Certificate in Cybersecurity and Information Assurance

The U.S. Department of Labor (DoL) reports the median annual wage for information security practitioners was $90,120 in May 2015 and in regards to employment, it is projected to grow 18 percent from 2014 to 2024, which is substantially faster than the average for all occupations (DoL, 2015).

This Certificate will not only allow you to compete but will provide you a well-rounded education. The courses of instruction are part of the Information Systems Security & Assurance Curriculum (ISSA series) as confirmed by the Information Assurance Courseware Evaluation (IACE) Program at the National Security Agency (NSA). Additionally, IACE approval requires that courseware meet all of the elements of a Committee on National Security Systems (CNSS) National Training Standard and the courses presented in this certificate via ISSA series have been validated for two specific standards: Information Systems Security (INFOSEC) Professionals, NSTISSI No. 4011, System Administrators, CNSSI No. 4013 Advanced Level, based on the CNSS course certifications and designation of Center of Academic Excellence in Information Assurance Education (CAE/IA) sponsored by the National Security Agency (NSA), Department of Defense (DoD), and Department of Homeland Security (DHS).

Upon successfully completing the program, you will be prepared to take the CompTIA Security+ which meets the ISO 17024 standard and is approved by U.S. Department of Defense to fulfill Directive 8570.01-M requirements.

Required Courses:

IT 1411 – Orientation to Computer Technology (one credit hour)
The student will be introduced to such varied topics as common IT terminology, career planning, basic programming logic, ethics, and other IT issues. The Business Information Technology portfolio project will also be discussed.

IT 2143 – Introduction to Networking (three credit hours)
Explores the theory and terminology of both local and wide area computer networks and their proper application to business and industry problems.

IT 2153 – Network Operating Systems 1 (three credit hours)
A popular operating system will be covered in detail. A study of components, functions, and relationships of computer operating systems and their interactions with user programs will be offered.

IT 3333 – Cybersecurity Investigation (three credit hours)
Hands-on laboratory-based application of Cybersecurity investigation utilizing common techniques and methods, hardware and software applications, in digital evidence collection, extraction, and recovery in accordance with legal standards of evidence as well as ethical implications of forensics methods.

IT 4353 – Information Assurance and Security Management (three credit hours)
An investigation of information assurance and security with an emphasis on the identification, assessment, and management of risks and threats to information security and privacy in the digital business environment. Mitigating measures are also explored.

IT 4373 – Information Assurance Regulation and Ethics (three credit hours)
An investigation into the law, policy, standards, and ethics concerning the digital resources of the business environment.

IT 4443 – Fundamentals of Information Security (three credit hours)
This course will introduce students to computing systems, which rely on networking and cybersecurity best practices for organizational network defenses. In so doing, students will learn how to use Nessus and other software to configure a scan policy and identify targets to scan as well as gain unauthorized file system access on a Windows Server, create a destructive virus with the potential to destroy or cripple an operating system and deliver and launch a Trojan on another system. In today's technologically advanced business organizations, these abilities are required to construct solid defenses to protect against such attacks.