International Civil Aviation Organization

MIDANPIRG/23 & RASG-MID/13 Meetings

(Cairo, Egypt, 14 – 18 June 2026)

Agenda Item 5.7: CNS

STRENGTHENING PROPORTIONATE CYBERSECURITY GOVERNANCE FOR AIR NAVIGATION SERVICES SYSTEMS

(Presented by The United Arab Emirates)

SUMMARY

This Working Paper highlights the need for proportionate, risk-based, and operationally informed cybersecurity governance for Air Navigation Services (ANS) systems. It emphasizes that cybersecurity controls should be scaled according to system criticality, safety consequence, service continuity impact, and exposure.
The paper further highlights the importance of aligning aviation safety regulation and national cybersecurity requirements through an integrated assurance approach, consistent with ICAO's aviation cybersecurity direction.

Action by the meeting is at paragraph 4.

REFERENCE

- ICAO AVIATION CYBERSECURITY STRATEGY.
- ICAO CYBERSECURITY ACTION PLAN.
- ICAO DOC 10213 – GLOBAL CYBER RISK CONSIDERATIONS, FIRST EDITION (ADVANCE UNEDITED), 2025.
- EUROCAE ED 205A – PROCESS STANDARD FOR SECURITY CERTIFICATION AND DECLARATION OF ATM/ANS GROUND SYSTEMS, 2022.
- (EASA), PART IS – INFORMATION SECURITY REGULATIONS (EU) 2022/1645 AND (EU) 2023/203

1. INTRODUCTION

1.1 ANS are increasingly dependent on interconnected digital platforms, supplier-supported systems, remote maintenance arrangements, data exchange, automation, and emerging AI-enabled capabilities. This evolution reinforces the need for robust cybersecurity and for a mature approach to selecting, scaling, and governing cybersecurity controls.

1.2 In some modernization and system replacement projects, cybersecurity requirements may be applied as a fixed compliance process rather than as a risk-based governance activity. While such an approach may satisfy procedural requirements, it may not always deliver proportionate or operationally meaningful security.

1.3 The main challenge is not the need for cybersecurity itself. The challenge lies in how cybersecurity is governed, interpreted, and implemented within a safety-critical operational aviation environment.

2. DISCUSSION

2.1 ANS systems, particularly ATM systems, operate in a complex space between traditional Information Technology (IT) and Operational Technology (OT). However, they should not be treated as either in isolation. Different ANS systems have different operational roles, safety consequences, exposure levels, and continuity requirements.

2.2 Therefore, cybersecurity controls should not be applied uniformly across all systems. Controls that are appropriate for corporate IT environments may require adaptation before being applied to live ANS operational environments, to avoid unintended operational, safety, or service continuity impacts.

2.3 Cybersecurity governance should be proportionate to the system's operational criticality, safety consequence, service continuity impact, and cyber exposure. Applying uniform cybersecurity requirements across all systems may lead to disproportionate effort for lower-risk systems and insufficient tailored assurance for systems with direct safety or service continuity implications. Accordingly, a mature cybersecurity governance model should ensure that the most critical systems receive appropriate tailored assurance, while lower-risk systems remain protected through proportionate baseline controls.

2.4 Cybersecurity in ANS should be integrated with safety, operations, engineering, change management, and service continuity arrangements. Cybersecurity controls should be assessed for both technical effectiveness and operational impact.

2.5 Cybersecurity requirements should be determined by considering the system's operational role, safety consequence, service continuity impact, exposure, supplier dependency, and the potential operational impact of the cybersecurity control itself. This approach would support cybersecurity as an enabler of resilience rather than a perceived barrier to operational delivery.

2.6 ANSPs are increasingly subject to cybersecurity expectations from both aviation regulators and national cybersecurity authorities. These expectations should be aligned to ensure that cybersecurity assurance supports aviation safety, service continuity, national resilience, and operational practicality.

2.7 If these expectations are managed separately, they may result in duplicated evidence, conflicting interpretations, or controls that satisfy one compliance requirement while creating operational challenges under another.

2.8 ANS cybersecurity governance should therefore act as the bridge between aviation safety regulation and national cybersecurity requirements. This would support one integrated assurance conversation covering safety, operational continuity, cyber resilience, and national critical infrastructure protection.

2.9 This is also consistent with ICAO's aviation cybersecurity direction, which recognizes cybersecurity as a cross-cutting aviation issue requiring coordination across aviation authorities, national cybersecurity entities, service providers, industry, and other relevant stakeholders.

2.10 While several international and sector-specific references are available, there is no single universally adopted ATM-specific cybersecurity governance model that fully addresses the operational, safety, and continuity context of ANS systems.

2.11 These references provide valuable guidance, but they do not remove the need for operational judgement. Their application must be interpreted in accordance with the safety, continuity,

and operational context of ANS systems. Therefore, the regional objective should include developing a common understanding of how cybersecurity frameworks can be applied proportionately to ANS environments.

2.12 The governance challenge will become more significant as AI, machine learning, and higher levels of automation become more embedded in ANS environments. AI-enabled and automated decision-support capabilities introduce additional governance considerations beyond traditional cybersecurity assurance.

2.13 Accordingly, cybersecurity governance for future ANS systems must be linked with safety assurance, human factors, data governance, operational validation, and regulatory oversight.

2.14 A proportionate cybersecurity governance model should be based on the following high-level principles:

- operational context and system criticality;
- safety and service continuity impact;
- proportionate assurance and control scaling;
- integration between cybersecurity, safety, operations, engineering, and change management;
- alignment between aviation and national cybersecurity requirements; and
- future readiness for automation and AI-enabled capabilities.

2.15 ANSPs may also benefit from classifying ANS systems at a high level to support proportionate cybersecurity assurance. Such classification may distinguish between safety-critical operational systems, operational support systems, training environments, information systems, and administrative or corporate systems.

2.16 A proportionate and operationally informed cybersecurity governance model would support improved protection of safety-critical ANS systems, better alignment between cybersecurity controls and operational realities, reduced duplication between aviation and national cybersecurity compliance, stronger integration across safety, engineering, operations, supplier governance and service continuity, and improved readiness for automation, AI, and future digital ANS capabilities.

3. CONCLUSION

3.1 Cybersecurity is essential for the protection of ANS systems and the continuity of air navigation service provision. However, cybersecurity should be governed in a proportionate and operationally informed manner, rather than applied as a uniform process across all systems.

3.2 ANS systems are not simply IT systems or generic OT systems. They are operational aviation systems with safety, service continuity, cyber resilience, and national critical infrastructure implications.

3.3 The required direction is therefore stronger governance based on operational judgement, system criticality, regulatory alignment, and the need to support safe, resilient, and continuous air navigation service provision.

4. ACTION BY THE MEETING

4.1 The meeting is invited to:

a) note the importance of applying cybersecurity governance to ANS systems in a proportionate, operationally informed, and risk-based manner;

b) recognize the need to align cybersecurity controls with the operational role, safety consequence, service continuity impact, and exposure of ANS systems;

c) encourage States and ANSPs to promote criticality-based cybersecurity governance for ANS systems, consistent with ICAO's aviation cybersecurity direction;

d) promote the integration of cybersecurity assessment with safety management, operational change management, engineering assurance, supplier governance, and service continuity planning;

e) encourage coordination between civil aviation authorities, national cybersecurity authorities, ANSPs, and industry stakeholders to support an integrated assurance approach; and

f) develop regional guidance material and facilitate the exchange of best practices on proportionate cybersecurity governance for ANS systems, including future automation and AI-enabled capabilities.

- END -