59th CONFERENCE OF DIRECTORS GENERAL OF CIVIL AVIATION ASIA AND PACIFIC REGIONS

Cebu, Philippines
14 to 18 October 2024

AGENDA ITEM 5: AVIATION SECURITY AND FACILITATION

ENHANCING CYBERSECURITY THROUGH COLLABORATION: THE EUROPEAN UNION'S APPROACH TO CYBERSECURITY

(Presented by EASA)

INFORMATION PAPER

SUMMARY

The EU has developed various regulatory frameworks and initiatives to enhance information sharing and operational safety standards. This paper aims to inform the Conference about these initiatives, focusing on the EU Part-IS (Information Security) framework and the benefits of increased information exchange.

ENHANCING CYBERSECURITY THROUGH COLLABORATION: THE EUROPEAN UNION'S APPROACH TO CYBERSECURITY

1. INTRODUCTION

1.1 The European Union Aviation Safety Agency (EASA) is dedicated to promoting aviation safety and security within the EU and globally. The EU has developed various regulatory frameworks and initiatives to enhance information sharing and operational safety standards. This paper aims to inform the Conference about these initiatives, focusing on the EU Part-IS (Information Security) framework and the benefits of information exchange.

2. DISCUSSION

2.1 The increasing exposure of civil aviation to cyber threats necessitates robust protective measures. The EU's cybersecurity objectives include standardised risk assessment methods, continuous adaptation of countermeasures, and enhanced information sharing.

2.2 EASA has identified several enablers to achieve these cybersecurity objectives, including:

- Training and Awareness: Building a cybersecurity culture through education and training.
- Cyber Security Centres: Facilitating voluntary information sharing and providing proactive services.
- Research and Development: Promoting research on aviation-specific cybersecurity vulnerabilities and secure design principles.
- Rulemaking and Regulatory Oversight: Ensuring cybersecurity considerations are integrated into all areas of civil aviation regulation.
- Collaboration: Establishing frameworks for coordinated strategies, policies, and plans at national, regional, and international levels.

2.3 To ensure effective protection against cyber threats, EASA has developed a common cybersecurity framework involving all aviation stakeholders. This framework defines the roles, responsibilities, and rules for maintaining operational resilience and recovering from cyber-attacks. The agency has also developed guidelines and acceptable means of compliance (AMC) to help organisations meet these cybersecurity regulatory requirements. These cover various aspects of cybersecurity, including personnel requirements, risk assessment, and incident management.

2.4 Key among EASA's regulations is the implementation of Part-IS[1], which outlines the Information Security Management System (ISMS) requirements. Part-IS regulation mandates that approved organisations 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 organisations to maintain detailed records of their cybersecurity activities, ensuring traceability and compliance with regulatory standards.

2.5 The key components of Part-IS include:

- Risk Management: Part-IS requires regular risk assessments and the implementation of

[1] A set of rules contained in Commission Delegated Regulation (EU) 2022/1645 of 14 July 2022 and in Commission Implementing Regulation (EU) 2023/203 of 27 October 2022 laying down requirements for the management of information security risks with a potential impact on aviation safety for aviation organisations and authorities across the entire aviation domain.

appropriate mitigation strategies.
- Information Protection: It mandates stringent measures for safeguarding information, such as encryption, access controls, and regular audits.
- Incident Response: The framework sets out protocols for detecting, reporting, and managing information security incidents.
- Awareness and Training: Ongoing education and training programs are essential for maintaining high awareness levels among aviation personnel.

2.6 EASA mandates that organisations 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 cybersecurity risks, and maintaining continuous improvement in cybersecurity practices. Additionally, EASA promotes training and awareness programmes to equip staff with the necessary skills to handle cybersecurity challenges effectively.

2.7 Implementing Part-IS across the EU has significantly strengthened the aviation sector's resilience against cyber threats by:

- Improving risk management practices
- Enhancing data protection and operational continuity
- Strengthening incident response capabilities
- Raising information security awareness among aviation professionals

2.8 EASA also recognises 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 relevant to the European aviation system.

2.9 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. In our interconnected aviation world, the safety and security of one region can impact others. EASA also collaborates with international bodies such as ICAO to coordinate cybersecurity matters at the global level.

2.10 The ICAO Trust Framework is an international initiative to establish a global, harmonised approach to information sharing and security in civil aviation. It aims to create a trusted environment where states can securely and efficiently exchange information, enhancing overall aviation safety and security. The EU’s commitment to the ICAO Trust Framework aims to:

- Enhance global aviation security standards
- Improve interoperability and information sharing capabilities
- Strengthen international partnerships and collaborations
- Increase resilience against emerging security threats

2.11 The EU’s commitment to the development and implementation of the ICAO Trust Framework includes:

- Active Participation: EASA takes part in ICAO meetings, working groups, and initiatives, sharing insights and best practices.
- Aligning Standards: The EU will ensure the alignment of its regulatory frameworks, including Part-IS, with the principles of the ICAO Trust Framework to ensure consistency and interoperability.
- Technological Integration: The EU will use advanced technologies to support secure information exchange, contributing to the technical aspects of the Trust Framework.

2.12 To support collaboration and competence building further, EASA also organises

workshops, conferences, and seminars to raise awareness, build capacity 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. For example, EASA organised a workshop in Sri Lanka in May 2024 for the Asia region to share the EU's experience in aviation cybersecurity, including challenges, threats, and regulatory responses. The workshop brought together more than 60 security, cybersecurity, and IT specialists from various countries, including Bangladesh, Bhutan, Brunei, Indonesia, Laos, Malaysia, Maldives Nepal, Pakistan, Philippines, Sri Lanka, Thailand, and Vietnam.

Key discussions focused on the following areas:

- Cyber Threat Intelligence and Information Sharing: Emphasizing the importance of defining cyber roles, sharing information among stakeholders, and distinguishing between threat data and threat intelligence.
- Risk Management: Addressing the iterative process of risk assessment and treatment, including defining asset inventory and establishing risk treatment methodologies.
- Incident Management and Reporting: Highlighting the need for comprehensive incident response plans and regular risk management exercises.

Industry practices were discussed by representatives from Airbus, Leonardo, and Spice Jet, while panel discussions revealed varying levels of cybersecurity implementation across different states, underscoring the need for greater collaboration.

The workshop concluded with recommendations for the region, including establishing a strategic coordination platform and a network of cybersecurity analysts in Asian. EASA expressed its commitment to supporting these efforts to foster greater collaboration and information exchange in the Asia region.

2.13 Fostering greater information exchange between regions is crucial. By sharing best practices, threat intelligence, and security incidents, regions can collectively improve their aviation safety and security standards. This can lead to:

- Better Threat Detection: Sharing threat intelligence helps detect and mitigate potential security threats early.
- Standardisation of Practices: Collaboration leads to harmonised security practices, reducing discrepancies and improving overall safety.
- Resource Optimisation: Joint initiatives allow pooling of resources, expertise, and technologies, optimising efforts and costs.
- Stronger Relationships: Regular communication and collaboration build stronger inter-regional relationships, fostering a unified approach to aviation security.

2.14 The European Union, through EASA, is committed to advancing aviation safety and security by promoting robust information security frameworks like Part-IS and actively engaging with global initiatives and partner regions. Increased information exchange between regions offers numerous benefits, including enhanced threat detection, standardised practices, resource optimisation, and stronger international relationships. Civil Aviation Authorities in the ICAO Asia Pacific region are encouraged to engage with these initiatives, leveraging shared knowledge and expertise to collectively raise the standards of aviation safety and security worldwide.

3. ACTION BY THE CONFERENCE

3.1 The Conference is invited to note the information contained in this paper and consider the potential benefits of greater collaboration and information exchange in enhancing aviation safety and security.

— END —