Information Assurance (IA)

IA 5001. Cyberspace Technology and Applications. 3 Hours.
Seeks to provide a systematic understanding of cyberspace technology and applications deployed in the global digital infrastructure. Covers topics in PC hardware architectures, server architectures, and operating systems. Designed to provide an understanding of computer and networking standards, such as Open Systems Interconnection Model and wireless family of IEEE standards dealing with local area networks and metropolitan area networks. Discusses relational database technology and storage systems. Gives an overview of virtualization technologies and cloud computing models. Students not in the information assurance ALIGN program may require instructor permission to enroll.

IA 5002. Concrete Mathematics. 3 Hours.
Offers students an opportunity to obtain a systematic understanding of mathematics necessary for mastering cyberspace tools and methods. Seeks to train students in mathematical concepts and the pragmatic use of these concepts in the field of information assurance and cybersecurity. Covers theory and hands-on exercises. Combines lectures with computer-based examples and assignments. Students not in the information assurance ALIGN program may require instructor approval for enrollment.

IA 5004. Introduction to Cyberspace Programming 1. 3 Hours.
Offers students an opportunity to obtain a systematic understanding of cyberspace programming languages and methods. Seeks to train students in Python using command-line interface-based editors and compilers, as well as integrated development environments, with industry-standard operating systems running on virtual machines. Trains students by implementing programming principles and methods, spanning the evolution of computer systems. Combines lectures with multiple computer-based exercises. Students not in the information assurance ALIGN program may require instructor approval for enrollment.

IA 5010. Foundations of Information Assurance. 4 Hours.
Builds a common cross-disciplinary understanding in the foundations of information assurance. Presents an overview of basic principles and security concepts related to information systems, including workstation security, system security, and communications security. Introduces information security via database technology. Discusses legal infrastructure such as DMCA, Telecommunications Act, wire fraud, and other ethical issues. Covers security methods, controls, procedures, economics of cybercrime, criminal procedure, and forensics. Describes the use of cryptography as a tool, software development processes, and protection. *Preq. Restricted to students in the College of Computer and Information Science and in the College of Engineering or by permission of instructor.*

IA 5040. Introduction to Cyberspace Programming. 4 Hours.
Seeks to provide a systematic understanding of cyberspace programming languages and methods. Trains students in Python and C using command-line interface-based editors and compilers, as well as integrated development environments, with industry-standard operating systems running on virtual machines. Offers students an opportunity to implement programming principles and methods, spanning the evolution of computer systems. Lectures are combined with multiple computer-based exercises. *Preq. Restricted to students in the College of Computer and Information Science and in the College of Engineering or by permission of instructor.*

IA 5120. Applied Cryptography. 4 Hours.
Surveys the principles and the practices of cryptography. Overviews the core cryptographic algorithms: symmetric encryption schemes (e.g., DES and AES); public key cryptosystems (e.g., RSA and discrete logarithm); and hash functions (e.g., the SHA family). Discusses core information assurance building blocks, such as authentication, digital signatures, key management, and digital certificates. Finally, applies these concepts to important security architectures, including the IP network stack (e.g., IPsec and SSL/TLS), the cellular system, and broadcast media. *Preq. Restricted to students in the College of Computer and Information Science and in the College of Engineering or by permission of instructor.*

IA 5130. Computer System Security. 4 Hours.
Explores issues involved in the security of computer systems. Topics include security models, authentication issues, access control, intrusion detection, and damage control. Includes case studies and laboratory exercises. *Preq. Restricted to students in the College of Computer and Information Science and in the College of Engineering or by permission of instructor.*

IA 5131. Lab for IA 5130. 0 Hours.
Offers small-group laboratory format to cover lab requirements in IA 5130.

IA 5150. Network Security Practices. 4 Hours.
Explores issues involved in the security of computer networks. Topics include firewalls, viruses, virtual private networks, Internet security, and wireless security. Includes case studies and laboratory exercises. *Preq. Restricted to students in the College of Computer and Information Science or by permission of instructor.*

IA 5151. Lab for IA 5150. 0 Hours.
Offers a small-group laboratory format to cover lab requirements for IA 5150.

IA 5200. Security Risk Management and Assessment. 4 Hours.
Creates the opportunity for competency in the development of information security policies and plans including controls for physical, software, and networks. Discusses different malicious attacks, such as viruses and Trojan horses, detection strategies, countermeasures, damage assessment, and control. Covers information system risk analysis and management, audits, and log files. Uses case studies, site visits, and works with commercial products. *Preq. CS 2550, IA 5010, or graduate standing; restricted to junior, senior, and graduate students in the College of Computer and Information Science or by permission of instructor.*

IA 5210. Information System Forensics. 4 Hours.
Designed to allow students to explore the techniques used in computer forensic examinations. Examines computer hardware, physical and logical disk structure, and computer forensic techniques. Conducts hands-on experiences on DOS, Windows operating systems, Macintosh, Novell, and Unix/Linux platforms. Builds on basic computer skills and affords hands-on experience with the tools and techniques to investigate, seize, and analyze computer-based evidence using a variety of specialized forensic software in an IBM-PC environment. *Preq. CS 2550, IA 5010, or graduate standing; restricted to junior, senior, and graduate students in the College of Computer and Information Science and in the College of Engineering or by permission of instructor.*

IA 5211. Lab for IA 5210. 0 Hours.
Offers a small-group laboratory format to cover lab requirements for IA 5210.

IA 5240. Cyberlaw: Privacy, Ethics, and Digital Rights. 4 Hours.
Describes the legal and ethical issues associated with information security including access, use, and dissemination. Emphasizes legal infrastructure relating to information assurance, such as the Digital Millenium Copyright Act and Telecommunications Decency Act, and emerging technologies for management of digital rights. Examines the role of information security in various domains such as healthcare, scientific research, and personal communications such as email. Examines criminal activities such as computer fraud and abuse, desktop forgery, embezzlement, child pornography, computer trespass, and computer piracy. *Preq. (a) CS 2550, IA 5010, or graduate standing and (b) junior, senior, or graduate standing; restricted to students in the College of Computer and Information Science and in the College of Engineering or by permission of instructor.*

IA 5250. Decision Making for Critical Infrastructure. 4 Hours.
Focuses on the art and science of security program management leadership in the context of critical infrastructure protection programs. Includes selected readings, review of decision-making models in crisis, lectures and insights from accomplished leaders in infrastructure protection, and examination of the students' own unique background and experiences. Trains students on the interaction of vulnerabilities, threats, and countermeasures and how to apply this knowledge to the protection of critical infrastructure using research and analysis of national and global strategies, historical and current legislation, and policies. Also seeks to give students a working knowledge of federal, state, and private-sector critical infrastructure protection resources and programs. *Preq. Restricted to students in the College of Computer and Information Science and in the College of Engineering or by permission of instructor.*

IA 5976. Directed Study. 1-4 Hours.
Seeks to provide information assurance (IA) students with the training experience of working on a specific IA project under the direction of an IA instructor. The instructor provides students with a plan of seminar sessions, including lectures, research, and development of project deliverables and with direction to complete the course. May be repeated without limit.

IA 5978. Independent Study. 2-4 Hours.
Offers independent work under the direction of members of the department on a chosen topic. Course content depends on instructor. May be repeated without limit.

IA 5984. Research. 2-4 Hours.
Offers an opportunity to conduct research under faculty supervision. May be repeated without limit.

IA 6120. Software Security Practices. 4 Hours.
Explores the principles and methodologies for addressing software security risk issues in organizations. Offers students an opportunity to learn software security vulnerabilities and to create software solutions to address software security issues in accordance with information assurance requirements and in compliance with U.S. and international laws, federal systems guidelines, standards, directives, and industry best practices. *Preq. Restricted to students in the College of Computer and Information Science and in the College of Engineering or by permission of instructor.*

IA 6121. Lab for IA 6120. 0 Hours.
Offers a small-group laboratory format to cover lab requirements for IA 6120.

IA 6962. Elective. 1-4 Hours.
Offers elective credit for courses taken at other academic institutions. May be repeated without limit.

IA 7900. Capstone Project/Seminar. 4 Hours.
Draws together candidates from diverse backgrounds (technical, legal, and/or law enforcement) in a collaborative activity to address one or more security issues from an integrated perspective. Requires a project proposal, generally industrially oriented, to be submitted and accepted prior to the semester in which the project is to be undertaken. *Preq. Restricted to students in the College of Computer and Information Science or by permission of instructor.*

IA 7962. Elective. 2-4 Hours.
Offers elective credit for courses taken at other academic institutions. May be repeated without limit.

IA 8660. Research Project in National Information Security. 4 Hours.
Engages students in national cybersecurity/information systems security problems. Offers students an opportunity to learn how to apply research techniques, think clearly about these issues, formulate and analyze potential solutions, and communicate their results. Working in small groups under the mentorship of technical clients from government and industry, each student has an opportunity to formulate, carry out, and present original research on current cybersecurity/information assurance problems of interest to the nation. Requires permission of instructor. May be repeated once.

IA 8982. Readings. 1-4 Hours.
Offers selected readings under the supervision of a faculty member. May be repeated without limit.

IA 9990. Dissertation. 4 Hours.
Offers selected work with the agreement of a thesis supervisor. May be repeated once.

IA 9996. Dissertation Continuation. 0 Hours.
Continues work with the agreement of a thesis supervisor. May be repeated without limit.