# Master of Science in Cybersecurity Studies

This Master of Science in Cybersecurity Studies takes a broad, multi-disciplinary approach to preventing and responding to large-scale cyber threats and cyber attacks. The first half of this program provides you with a foundation in network security, information assurance, cybercrime, and digital forensics. The second half of this program focuses on the issues, policies, practices, and perspectives of various sectors, critical infrastructures, agencies, and disciplines, such as national security, intelligence, criminal justice, and emergency management. Cyber threats can have an adverse effect on public confidence, stock markets, economic sectors, and other critical infrastructures. The need for trained experts in this field who can prevent, detect, and eliminate such threats is critical to our national security.

This program has specific admission requirements.

## Degree Program Objectives

In addition to the institutional and degree level learning objectives, graduates of this program are expected to achieve these learning outcomes:

- Analyze the national cyber threat landscape and cybersecurity challenges from both external entities and domestic sources.
- Examine the legal, social, regulatory, ethical, and technical issues related to securing information systems and national critical infrastructures.
- Compare and contrast the interdisciplinary policies, practices, perspectives and products required to address the cyber threats to our information systems and critical infrastructures.
- Appraise the methodologies for performing vulnerability assessment, risk mitigation, auditing, and certification of information systems and critical infrastructures.
- Categorize the cybersecurity related roles, responsibilities, and policies for managers of critical infrastructures, national security, corporate security, criminal justice, and intelligence/counter intelligence.

## Programmatic Admission Requirements

For this program, you must provide an official transcript of your previously-completed bachelor's or master's degree and have ONE of the following:

- Associate or bachelor's degree in information technology or a related field (ex: computer science, information systems, database development, etc.).
- Completion of one of our undergraduate IT certificates
- Completion of 6 upper-level (300-400) undergraduate credits in IT-related courses.
- Completion of CISSP certification (valid up until the expiration date)
- Completion of an IT-related minor of concentration in student's undergraduate program.
- 5 years of work experience in cybersecurity operations, cybersecurity policy, or cybersecurity management, including at least 6 months of verifiable hands-on information technology or information security experience.
- 5 years of work experience at the senior level in information security, criminal justice, emergency management, intelligence, or homeland security, including at least 6 months of verifiable hands-on information technology or information security experience.
- Certifications in at least one of the below:

1. CompTIA Security+
2. CompTIA Network+
3. SSCP
4. EC-Council Ethical Hacking
5. Cisco CCNA Security

Notes:

- If the IT-specific requirements are not noted in the official bachelor's or master's transcript, you must provide official copies of your undergraduate transcripts that show the appropriate coursework.
- The 5-year work experience requirement must be documented in your resume or your Joint Services Transcript (JST) and DD214, complete with phone and email contact information for your supervisor to allow for official verification of the employment.
- Preadmission courses completed at the undergraduate level must be graded C or better; B or better at the graduate level.

Please visit our AMU (https://www.amu.apus.edu/admissions/graduate-requirements.html) or APU (https://www.apu.apus.edu/admissions/graduate-requirements.html) graduate admission page for more information on institutional admission requirements.

### Need help?

If you have questions regarding a program’s admission requirements, please contact an admissions representative at 877-755-2787 or info@apus.edu.

# Degree at a Glance

| Code | Title | Semester Hours |
|---|---|---|
| Core Requirements | | 33 |
| Final Program Requirements | | 3 |
| Total Semester Hours | | 36 |

# Degree Program Requirements

## Core Requirements (33 semester hours)

| Code | Title | Semester Hours |
|---|---|---|
| NSEC506 | Cyber Policy and Practice in National Security [1] | 3 |
| ITCC500 | Research Methods in Information Systems and Technology | 3 |
| EDMG600 | Emergency Management Perspectives on Cybersecurity | 3 |
| HLSS505 | Security Risk Management | 3 |
| INTL647 | Cyber Intelligence | 3 |
| ISSC621 | Computer Forensics | 3 |
| ISSC630 | Advanced Cybercrime Analysis | 3 |
| ISSC641 | Telecommunications and Network Security | 3 |
| ISSC642 | Intrusion Detection and Incident Handling | 3 |
| ISSC660 | Information Assurance | 3 |
| LSTD517 | Law, Ethics and Cybersecurity | 3 |
| Total Semester Hours | | 33 |

[1] Required as the first course in the program but may be taken concurrently with another course.

## Final Program Requirements (3 semester hours)

| Code | Title | Semester Hours |
|---|---|---|
| Select 1 course from the following: | | 3 |
| ISSC698 | Cybersecurity Studies: Capstone Practical [1] | |
| ISSC699 | Cybersecurity Studies Capstone [1] | |
| Total Semester Hours | | 3 |

[1] This course may not be taken until all other courses are completed and student has a 3.0 GPA