NATIONAL SECURITY AGENCY, CERTIFICATE

Requirements for an undergraduate certificate may be completed at any campus location offering the specified courses for the certificate.

Certificate Learning Objectives

- **Knowledge/Application:** Explain and apply the interdisciplinary knowledge of information sciences in a security context to recognize, analyze, defend against, and manage cyber risks.
  - Students will be able to describe which cryptographic protocols, tools and techniques are appropriate for a given situation.
- **Problem-Solving:** Understand, apply and adapt various problem solving strategies, using appropriate technology and methods.
  - Students will be able to demonstrate proficiency in the use of a programming language to solve complex problems in a secure and robust manner.
  - Students will be able to demonstrate the ability to design and develop basic programs for modern computing platforms (e.g., PC, cloud, mobile, web).
  - Students will be able to write simple linear and looping scripts.
  - Students will be able to write simple and compound conditions within a programming language or similar environment (e.g., scripts, macros, SQL).
  - Students will be able to describe how basic statistics and statistical methods can be applied in a given situation.
  - Students will be able to evaluate probabilities to solve applied problems.
  - Students will be able to apply standard statistical inference procedures to draw conclusions from data.
  - Students shall be able to use one or more common DF tools, such as EnCase, FTK, ProDiscover, Xways, SleuthKit.
  - Students will be able to identify the bad actors in cyberspace and compare and contrast their resources, capabilities/techniques, motivations, aversion to risk.
  - Students will be able to examine the placement of security functions in a system and describe the strengths and weaknesses.
- **Communication (Individual and Team):** Communicate and work effectively (both individually and in teams) with a range of perspectives and audiences through a variety of media.
  - Students will be able to develop system specific plans for (IST 456):
    - The protection of intellectual property; - The implementation of access controls; and
    - Patch and change management.
  - Students will be able to develop contingency plans for various size organizations to include: business continuity, disaster recovery and incident response.
- **Professional Responsibilities:** Describe professional responsibilities in terms of the ethical, legal and security policy aspects of information assurance and security.
  - Students shall be able to discuss the rules, laws, policies, and procedures that affect digital forensics.
  - Students will be able to describe the steps in performing digital forensics from the initial recognition of an incident through the steps of evidence gathering, preservation and analysis, through the completion of legal proceedings.
  - Students will be able to describe how the type of legal dispute (civil, criminal, private) affects the evidence used to resolve it.
  - Students will be able to list the applicable laws and policies related to cyber defense and describe the major components of each pertaining to the storage and transmission of data.
  - Students will be able to describe how standards, such as the Orange Book, may be applied to the requirements for a sub-contractor or customer.