CYBERSECURITY AND OPERATIONS (CSO)

CSO 500 — Prin of InfoSec and Fed Law (VAU) (3 credits)
Presents students with the opportunity to explore and discuss information security, to learn about current information security threats and how to protect information. Students will gain experience in the use of network protection mechanisms such as firewalls, intrusion detection systems, and other security tools.

CSO 510 — Data Privacy (VAU) (3 credits)
Introduces the students to research and topics in Data Privacy. Privacy is increasingly becoming critical to both organizations and private citizens. This course explores privacy from various fronts including its impact on businesses. Additionally, students will examine privacy from a global perspective, in particular, how international privacy policies concerning information security compare to those in the US.

CSO 520 — Managing Security Risk (VAU) (3 credits)
A study of the existing risk management frameworks, models, processes and tools to equip students with the theory, science and practical knowledge to operationalize risk management in an organization or government agency.

CSO 530 — Ethical Hacking (VAU) (3 credits)
Presents students with the opportunity to explore and discuss ethical hacking, and to specifically learn about methods used to prevent unauthorized access to networks. Students will gain experience in the use of penetration testing tools, vulnerability assessment tools as well as reporting. Furthermore, students will look at exploits in detail to understand preventative measures.

CSO 540 — Network Security (VAU) (3 credits)
Introduces network firewall security. It will cover basic installation techniques, discuss how to make an intelligent choice of firewall technology and present basic firewall troubleshooting. Moreover, it will cover different intrusion detection systems and their signatures. Students will complete hands-on exercises and case projects for testing and evaluating various firewall techniques.

CSO 550 — Software Security (VAU) (3 credits)
Introduces students to research in foundations of software security. Basic static and dynamic enforcement of security policies to enhance software security will be investigated. Language-based security and tools for specifying security policies for different programming languages will also be discussed.

CSO 565 — Computer Forensics I (3 credits)
Introduces students to the techniques and tools of computer forensic investigations. Students will learn how to utilize computer forensic tools in investigations. The course maps to the objectives of the IACIS certification. Topics include coverage of the latest technology including cell phones, and portable devices.

CSO 580 — Modern Cryptography (VAU) (3 credits)
Introduces students to the foundations of modern cryptography, with an eye toward practical applications. The objective of this course is to provide a foundation of cryptography in an applied manner so that students can grasp its importance in relation to the rest of the information security field. The course covers the principles of number theories and cryptographic algorithms and cryptanalysis.

CSO 585 — Computer Forensics II (VAU) (3 credits)
*Prerequisite Take CSO*565*

Advances student's knowledge of computer forensics and allows students to sit for the ACE certification. Topics include password recovery, network forensics and forensic case investigations. Additionally, students will research current computer forensics issues in a changing digital world.

CSO 595 — Mobile Forensics (VAU) (3 credits)
Prerequisite Take CSO 565

Will familiarize students with mobile devices and technology used by carriers as it relates to mobile forensics. Students will identify data that can be retrieved from mobile devices, such as cell phones, smart phones, and GPS devices. Recovered data will be analyzed and investigated to recreate crime scenes.

CSO 598 — Topic: (3 credits)
Special topics courses in a particular area of information security including, but not limited to, such areas as cloud security, digital forensics, web application security and/or emerging issues in the field. These courses may not be offered on a regular basis.

CSO 600 — Capstone Project/Research (VAU) (3 credits)
The combination of theory, principles, best practices, methodologies, tools, and technologies associated with Information Security and digital forensics. The Capstone seminar uses scholarly research methods to develop analytics, problem- solving, and research skills required to solve a real-world information security challenges.

CSO 601 — Capstone/Research Project 2 (VAU) (3 credits)
*Prerequisite Take CIS*600*

The combination of theory, principles, best practices, methodologies, tools, and technologies associated with Information Security and digital forensics. The Capstone seminar uses scholarly research methods to develop analytics, problem- solving, and research skills required to solve a real-world information security challenges. CIS 600/601 require ISDF students to present their findings/research to an open forum on campus