EMBRY-RIDDLE
Aeronautical University
ASIA

Graduate Certificate in Aviation Cybersecurity (Asia-focus)

Topics in Aviation Cybersecurity

This course is one of four cybersecurity courses required for the Aviation Cybersecurity Graduate Certificate. This 3-day, 24-hour course is designed with a particular emphasis on the Asia-Pacific Region.

Upon completion of this course, students should understand the cyber threat landscape, and apply the lessons of cyber defence to many actors within the aviation and aeronautics industry, including airlines, airplanes, manufacturers, airports, cargo and other vendors, unmanned systems, and more. Topics include cyber threats to all aspects of the industry, including communications, navigation, supply chain, and airports. Examination of frameworks being devised to protect assets from the cyber-attack vector, as well as vulnerabilities, protection, and countermeasures. Students will explore the current research literature concerning cybersecurity and information assurance as it impacts aviation.

Learning Objectives

Upon course completion, trainees will be able to:

- Characterize the latest issues and trends in the field of cybersecurity, particularly as they impact aviation.
- Compare and contrast the evolving aviation cybersecurity threat landscape that will dominate the field in the next three to five years.
- Identify the system of systems that comprise the aviation and aeronautics sector and cyber-attack vectors unique to the aviation industry.
- Communicate to colleagues and superiors about the current state of research in a particular aviation cybersecurity subject area.
- Evaluate the legal, policy, and societal implications of emerging cybersecurity technologies and research, and the potential impact on the future of the aviation industry.
- Describe the methods by which an attacker would plan an attack on a system, and find and exploit vulnerabilities, and the methods by which a defender would build a proper cyber defense.

Course Contents

- System of Systems overview
- Aviation System Design and Vulnerabilities
- Threat Landscape and Attack Vectors
- Information Security Risk Assessments
- Emerging Technologies and Research Trends
- Cyber Security Defense Mechanisms
- Policy and Training

Who Should Attend

- Students about to enter, or recently entered the aerospace workforce
- Aerospace professionals in an operations or management role (airport, airline, air navigation, MRO, legal, etc.)
- Government officials in the aerospace industry
- Other professionals interested in the Aviation Cybersecurity landscape in Asia-Pacific

Training Method

- Face-to-Face instructions in classroom or using Virtual Reality, or online synchronous
- Supported by practical case studies
- OJT may be provided if coordinated with airport authority.

General Information

Duration: 3 days or 24 hours

Venue: Local or Virtual Classroom

Participants: Maximum 25

Prerequisites:

- Familiarity with IT word-processing and presentation software
- Basic knowledge of aviation industry