Admission Requirements

Unconditional Admission:
Unconditional admission requires a GPA of 3.0 (4.0 scale), a minimum of a 1000 on the GRE verbal and quantitative sections and a minimum of a 3.0 on the analytical and writing portions; or a minimum of 500 on the GMAT. Also, international students must have an acceptable score on the TOEFL or IELTS. Applicants for MSIAS need to have a bachelor’s degree in a curriculum related to one of the following: Management in Computer Information Systems, Computer Science, Electrical Engineering, Computer Engineering or Information Systems Security Engineering.

The program is offered in three different disciplines (tracks). Additional requirements for each track are as follows:

Business: Bachelor’s degree in a business or related field; students with a bachelor’s in an unrelated field will be required to take the following prerequisites - Economics/microeconomics, Calculus and Statistics.

Computer Science: Bachelor’s degree in computer science or a related field; student’s with a bachelor’s in an unrelated field will be required to take the following prerequisites - Data Structure, Operating Systems, Algorithm Design and Analysis, Computer Architecture and Probability and Statistics.

Engineering: Bachelor’s degree in engineering from an ABET accredited program; students with a bachelor’s in an unrelated field will be required to take the following prerequisites - Data Structure, Operating Systems, Algorithm Design and Analysis, Computer Architecture, Probability and Statistics.

Conditional Admission:
For those who do not satisfy the unconditional requirements, applications will be considered for conditional admission.

Core Classes:

IS 501-Introduction to Information Assurance: Overview of information security from a technical project management and risk management perspective.

IS 563-Computer Forensics: Looks at problems and concerns related to computer investigations blending traditional methods with classic systems analysis technique.

CPE 549-Introduction to Information Assurance Engineering: Introduction to information security requirements and hardening techniques such as cryptography, Network O/S, and file structures.


CS 570-Introduction to Computer Networks: Introduction to the organization, secure architecture and operation of computer networks.

CS 670-Computer Networks: Detailed analysis of the organization and operation of computer networks focusing on algorithms and organizations for the Transport Layer, Network Layer and Data Link.
The Engineering track takes existing and proven practices and enhances them with an education in the National Institute of Standards and Technology (NIST) and the Defense Information Assurance Certification And Accreditation Process (DIACAP). This approach will address security issues in future technologies during the concept & requirements stages of system design and the formulation of the hardware design. This type of forward thinking security design is a void in the industry today.

The Computer Science track involves developing, documenting and maintaining secure coding practices for scripts and applications. Also included are the design aspects of networks ensuring a risk mitigated network in relation to confidentiality, integrity and the availability of data and devices.

The Business track looks at the security requirements mandated by statutory authority and analysis of business impact as it relates to the System Development Life Cycle. This track introduces tools and techniques for proven methodologies in technical project management related to integrating information security best practices into system development while minimizing associated risks.

Business Track Courses (15 hours):
- IS 577 (3 hours)-Network defense and Operation Systems
- IS 560 (3 hours)-Telecommunications and Networking
- IS 660 (3 hours)-Information Security Management
- IS 670 (3 hours)-Business Continuity Planning (capstone course of the Business track)
- 600 level elective (3 hours) in IS, CS, or ECE.

Computer Science Track Courses (15 hours):
- CS 585 (3 hours)-Introduction to Computer Security
- CS 685 (3 hours)-Computer Security
- CS 553 (3 hours)-Client/Server Architectures
- Two courses in Computer Science at the 600 level which must be approved by the department (6 hours)
- All students must pass a written comprehensive final examination

Engineering Track Courses (15 hours):
- EE693 (3 hours)-ECE capstone (required)
- Choose 4 of the following:
  - CPE 645 (3 hours)-Advanced Computer Network Security
  - CPE 551 (3 hours)-Software Design and Engineering
  - CPE 645 (3 hours)-Ubiquitous Computing
  - CPE 748 (3 hours)-Mobile and Wireless Networks
  - CPE 648 (3 hours)-Advanced Computer Networks

- Vulnerability Assessments
- Policy, Procedures, Standards & Guidelines
- Forensics
- Physical Security
- Cryptography

- Application & DB Security
- Network Penetration Testing

- Business Continuity
  - Disaster Recovery
  - Incident Response