International Civil Aviation Organization
North American, Central American and Caribbean Office

INFORMATION PAPER

NACC/DCA/12 — IP/13
18/06/24

Twelfth North American, Central American and Caribbean Directors of Civil Aviation Meeting (NACC/DCA/12)

Placencia, Stann Creek District, Belize, 9-11 July 2024*

Agenda Item 3: Aviation Security (AVSEC) and Facilitation (FAL)

EASA'S CYBERSECURITY INITIATIVES IN AVIATION

(Presented by EASA)

EXECUTIVE SUMMARY	
The European Union Aviation Safety Agency (EASA) has been actively engaged in enhancing cybersecurity within the aviation sector through a multifaceted approach. This involves rulemaking, support for information sharing, and competence building, all aimed at strengthening the industry's resilience against cyber threats.	
Strategic Objectives:	• Safety • Security & Facilitation
References:	• EASA Part-IS Regulation

1. Introduction

1.1 The below image summarises the different activities carried out by the Agency to improve cyber resilience in aviation.

2. Competence Building and Workshop in Costa Rica (under the EU LAC APP II project)

2.1 Fostering competence building in cybersecurity is a critical aspect of EASA's efforts. The agency has developed guidelines and acceptable means of compliance (AMC) to help organizations meet cybersecurity regulatory requirements. These guidelines cover various aspects of cybersecurity, including personnel requirements, risk assessment, and incident management.

2.2 EASA mandates that organizations appoint accountable managers and nominate responsible personnel with the appropriate knowledge, background, and experience to oversee cybersecurity activities. These individuals are tasked with ensuring compliance with regulations, managing the cybersecurity risks, and maintaining continuous improvement in cybersecurity practices. Additionally, EASA promotes the use of training and awareness programs to equip staff with the necessary skills to handle cybersecurity challenges effectively.

2.3 To further support competence building, EASA organises workshops, conferences, and seminars to raise awareness and promote a culture of cybersecurity within the aviation sector. These events provide an opportunity for participants to share knowledge, discuss challenges, and explore solutions to enhance cybersecurity resilience in aviation.

2.4. To this end, and following an interest expressed by ACSA/COCESNA, EASA is organising a workshop in Costa Rica in October to share the EU's experience in aviation cybersecurity, including the challenges and threats faced and the regulatory responses formulated. The workshop will also allow participants to explore the impact of security breaches on aviation safety and the potential operational disruptions they can cause.

3. Rulemaking

3.1 EASA's rulemaking activities focus on establishing comprehensive regulations and guidelines to ensure robust cybersecurity practices across the aviation industry. A cornerstone of these regulations is the Basic Regulation, which establishes the legal framework for compliance with the certification

requirements for civil aircraft. Every aircraft designed and manufactured in the European Union requires a certification issued by EASA. The procedures for certification of aeronautical products (aircraft, engines, and propellers) are contained in EC Regulation 748/2012 Annex I – Part 21.

3.2 Following the updated mandate in the Basic Regulation of July 2018, EASA has implemented amendments to the certification provisions to address information security aspects in the certification process of aeronautical products. Specifically, the EASA ED Decision 2020/006/R of July 2020 issued amendments to CS-25, CS-27, CS-29, CS-APU, CS-E, CS-ETSO, CS-P, and to the related acceptable means of compliance (AMC) and/or guidance material (GM), along with the creation of **AMC 20-42**, AMC/GM to CS-23, and AMC/GM to Part 21.

3.3 In the context of aircraft certification, cybersecurity is commonly understood as the protection of aviation information systems against intentional unauthorized electronic interactions (IUEI), and the means to mitigate their consequences on safety. To this extent, the amendments to the Certification Specifications (CS) mandate that “aeroplane equipment, systems and networks, considered separately and in relation to other systems, must be protected from intentional unauthorized electronic interactions that may result in adverse effects on the safety of the aeroplane.”

3.4 Key among EASA's regulations is the implementation of Part-IS, which outlines the Information Security Management System (ISMS) requirements. Part-IS regulation mandates that approved organizations implement measures for the detection, response, and recovery from information security incidents. This includes developing detection strategies to identify deviations from functional baselines, defining response procedures to contain and mitigate incidents, and establishing recovery measures to restore normal operations. Additionally, the regulations require organizations to maintain detailed records of their cybersecurity activities, ensuring traceability and compliance with regulatory standards.

4. Collaboration and Information Sharing

4.1 EASA recognizes the importance of information sharing in enhancing cybersecurity resilience. To this end, the agency has supported the creation of the European Centre for Cybersecurity in Aviation (ECCSA) which serves as a sharing platform for organisations and authorities that are relevant for the European aviation system.

4.2 EASA has also established the European Strategic Coordination Platform (ESCP), which brings together national aviation authorities, airlines, and other industry players to share intelligence on emerging threats and vulnerabilities. Additionally, EASA collaborates with international bodies such as the International Civil Aviation Organization (ICAO) to coordinate on cybersecurity matters at global level.

— END —