

Certificate Overview

The role of Information Systems Security Engineering (ISSE) is to help ensure that the security requirements of systems are met. Due to a lack of proper security engineering, systems fail to be certified and accredited, causing costly delays or failures.

Today, professional certificate programs exist that attempt to address the ISSE void; however, these are essentially “cookbook” and process-oriented. The student merely has to memorize the process for these certificates, and this results in individuals lacking the knowledge and analysis approaches required to address the variety and complexity of real systems.

As a result, NPS, in partnership with the NSA, has developed a certificate program in ISSE. The course sequence will provide the knowledge and analytical skills required to contribute productively in both existing and new system developments where cyber security is a concern.

For Certificate Costs,
Contact:
CISRContact@nps.edu



About CISR

The Center for Information Systems Security Studies and Research (CISR) has created the ISSE Certificate to serve the DoD and Federal Agencies.

Through CISR, the National Security Agency (NSA) and the Department of Homeland Security (DHS) have designated NPS as a Center of Academic Excellence in Information Assurance (IA) Education and IA Research.

CISR is approved to award the CNSSI/NSTISSI certificates: 4011-4015.



CISR

Naval Postgraduate School
Computer Science Department
Monterey, CA

CISRContact@nps.edu

<http://www.cisr.us>



NAVAL POSTGRADUATE SCHOOL



Information Systems Security Engineering (ISSE) Certificate



<http://www.cisr.us>



Take the challenge...
Become an ISSE!

The ISSE certificate program at NPS focuses on security theories, principles and practices of systems security engineering from a life cycle perspective. The five courses afford students the knowledge and skills required to derive security requirements, design and develop secure systems, and analyze the security posture of deployed systems. Risk assessment and mitigation are addressed in accordance with the Risk Management Framework defined by the National Institute of Standards and Technology (NIST) and regulatory directives and guidelines for federal information systems and national security systems, e.g., NIST SP 800-53, CNSS Instruction 1253.

CERTIFICATE COMPONENTS

CS3690 Network Security

Understand the underlying principles involved in the “bits-in-transit” aspect of information security. This includes two major topic areas: 1) the protection of legitimate network traffic via cryptographic mechanisms, and 2) the detection and filtering of malicious network traffic via authentication mechanisms, attack signature recognition, and filter mechanisms and strategies.

CS3695 Network Vulnerability Assessment and Risk Mitigation

Students will be able to: (1) describe methodology used to assess the vulnerability of an organization connected to the Internet & how to mitigate those vulnerabilities; (2) employ common tools of the trade used during assessments & that assist in mitigation; (3) define/ describe current types of vulnerabilities, how they leave an organization open to threats, & how to protect against them; (4) compile new assessment & vulnerability tools; (5) describe the motivations & different types of hackers.

CS4600 Secure System Principles

Describe the basic concepts & principles to secure system construction. Differentiate major categories of system policies, describe secure component interconnection & composition, as well as articulate how design choices affect system security. The major notions to be understood include structural considerations for secure systems, trustworthiness by construction; secure composition; functional mechanisms; & lifecycle assurance techniques.

CS4650 Fundamentals of Information Systems Security Engineering

Articulate the security engineering activities associated with different phases of an IT system’s life cycle. 1) characterize an IT system in terms of its primary security attributes, properties & characteristics; 2) analyze threats & risks related to environmental factors & operational capabilities, and 3) understand the scope & relationship between security requirements for international/national standards, public laws, & national/organizational security-related policies & regulations

CS4652 Applied Information Systems Security Engineering

Identify properties used to evaluate different security architectures, describe the inherent trust problems relating to the composition of systems and components, & perform engineering, architectural and design analyses with respect to requirements and capabilities. Identify mechanisms applicable to various security requirements, determine the security boundaries of a large system, and apply concepts such as *reference monitor*, *least privilege* and *balanced assurance* to assess the security of a design.