NATIONAL UNIVERSITY

SCHOOL OF ENGINEERING AND COMPUTING

MASTER OF SCIENCE IN CYBERSECURITY

Help Protect the World’s Computing and Information Systems

The Master of Science in Cybersecurity is a professional degree for those who endeavor through technical and managerial measures to ensure the security, confidentiality, integrity, authenticity, control, availability, and utility of the world's computing and information systems infrastructure. The program has a required core and a required specialization, which can be selected from some alternatives. The core is designed to provide a means of supporting the variety of backgrounds (both education and work experience) that those who wish to study this area may bring to the program. The core is also a statement of the knowledge domain that is common to most efforts in this area. The specializations provide for study in particular domains of knowledge within the field, which are also tied to communities of effort within the field.

Program highlights:

- Entire program can be completed online
- Explore threats to computer infrastructures and digital assets, and develop prevention and mitigation plans
- Examine the effect of technical advances and legislative developments on CSIA
- Specializations available in Ethical Hacking and Pen Testing and Information Assurance and Security Policy
- Designated NSA/DHS Center of Academic Excellence in Cyber Defense Education

LEARN MORE TODAY

Online and On-campus Programs
Monthly Starts and Accelerated Classes
WSCUC Accredited

NATIONAL UNIVERSITY

Veteran Founded. Nonprofit. I NU.EDU

Accredited by the WASC Senior College and University Commission (WSCUC). Designated a Center of Academic Excellence in Information Assurance Education (CAE IAE) for the Master of Science in Cybersecurity and Information Assurance program. National University is nonprofit and does not discriminate in any of its policies or practices on the basis of race, ethnicity, religion, national origin, sex, disability, age, or veteran status.

MASTER OF SCIENCE IN CYBERSECURITY

Academic Program Director: Christopher Simpson; (858) 309-3418; csimpson@nu.edu

The Master of Science in Cybersecurity is a professional degree for those who endeavor through technical and managerial measures to ensure the security, confidentiality, integrity, authenticity, control, availability, and utility of the world's computing and information systems infrastructure. The program has a required core and a required specialization which can be selected from some alternatives. The core is designed to provide a means of supporting the variety of backgrounds (both education and work experience) that those who wish to study this area may bring to the program. The core is also a statement of the knowledge domain that is common to most efforts in this area. The specializations provide for study in particular domains of knowledge within the field, which are also tied to communities of effort within the field.

Program Admission Requirements

All students who seek to enroll in the MS-CSIA program must interview with the Academic Program Director noted above prior to enrolling in the first course of the program.

Program Learning Outcomes

Upon successful completion of this program, students will be able to:

- Devise a mitigation plan against both external and internal vulnerabilities to enterprise computer infrastructures and sensitive digital assets.
- Analyze and evaluate multiple risk assessment methods and strategies.
- Compare and contrast the legal and ethical aspects of cybersecurity at the Federal, State, and International level.
- Assess and summarize the legal and ethical requirements of a cyber security professional.
- Integrate project management skills to produce a cybersecurity solution.
- Evaluate the results of a security assessment to assess the security status of a network or computer system.
- Conduct in-depth research into a specific CSIA topic, including finding and integrating relevant research results of others.
- Integrate systems-level-infrastructure thinking into CSIA problem identification and resolution, and effectively communicate the solution

Degree Requirements

To obtain the Master of Science in Cybersecurity, students must complete 58.5 graduate units. A total of 13.5 quarter units of graduate credit may be granted for equivalent graduate work completed at another regionally accredited institution, as it applies to this degree, and provided the units were not used in earning another advanced degree. All students must complete the 9 core requirements and choose an area of specialization. Please refer to the graduate admissions requirements for specific information regarding application and evaluation.

Core Requirements

(9 Courses; 40.5 quarter units)

CYB 600	Cyber Security Technology
CYB 601	Cyber Sec. Toolkit Utilization *Prerequisite: CYB 600 with a minimum grade of B*
CYB 602	Threat Modeling & Intel *Prerequisite: CYB 601*
CYB 603	Cyber Security Ethical Issues *Prerequisite: CYB 602*
CYB 604	Wireless and Mobile Security *Prerequisite: CYB 603*
CYB 606	Net Defense & Cloud Security *Prerequisite: CYB 604*
CYB 699A	Cyber Security Project I *Prerequisite: CYB 608 and completion of one specialization area.*
CYB 699B	Cyber Security Project II *Prerequisite: CYB 699A*
CYB 699C	Cyber Security Project III *Prerequisite: CYB 699B with a minimum grade of S*

All students must choose **one (1)** specialization defined below:

Specialization in Ethical Hacking & Pen Testing

The Ethical Hacking & Pen Testing specialization is designed to provide unique applications involved in the professional domain of Cyber Security and Information Assurance (CSIA). The curriculum focus is directed toward ethical hacking and penetration (Pen) testing. Penetration tests probe network and information system security components by conducting simulated attacks on systems. This specialization prepares the professional to develop rules of engagement, prepare a tool kit, discover and exploit system vulnerabilities, ethically conduct a penetration test and prepare penetration test documentation. Red Teaming practices are utilized, and Red vs. Blue team exercises are executed.

Program Learning Outcomes

Upon successful completion of this program, students will be able to:

- Devise a mitigation plan against both external and internal vulnerabilities to enterprise computer infrastructures and sensitive digital assets.
- Integrate systems-level-infrastructure thinking into CSIA problem identification and resolution, and effectively communicate the solution.
- Forecast the impact of continually advancing technology and national and international cyber-legislation on CSIA.
- Conduct in-depth research into a specific CSIA topic, including finding and integrating relevant research results of others.
- Generate critical thinking in analysis and synthesis of enterprise and global CSIA issues through effective individual and team graduate-level written and oral assignments.
- Integrate project development skills in producing a security system.
- **Specialization:** Produce a pen test authorization and rules of engagement document.
- **Specialization:** Prepare and synthesize process specifications of Red Team actions against a Blue Team defense of a computer infrastructure.
- **Specialization:** Prepare and synthesize process specifications of a Blue Team defense used to protect the computer infrastructure against a Red Team attack.

Program Requirements

(4 courses; 18 quarter units)

CYB 608	Ethical Hacking *Prerequisite: CYB 606*
CYB 632	Info. Sys. Vulnerab. & Attacks *Prerequisite: CYB 608*
CYB 633	Red Teaming *Prerequisite: CYB 632*
CYB 634	Red vs. Blue Team Exercise *Prerequisite: CYB 633*

Specialization in Information Assurance and Security Policy

The specialization in Information Assurance and Security Policy provides study in the professional domain of Cyber Security and Information Assurance that focuses on the organizational and informational portion of the field. This arena particularly involves larger organizations, often in government, that have codified standards, policies, and practices for this field.

Program Learning Outcomes

Upon successful completion of this program, students will be able to:

- Differentiate among the models, architectures, challenges and global legal constraints of secure electronic commerce technologies used to ensure transmission, processing and storage of sensitive information.
- Prescribe how to provide message privacy, integrity, authentication and non-repudiation using network security practices and infrastructure hardening techniques.
- Assess, from both a national and global perspective, the relative demands of internet-openness, legislation and law-enforcement, and individual right-to-privacy.
- Forecast the impact of continually advancing technology and national and international cyber-legislation on CSIA.
- Generate critical thinking in analysis and synthesis of enterprise and global CSIA issues through effective individual and team graduate-level written and oral assignments.
- Produce a successful project using project development skills.
- **Specialization:** Prepare an IT risk mitigation and security plan.
- **Specialization:** Prepare and create an enterprise disaster recovery and business continuity plan.
- **Specialization:** Derive information assurance from an INFOSEC perspective.

Program Requirements

(4 courses; 18 quarter units)

CYB 608	Ethical Hacking *Prerequisite: CYB 606*
CYB 612	Disaster Rec./Bus. Continuity *Prerequisite: CYB 608*
CYB 613	Information Assurance *Prerequisite: CYB 608*
CYB 616	Certification & Accreditation *Prerequisite: CYB 613*

For complete program information, see the National University Catalog 82, effective 10/2018.