61ST CONFERENCE OF DIRECTORS GENERAL OF CIVIL AVIATION ASIA AND PACIFIC REGION

Kuala Lumpur, Malaysia
7 – 11 September 2026

AGENDA ITEM 5: AVIATION SECURITY AND FACILITATION

STRENGTHENING AVIATION CYBERSECURITY THROUGH PRACTICAL COLLABORATION: THE EUROPEAN UNION'S APPROACH AND OPPORTUNITIES FOR THE ASIA/PACIFIC REGION

Presented by the European Union Aviation Safety Agency (EASA)

SUMMARY

Civil aviation increasingly depends on connected digital systems, shared operational data and third-party services. A significant information security event can disrupt operations, reduce confidence and, where safety-relevant systems or data are affected, create safety risk. This paper presents the European Union's risk-based approach to aviation cybersecurity, with a focus on Part-IS, the EU framework for managing information security risks with a potential impact on aviation safety.

The paper also describes supporting work by EASA on guidance, awareness, cooperation between competent authorities, trusted information sharing and international engagement through ICAO. It suggests practical areas for voluntary regional cooperation among Asia/Pacific CAAs and industry, taking account of different national contexts, resources and levels of maturity.

STRENGTHENING AVIATION CYBERSECURITY THROUGH PRACTICAL COLLABORATION: THE EUROPEAN UNION'S APPROACH AND OPPORTUNITIES FOR THE ASIA/PACIFIC REGION

1. INTRODUCTION

1.1 Civil aviation now relies on interconnected digital systems, shared data, software-enabled aircraft and equipment, air traffic management tools, airport systems, maintenance records, cloud services and specialist suppliers. These developments bring clear safety, efficiency and service benefits, but they also create new dependencies.

1.2 An information security event does not need to involve direct interference with an aircraft to be relevant to aviation. Loss of availability, integrity or confidentiality of safety-relevant data, operational systems or trusted communications can delay decisions, disrupt services, weaken oversight or, in some circumstances, contribute to safety risk.

1.3 For Civil Aviation Authorities (CAAs), aviation cybersecurity is therefore not only an information technology issue. It is also relevant to safety oversight, aviation security, certification, continuing airworthiness, air operations, air navigation services, aerodromes and the management of sensitive information between authorities and industry.

1.4 The Asia/Pacific region includes some of the world's largest aviation hubs, rapidly growing markets, small island and remote operations, and States with different regulatory, technical and resource starting points. A useful approach to aviation cybersecurity therefore needs to be risk-based, scalable and proportionate, while still supporting common principles and trusted cooperation.

1.5 This paper shares the European Union's experience in developing and implementing a framework for managing information security risks with a potential impact on aviation safety. It focuses on the EU Part-IS framework and related EASA activities on guidance, information sharing, awareness raising and capacity building. The intention is not to present the EU model as the only possible solution, but to offer practical points that may support discussion among Asia/Pacific CAAs.

2. DISCUSSION

The aviation cybersecurity challenge

2.1 The aviation cybersecurity challenge is partly technical, but it is also organisational. Effective protection depends on knowing which systems, data, interfaces and services are safety-relevant; understanding how they are connected; assigning clear responsibilities; and ensuring that events can be detected, reported, assessed and managed in a timely manner.

2.2 A practical starting point is to identify the information assets and services that matter most for safe and secure operations. These may include operational data, flight and maintenance information, aerodrome and air navigation systems, digital certificates, identity and access management arrangements, communications with suppliers and information held by service providers.

2.3 For authorities and organisations with limited resources, the priority is not to create a large new administrative burden. It is to define the scope, establish ownership, understand the main dependencies, treat the most important risks and ensure that staff know how to report and escalate issues. More mature arrangements can then be developed progressively.

2.4 The EU approach has been developed around several mutually supporting elements:

- a risk-based regulatory framework for organisations and competent authorities;
- clear accountability for managing information security risks with potential aviation safety

impacts;

- acceptable means of compliance and guidance material to support implementation and oversight;
- training and awareness to build a common understanding between safety, aviation security, operational and technical staff;
- trusted information sharing between authorities and industry; and
- international cooperation, including through ICAO activities.

Part-IS: a risk-based framework

2.5 Part-IS (Information Security) is the EU framework for managing information security risks with a potential impact on aviation safety. It is contained in Commission Delegated Regulation (EU) 2022/1645 and Commission Implementing Regulation (EU) 2023/203. It applies to relevant aviation organisations and competent authorities and requires an Information Security Management System (ISMS) that is appropriate to the nature and complexity of the organisation.

2.6 In practical terms, an ISMS provides a structured way to identify information security risks, decide what controls are needed, monitor whether those controls remain effective and improve the system over time. Under Part-IS, attention is placed on events and vulnerabilities that could affect aviation safety, rather than on cybersecurity in the abstract.

2.7 Key elements of Part-IS include:

- identifying information assets, systems, interfaces, dependencies and services that may be relevant to aviation safety;
- assessing information security risks and treating them through proportionate measures;
- establishing arrangements for detection, response, recovery and reporting;
- defining responsibilities for accountable managers and nominated personnel;
- ensuring appropriate competence, awareness and trustworthiness of staff; and
- maintaining records and using lessons learned to support continuous improvement.

2.8 A central feature of the framework is proportionality. It does not require every organisation to have the same structure or the same controls. It does require each organisation and authority to understand its own risk exposure, justify its chosen measures and be able to show that the arrangements are effective in practice.

The role of competent authorities

2.9 The role of the competent authority is important in two respects. First, authorities need to manage their own information security risks, including risks to oversight data, information exchanges and internal systems. Secondly, they need an oversight approach that allows them to assess whether regulated organisations have understood and managed their safety-relevant information security risks.

2.10 This often requires closer cooperation between functions that may not traditionally have worked together on routine oversight. These include safety oversight, aviation security, information technology or cybersecurity teams, legal advisers, crisis management functions, national cybersecurity agencies and, where relevant, Computer Security Incident Response Teams.

2.11 Experience in the EU suggests that implementation is most effective when it is treated as

a progressive risk management exercise rather than a checklist. Common implementation challenges include defining the scope of safety-relevant information assets, understanding dependencies between organisations, setting proportionate expectations for smaller entities, and deciding how sensitive reports should be protected and followed up.

2.12 EASA has developed Acceptable Means of Compliance (AMC) and Guidance Material (GM) to support authorities and organisations. These materials help translate regulatory requirements into practical implementation and oversight considerations, including risk assessment, incident management, personnel requirements, documentation and continuous improvement.

Trusted information sharing

2.13 Information sharing is another important part of the EU approach. Aviation systems are interconnected, and a weakness or incident in one part of the system may be relevant to others. At the same time, cybersecurity information is often sensitive. Useful sharing therefore depends on trust, clear handling rules, protection of sensitive information and a shared understanding of how the information will be used.

2.14 EASA has supported the creation of the European Centre for Cybersecurity in Aviation (ECCSA), a voluntary platform for sharing relevant information within the European aviation system. Such arrangements can help organisations and authorities identify emerging risks earlier and avoid addressing similar issues in isolation.

2.15 At authority level, EASA and the Member States Advisory Board have established the Network of Cybersecurity Analysts (NoCA). NoCA supports cooperation between competent authorities, including analysis of information security incidents that have or may have an impact on aviation safety. It also helps authorities develop a more common understanding of emerging risks and practical oversight questions.

International and regional cooperation

2.16 The EU also participates in relevant ICAO initiatives. The ICAO Trust Framework is intended to support secure and trusted exchange of information in civil aviation. EASA also participates in the ICAO Cybersecurity Panel, which supports coordinated and globally harmonised cybersecurity action in civil aviation, including work related to Standards and Recommended Practices.

2.17 Regional dialogue is essential because cybersecurity risks do not stop at national or organisational boundaries. Airlines, airports, air navigation service providers, manufacturers, maintenance organisations and digital service providers often operate across jurisdictions. Trusted cooperation can help authorities and industry identify common risks earlier and respond more consistently when incidents occur.

2.18 In April 2026, EASA, with the support of the Association of Aerospace Industries (Singapore) and the Civil Aviation Authority of Malaysia, organised aviation cybersecurity workshops in Singapore and Kuala Lumpur. The workshops brought together more than 230 representatives from authorities and industry, including participants with safety and security backgrounds. Discussions covered the structure of Part-IS, early implementation experience, risk assessment and treatment, asset inventories, personnel requirements, incident management, reporting, exercises and oversight approaches.

2.19 The level of participation showed strong regional interest in practical approaches to aviation cybersecurity. It also suggested that future exchanges would be most useful if they focus on concrete oversight questions, realistic scenarios and trusted discussion between authorities and industry.

Possible areas for practical cooperation

2.20 For Asia/Pacific CAAs, possible areas for practical cooperation could include the following:

Area	Why it matters	Possible activity
Oversight organisation	Authorities need clear roles across safety, aviation security, cyber, legal and crisis functions.	Peer exchange on oversight models and escalation contacts.
Safety-relevant scope	Oversight depends on knowing which systems, data, interfaces and suppliers could affect safety.	Short workshop using sample airline, airport or ANS scenarios.
Occurrence reporting and handling	Reports only have value if they are protected, assessed and acted upon.	Compare reporting channels, confidentiality rules and follow-up processes.
Tabletop exercises	Decision-making and coordination are easier to improve before a real incident.	Regional exercise based on a supplier, airport or air navigation service disruption.
Training for inspectors and managers	Cyber oversight needs a shared vocabulary across disciplines.	Practical training module for safety, security and technical staff.
Trusted information exchange	Many risks and lessons learned are relevant beyond one State or organisation.	Voluntary contact network with agreed handling expectations.

2.21 These exchanges need not require identical regulatory models. They can support a common understanding of safety-relevant information security risks while allowing each State to adapt measures to its own legal framework, resources and maturity level.

2.22 EASA has also organised Part-IS implementation workshops in Cologne in 2024 and 2025, with public livestreaming, and a further workshop is planned in 2026 in hybrid mode. These activities are intended to support implementation, share lessons learned and make practical material available beyond the EU.

2.23 EASA has published guidance documents on Part-IS implementation, developed in cooperation with EU Member State authorities. These documents are available through the EASA Cybersecurity Community and may be useful reference material for authorities or organisations considering how to structure their own approaches.

2.24 The European Union, through EASA, remains committed to cooperation with ICAO, partner States and regional organisations on aviation cybersecurity. The EU experience indicates that useful progress can be made when cybersecurity is addressed as part of aviation safety and security governance, supported by proportionate regulation, trusted information sharing and practical capacity building.

3. ACTION BY THE CONFERENCE

3.1 The Conference is invited to:

a) note the information contained in this paper;

b) encourage Administrations to consider, as appropriate, how information security risks with potential aviation safety impacts are identified and managed within existing safety, aviation security and oversight arrangements;

c) support practical, voluntary and trusted exchange of experience among States, industry and regional partners on aviation cybersecurity, including coordination with national cybersecurity bodies, risk management, incident response, reporting, exercises and oversight; and

d) invite ICAO Asia and Pacific, interested Administrations and relevant partners to consider a follow-up regional activity, supported by EASA, to identify practical priorities for cooperation, including trusted information sharing.

— END —