSC 5325. Organization System Security. 3 Hours.
This course provides advanced study of system security concepts as applied to the protection of organizational systems including (1) principles of security modeling, accountability and access control, (2) the ISO model for network infrastructure design and protection, (3) communication security and control management, (4) auditing and monitoring, (5) incident management, and(6) law, investigations and ethics.
Prerequisite: DFSC 5310.

DFSC 5327. Digital Forensics Investigatn. 3 Hours.
This course explores tools for the recovery of information on hardware or hidden within other formats. Topics also include cryptographic analysis, password recovery, the bypassing of specific target operating systems, and obtaining data from a digital device that has been destroyed.

DFSC 5328. Software Forensic Evidence Mgt. 3 Hours.
Analysis of investigative techniques and tools in the detection, investigation and analysis of digital crimes. This course examines the nature of cyberevidence and the tracking and identification of cybercriminals.

DFSC 5336. Business Continuity Management. 3 Hours.
This course examines identification and assessment of threat, risk, vulnerability and business continuity in case of disaster, as applied to enterprise IT systems. It incorporates the physical safeguards and policies necessary to meet the requirements for the protection of data in a fixed site. This course also discusses techniques and strategies designed to keep enterprise data in service under critical circumstances.

DFSC 5340. Spcl Tpcs In Digital Forensics. 3 Hours.
Topics and courses are selected to suit individual needs of students. The course may be repeated for additional credit.
Prerequisite: Approval by the graduate advisor.

DFSC 6310. Cyber Warfare & Terrorism. 3 Hours.
This course will focus on philosophies, tactics, and targets of cyber terrorist organizations. The course includes discussion of emerging cyber war trends and the roles of the private sector and U.S. Government in responding to, mitigating and preventing electronic offensive actions.

DFSC 6312. Multimedia Forensics. 3 Hours.
This course examines the theory and practice of multimedia security and forensics. Topics include image processing, JPEG compression, audio compression (MP3, Advanced Audio Coding, and VOIP), MPEG compression, multimedia source identification, biometrics, steganography, steganalysis, multimedia forgery detection, and pattern recognition techniques for multimedia analysis, multimedia forensics software, and advances in multimedia forensics.

DFSC 6313. Wireless Network Security. 3 Hours.
This course provides advanced study of the full range of algorithms, mechanisms, and technologies in securing various types of wireless communication networks, such as cellular networks, Wireless Local Area Networks, Bluetooth Networks, Mobile Ad Hoc Networks, and Wireless Sensor Networks. Research and applications will be explored.

DFSC 6347. Directed Mgt & Development Prj. 3 Hours.
This course will provide the rationale and necessity for a full range of security concepts and techniques and how to apply them to multiple operating systems. The course will cover methodologies for the design of operating system security and forensic techniques for operating systems. Also covered will be the identification of best practices in the administration, testing and security for operating systems. Continuous enrollment in DFSC 6347 is required until graduation.
Prerequisite: 24 hours graduate coursework.