NATIONAL SECURITY AGENCY, CERTIFICATE

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

Program Description

The NSA certificate indicates students have completed the courses representing the required knowledge units as specified by the National Security Agency and the Department of Homeland Security as part of Penn State's designation as a National Center of Academic Excellence in Cyber Defense.

What is National Security Agency?

Penn State and the College of Information Sciences and Technology are designated as a national Center of Academic Excellence (CAE) in Cyber Defense by the National Security Agency and the Department of Homeland Security. As such, the College of IST is authorized to grant security certificates of recognition and achievement to graduating students who meet certain academic criteria. The certificates certify that the student graduated from an institution and program whose faculty, resources, curricula, and commitment were evaluated and found to be of high quality, as defined by NSA/DHS for cyber security professionals.

MORE INFORMATION ABOUT NATIONAL SECURITY AGENCY (https://ist.psu.edu/current/undergraduate/certificates/nsa/)

You Might Like This Program If...

- You want to protect digital information, data stores, and computer networks from threats.
- You want to learn the cyberdefense strategies used to anticipate, recognize, and defend against computer attacks.
- You're passionate about how we can keep sensitive information out of the hands of hackers, cybercriminals, and terrorist organizations.

MORE INFORMATION ABOUT WHY STUDENTS CHOOSE TO STUDY NATIONAL SECURITY AGENCY (https://ist.psu.edu/current/undergraduate/certificates/nsa/)

Entrance to Certificate

Must be enrolled in ISTBS, SRA, SRAAL, SRABK or SRACA major.

Program Requirements

To earn an undergraduate certificate in National Security Agency, a minimum of 28 credits is required.

A grade of "C" or higher is required in all courses for the certificate; no course substitutions are permitted. Courses taken more than 10 years ago will not apply automatically towards completion of the certificate but instead will require review by the academic unit.

Code	Title	Credits
Prescribed Courses		
Prescribed Courses: Require a grade of C or better		
IST 140	Introduction to Application Development	3
or CMPSC 101	Introduction to Programming	
IST 210	Organization of Data	3
IST 220	Networking and Telecommunications	3
IST 451	Network Security	3
IST 454	Computer and Cyber Forensics	3
IST 456	Information Security Management	3
SRA 111	Introduction to Security and Risk Analysis	3
SRA 221	Overview of Information Security	3
STAT 200	Elementary Statistics	4

Certificate Learning Objectives

- **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:
    - 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.
- **Knowledge/Application:** Explain and apply the interdisciplinary knowledge of information sciences in a security context to recognize, analyze, defend against, and manage cyber risks.
  - Given a specific scenario, students will be able to identify the needed design principle.
  - Students will be able to describe how crypto can be used, strengths and weaknesses, modes, and issues that have to be addressed in an implementation (e.g., key management), etc.
  - Students will be able to describe the differences between symmetric and asymmetric algorithms.
  - Students will be able to describe which cryptographic protocols, tools and techniques are appropriate for a given situation.
  - Students will be able to examine the architecture of a typical, complex system and identify significant - vulnerabilities, -risks,- and points at which specific security technologies/methods should be employed.
  - Students will be able to identify the elements of a cryptographic system.
  - Students will be able to apply security principles to the design and development of database systems and database structures.
  - Students will be able to identify and describe common security concerns in database management systems.
  - Describe a basic network architecture given a specific need and set of hosts/clients.
  - Students will be able to apply their knowledge of network technologies to design and construct a working network.
  - Students will be able to demonstrate the use of a network monitor to display packets.
  - Students will be able to analyze a trace of packets to identify the establishment of a TCP connection.
  - Students will be able to track and identify the packets involved in a simple TCP connection (or a trace of such a connection).
  - Students will be able to describe the fundamental concepts, technologies, components and issues related to communications and data networks.
  - Students will be able to describe the hardware components of modern computing environments and their individual functions.

- Students will be able to describe the fundamental concepts, technologies, components and issues related to communications and data networks.
- Students will be able to use a network mapping tool (e.g., Nmap).
- Students will be able to apply their knowledge to implement network defense measures.
- Demonstrate their proficiency in the use of scripting languages to write simple scripts (e.g., to automate system administration tasks).
- Students will be able to use a network monitoring tools (e.g., WireShark).
- Students will be able to describe the various concepts in network defense.
- Students will be able to apply cyber defense methods to prepare a system to repel attacks.
- Students will be able to describe appropriate measures to be taken should a system compromise occur.
- Students will be able to describe common security models of database management systems.
- Students will be able to compare the advantages and disadvantages of various risk assessment methodologies.
- Students will be able to describe how risk relates to a system security policy.
- Describe various risk analysis methodologies.
- Students will be able to select the optimal methodology based on needs, advantages and disadvantages.

- **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. (STAT 200, SRA 365)
  - 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.
- **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.

Academic Advising

The objectives of the university's academic advising program are to help advisees identify and achieve their academic goals, to promote their intellectual discovery, and to encourage students to take advantage of both in-and out-of class educational opportunities in order that they become self-directed learners and decision makers.

Both advisers and advisees share responsibility for making the advising relationship succeed. By encouraging their advisees to become engaged in their education, to meet their educational goals, and to develop the habit of learning, advisers assume a significant educational role. The advisee's unit of enrollment will provide each advisee with a primary academic adviser, the information needed to plan the chosen program of study, and referrals to other specialized resources.

READ SENATE POLICY 32-00: ADVISING POLICY (https://senate.psu.edu/policies-and-rules-for-undergraduate-students/32-00-advising-policy/)

University Park

Undergraduate Academic Advising Center
E103 Westgate Building
University Park, PA 16802
814-865-8947
advising@ist.psu.edu

Career Paths

Students who earn the Security certificate are prepared to pursue careers in intelligence, risk analysis, defense, and emergency management. Earning the certificate demonstrates that the student completed a program whose curriculum and resources were designated as high quality by the National Security Agency and Department of Homeland Security.

Careers

Because our courses blend technical knowledge with skills in communication and business, a Security certificate allows students to pursue opportunities in intelligence, counterterrorism, computer forensics, and a number of other growing careers.

MORE INFORMATION ABOUT POTENTIAL CAREER OPTIONS FOR GRADUATES WITH A CERTIFICATE IN NATIONAL SECURITY AGENCY (https://ist.psu.edu/current/careers/development/process/path/)

Contact

University Park

COLLEGE OF INFORMATION SCIENCES AND TECHNOLOGY
411 Eric J. Barron Innovation Hub Building

State College, PA 16801
814-865-3528