CSSS - Cybersecurity

CSSS 5000 Introduction to Cybersecurity (3)

This requisite course is designed to provide the student an overview of the major core areas of study they will encounter throughout this program. Introduction of computer system architectures, vulnerabilities, critical infrastructures, the growing threat of social networks, intelligence and counter intelligence, international laws, security policies, privacy and information liability, cyber attacks and counter cyber attacks, encryption, risk assessment, cybersecurity forensics including data gathering and recovery, and a forward look at future cyber technology developments.

CSSS 5100 Secure Software Design and Threat Analysis (3)

Students will be introduced to the concept and process of Threat Modeling as a key enabler for architecting effective and appropriate security for software and information assets. Topics include an in-depth review of the various types of threats against software. Students will learn the basics of building secure software that prevents security vulnerabilities exploited by hackers. Topics covered include buffer overflows, un-validated input, race conditions, access-control problems, authentication or authorization weaknesses, hashing, and other security practices. Students will also learn best practices to avoid most security vulnerabilities. This course also investigates the security traits of many of the top programming languages such as C, C++, C#, Java, Python, PHP, and Ruby.

CSSS 5110 Cybersecurity Communications (3)

Digital communications has grown rapidly and provides increased opportunities to: access information; share and disseminate knowledge; create new innovative services; and compete in a global environment. It presents new opportunities and a growing threat posed by a connected society that can impact critical United States interests. The basics of communication systems, the ISO Layer Model, topologies such as Local-Area-Networks (LANs), Wide-Area-Networks (WANs), World Wide Web and the internet, space-based communications used by the Department of Defense (DoD) and commercial entities, fiber-optics, as well as the rapidly developing personal mobile communication technologies such as Wireless Local Area Network (WiFi). **Prerequisite**: CSSS 5000.

CSSS 5120 Cybersecurity Infrastructures (3)

The impact of September 11, 2001 cemented our attention on physical attacks on United States critical infrastructures. Although still a concern, a growing cybersecurity threat requires additional focus on potential virtual attacks on these same critical infrastructures. Both physical and virtual in capacitance of a critical infrastructure such as the Power Grid, communications and financial transactions can have as great, or greater, impact on our society, Cyber attacks have and can cripple an industry and the services they provide to millions of users. The critical infrastructures identified by the Department of Homeland Security (DHS) are examined from a cybersecurity perspective. **Prerequisite**: CSSS 5000 or CSSS 5100* (*If in the Artificial Intelligence or Data Analytics emphasis).

CSSS 5130 Cybersecurity Intelligence/Counter-Intelligence (3)

Students examine methods, ethics, policies and procedures for accessing and gathering information for positive or negative use, and applying counterintelligence to evade, trick or trap individuals, agencies, or national entities who wish to steal, damage or deny access to valid users of critical information and its sources. Active measures, passive counter measures and intelligence gathering processes as well as determining the validity and success of gathering information will be included. **Prerequisite**: CSSS 5000.

CSSS 5140 Cybersecurity Strategic Operations (3)

Specific methods, ethics, laws, policies and procedures for conducting strategic operations and countermeasures are the focus of this course. Students will learn how to identify critical infrastructures, communication channels, and information protection schemes and how to detect threats, assess vulnerabilities, penetrate and exploit cyber targets, understand how to monitor, spoof, redirect and deny access, as well as protect critical assets. **Prerequisite**: CSSS 5000.

CSSS 5160 Encryption Methods and Techniques (3)

The history and application of ciphers, codes and encryption/decryption methods and techniques are examined. Public and private keys, protocols, number generators, digital signatures, and other facets of encryption will be included. Additionally, an investigation of the role ethics and information privacy have on the science when security is applied to public systems and email content as well as higher levels of security for corporations proprietary and government classified information. **Prerequisite**: CSSS 5000 or CSSS 5100* (*If in the Artificial Intelligence or Data Analytics emphasis).

CSSS 5180 Social Engineering (3)

Examines social engineering -- the science of influencing a target to perform a desired task or divulge information. The course provides the student with current information defining the many methods of deception hackers use in order to gather information with the intent of executing identity theft, fraud, or gaining computer system access; discusses actives toward preventing social engineering threats ranging from elicitation, pretexting, influence and manipulation. The elements of social engineering are presented, discussed and explained by using real-world examples and the science behind them to unravel the mystery in social engineering.

To complement the social engineering threat, the course analyzes the ethical and social implications of computer technology. The course explores technological, social and philosophical issues to include the ramifications of automation, the ethical obligations of computer specialists and the threats to privacy that come with increased computerization. Combining the criminal-centric role of social engineering with the ethical, legal and moral impacts of technology upon individuals results in a course that provides the student a comprehensive overview of the challenges, threats and issues of everyday life in the digital age. **Prerequisite**: CSSS 5000 or CSSS 5100* (*If in the Artificial Intelligence or Data Analytics emphasis).

CSSS 5210 Cybersecurity Law and Policy (3)

The laws and policies dealing with cyber-crime, cyber warfare, privacy and international perspectives as well as an in depth look at the National Security Act, the United States Cybersecurity Electronic Security Act, the Cyber Security Enhancement Act, the Protecting Cybersecurity as a National Asset Act, the Communications Assistance for Law Enforcement Act (CALEA), cyber-crime laws, international cyber-crime laws and other current laws and policies will be reviewed and discussed. **Prerequisite**: CSSS 5000.

CSSS - Cybersecurity

CSSS 5220 Cybersecurity Threat Detection (3)

Students will examine various methods used to threaten our Cyber systems such as: viruses; spoofing; denial of service; fraud; theft; phishing; spy bots; spam; Trojan horses; email and active malware attachments; viral applications; hardware (computers and portable storage devices) with built in viruses or trap-doors; fake websites; as well as eaves dropping via wireless networks; criminal access to national, corporate or personal data; and the growing loss of privacy over social networks. **Prerequisite**: CSSS 5000 or CSSS 5100* (*If in the Artificial Intelligence or Data Analytics emphasis).

CSSS 5230 Cybersecurity Forensics (3)

This course covers methods and procedures for identification and recovery of damaged or erased digital data, tracing information access (web history, cookies, cache memory and internet source identification), determination of system vulnerabilities (e.g., TEMPEST), communication ports and computer system architectures and encryption methods, as well as incident monitoring and response. **Prerequisite**: CSSS 5000 or CSSS 5100* (*If in the Artificial Intelligence or Data Analytics emphasis).

CSSS 5250 Use and Protection of Space Assets (3)

A unique course, it focuses on all three segments (space, ground and user) of fixed and mobile communication and Global Positioning System (GPS) assets and their attributes. Secure and non-secure systems are examined to show the breadth of capabilities along with the pros and cons. Uplink and downlink signal characteristics, signal bouncing and relaying capabilities. Frequency hopping, spread-spectrum, interception and overpowering of signals through use of steerable beams, application of laser and fiber-optics, and encryption techniques are covered. **Prerequisite**: CSSS 5000.

CSSS 5265 Foundations of Software Development (3 hours)

This is an introductory software development course with focus on fundamental and foundational concepts. These concepts include general problem solving and algorithm creation techniques, primitive and abstract data types, constants, variables, expressions, Boolean logic, control flow, and object-oriented concepts. The Java programming language will be used. In addition, the fundamentals object-oriented concepts, such as classes, interfaces, and objects, instantiation and garbage collection, method implementation, and method invocation will be discussed. **Prerequisite:** CSSS 5000

CSSS 5270 Cybersecurity in Cloud Computing (3)

This course begins with an introduction to cloud computing and security and then provides an examination of cloud security architecture. The essential characteristics of cloud computing are discussed using the National Institute of Standards and Technology (NIST) Cloud Computing Model, SPI cloud service models and the different cloud delivery models. With this background, key strategies and best practices for cloud security are developed, including data protection methods, cloud security controls and countermeasures, virtualization, security management, and securing of data in rest and in motion. In addition, legal and regulatory considerations for different types of clouds are presented. Based on the cloud security requirements, the course defines the steps for an organization to use in selecting an external cloud service provider (CSP). In addition to commercial selection requirements, the U.S. Department of Defense Enterprise Cloud Service Broker Cloud Security Model, which specifies what controls the CSP must implement in the military environment, is reviewed. **Prerequisites**: CSSS 5000 and CSSS 5110.

CSSS 5290 Cybersecurity Risk Management Framework (3)

This course provides a detailed review and analysis of the six-step Risk Management Framework (RMF) process utilizing the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Security and Privacy Controls for Federal Information Systems and Organizations. The course includes the process for risk analysis and categorizing cyber risks for information systems, and the application of controls to minimize cyber risks for managing information. It also presents an in-depth overview of each step RMF along the framework path as well as the methodology for monitoring IT systems.

CSSS 5990 Advanced Topics in Cybersecurity (3)

This course is designed to permit addressing advanced and emerging topics in cybersecurity that may include, but not be limited to, cybersecurity communications, cyber warfare planning and execution, forensics, ethics, policies and laws, encryption/decryption and future topics e.g., application of quantum non-locality. This course may be repeated for credit if the content differs. **Prerequisite**: CSSS 5000.

CSSS 6000 Practical Research in Cybersecurity (3)

The student is expected to synthesize and integrate the learning experiences acquired throughout the MS in cybersecurity and to evaluate current and future topics relative to this major. Specific papers, projects, or other methodologies must include cybersecurity related technical and management areas than span this entire degree emphasis. **Prerequisite**: Successful completion of all required core courses in this major.

CSSS 6002 Practical Research in Cybersecurity II (3)

The student is expected to synthesize and integrate the learning experiences acquired throughout the MS in cybersecurity and to evaluate current and future topics relative to this major. Specific papers, projects, or other methodologies must include cybersecurity related technical and management areas than span this entire degree emphasis. **Prerequisite**: Successful completion of CSSS 6000.

CSSS 6500 Cybersecurity Internship (3)

Students undertake, with the supervision of a qualified professional, an approved internship in a cybersecurity-related setting. The course includes work and academic experience. The work experience involves professional cybersecurity duties. The academic experience involves written assignments by the faculty advisor. The outline of duties and evaluative methods are established by the student and the internship mentor and approved by the faculty advisor prior to initiation of the program. **Prerequisites**: Completion of all of the required cybersecurity courses (except CSSS 6000/CSSS 6002).