

Master of Aviation Cybersecurity

Designed for working professionals in or seeking leadership roles, the degree focuses on aviation systems security, cyber risk management, and regulatory compliance. Students develop an understanding of technical vulnerabilities affecting modern aviation infrastructure and apply cybersecurity concepts to strategic decision-making for technical and executive contexts. Graduates are prepared to support the protection of aviation assets and contribute to cybersecurity initiatives in aviation environments.

Housed in the Department of Applied Aerospace Science within the College of Aviation, the Master of Aviation Cybersecurity at the **Worldwide Campus** addresses cybersecurity within the global aviation industry. The program examines cybersecurity within the interconnected aviation and aerospace ecosystem, including aircraft systems, airports, air traffic management, and emerging technologies, with emphasis on protection against evolving cyber threats.

Program-Level Student Learning Outcomes

Students will:

- Analyze cybersecurity risks and strategies.
- Apply fundamentals of cybersecurity and information assurance.
- Communicate cybersecurity risks and strategies with both technical and non-technical stakeholders.
- Evaluate the air transportation ecosystem impacts.
- Evaluate cybersecurity risks within the aviation/aerospace ecosystem.
- Examine the impact of operation technology on aviation/aerospace supply chains, maintenance, and operations.
- Develop effective cybersecurity mitigation strategies specific to the aviation/aerospace ecosystem.

Worldwide Program Requirements

Core Requirements	30
Total Credits	30

Program Details

The Master of Aviation Cybersecurity requires successful completion of a minimum of 30 credit hours. Students enrolled in the Worldwide Graduate Online program may complete the degree in six terms, or approximately two years, assuming full-time enrollment and continuous progress. Students pursuing this graduate degree must earn a minimum cumulative grade point average (CGPA) of 3.00 for all work completed at the University. The courses required to earn this degree are listed below.

Students should be aware that many courses have prerequisites and/or corequisites. Students are responsible for ensuring that all prerequisite and degree requirements are satisfied prior to enrollment in advanced coursework. The suggested plan of study is provided as a guide. A student's actual plan of study may vary based on term of admission, course availability, transfer credit, and other academic considerations. Students should consult with their academic advisor to develop an individualized plan of study.

Core Requirements

AMNT 609	Aircraft Maintenance Management	3
CYAV 510	Security Engineering and Management	3
CYAV 515	Foundations of Aviation Cybersecurity	3
CYAV 516	Operational Technology Risks in Aviation - IoT, ICS, SCADA	3
CYAV 517	Uncrewed and Autonomous Systems Cybersecurity	3

CYAV 520	Aviation Cybersecurity Threats, Actors, Tools, and Techniques	3
CYAV 525	Aviation Cybersecurity Risk Management and Resilience	3
CYAV 526	Cybersecurity Standards, Laws, and Regulations	3
ASCI 602	The Air Transportation System	3
SPAC 515	Cybersecurity Applications in Space	3
Total Credits		30

Suggested Plans of Study

Two Year Plan

Year One

Requirements	Credits
ASCI 602 - The Air Transportation System	3
Semester Hours	3

Requirements	Credits
CYAV 515 - Foundations of Aviation Cybersecurity	3
Semester Hours	3

Requirements	Credits
CYAV 520 - Aviation Cybersecurity Threats, Actors, Tools, and Techniques	3
Semester Hours	3

Requirements	Credits
CYAV 525 - Aviation Cybersecurity Risk Management and Resilience	3
Semester Hours	3

Requirements	Credits
AMNT 609 - Aircraft Maintenance Management	3
Semester Hours	3

Total Credits

Total Hours for All Requirements: 15

Year Two

Requirements	Credits
CYAV 510 - Security Engineering and Management	3
Semester Hours	3

Requirements	Credits
CYAV 516 - Operational Technology Risks in Aviation - IoT, ICS, SCADA	3
Semester Hours	3

Requirements	Credits
CYAV 517 - Uncrewed and Autonomous Systems Cybersecurity	3
Semester Hours	3

Requirements	Credits
SPAC 515 - Cybersecurity Applications in Space	3
Semester Hours	3

Requirements	Credits
CYAV 526 - Cybersecurity Standards, Laws, and Regulations	3
Semester Hours	3

Total Credits

Total Hours for All Requirements: 15

One Year Plan

Year One

Requirements	Credits
ASCI 602 - The Air Transportation System	3
CYAV 515 - Foundations of Aviation Cybersecurity	3
Semester Hours	6

Requirements	Credits
CYAV 520 - Aviation Cybersecurity Threats, Actors, Tools, and Techniques	3
CYAV 525 - Aviation Cybersecurity Risk Management and Resilience	3
Semester Hours	6

Requirements	Credits
AMNT 609 - Aircraft Maintenance Management	3
CYAV 510 - Security Engineering and Management	3
Semester Hours	6

Requirements	Credits
CYAV 516 - Operational Technology Risks in Aviation - IoT, ICS, SCADA	3
CYAV 517 - Uncrewed and Autonomous Systems Cybersecurity	3
Semester Hours	6

Requirements	Credits
SPAC 515 - Cybersecurity Applications in Space	3
CYAV 526 - Cybersecurity Standards, Laws, and Regulations	3
Semester Hours	6

Total Credits

Total Hours for All Requirements: 30

Estimated Cost of Attendance

Estimated Cost of Attendance: California Student Information (<https://catalog.erau.edu/student-life/student-affairs/california-student/>)