International Civil Aviation Organization

MIDANPIRG/20 and RASG-MID/10 Meetings

(Muscat, Oman, 14-17 May 2023)

Agenda Item 6.6: CNS

ANS CYBER RESILIENCE

(Presented by the Secretariat)

SUMMARY

This paper presents the outcome ANS Cyber Resilience Table-top exercise and the first meeting ANS Cyber Security Working Group. The Paper proposes action list to be endorsed as MID Region ANS Cyber security Actions plan and propose actions to enhance the functions and use of the ATM Data cyber security portal (ADCS).

Action by the meeting is at paragraph 3.

REFERENCES

- ICAO Assembly Resolution A41-19
- MIDANPIRG/19

1. INTRODUCTION

1.1 The aviation sector is increasingly reliant on the availability, integrity and confidentiality of information, data, and systems; Mindful that cyber threats to civil aviation are rapidly and continuously evolving, that aviation continues to be a target for perpetrators in the cyber domain as in the physical one, and that cyber threats can evolve to affect critical civil aviation systems worldwide.

1.2 The multi-faceted and multi-disciplinary nature of cybersecurity challenges and solutions and noting that cyber risks can simultaneously affect a wide range of aviation areas and spread rapidly.

1.3 The amendment 12 of the Annex 17 (effective 2011) included provisions to further strengthen Standards and Recommended Practices in order to address new and emerging threats to civil aviation including the security of air traffic service providers.

1.4 The first Meeting of ANS Cyber Security Working Group (ACS WG/1) was successfully held during in Amman, Jordan, 16 November 2022 back-to- back with the ANS Cyber Resilience Tabletop exercise (13-15 November 2022).

2. DISCUSSION

2.1 The ATSPs contribute to aviation security in the prevention of, and response to, acts of unlawful interference. This contribution to aviation security usually involves ATSP airspace management for ATM security purposes. Specific ATSP responsibilities for airspace management for ATM security purposes should be identified in agreements with air defence and law enforcement agencies to ensure proper integration of responsibilities of all agencies directly responsible for the State's airspace security.

2.2 ICAO Assembly resolution A41-19 called upon States and industry stakeholders to take the following actions to address cyber threats to Civil Aviation:

a) implement the ICAO Aviation Cybersecurity Strategy, and make use of the ICAO Cybersecurity Action Plan as a tool to support the implementation of the Aviation Cybersecurity Strategy;
b) designate the authority competent for aviation cybersecurity, and define the interaction between that authority and concerned national agencies;
c) define the responsibilities of national agencies and industry stakeholders with regard to cybersecurity in civil aviation;
d) develop and implement a robust cybersecurity risk management framework that draws on relevant safety and security risk management practices, and adopt a risk-based approach to protecting critical civil aviation systems, information, and data from cyber threats;
e) establish policies and instruments, and allocate resources to ensure that, for critical aviation systems: system architectures are secure by design; systems are protected and resilient; data is secured and available in storage and while in transfer; system monitoring, and incident detection and reporting, methods are implemented; incident recovery plans are developed and practiced; and forensic analysis of cyber incidents is carried out;
f) encourage government/industry coordination with regard to aviation cybersecurity strategies, policies, and plans, as well as sharing of information to help identify critical vulnerabilities that need to be addressed;
g) encourage civil/military cooperation with regard to identifying, protecting, and monitoring common vulnerabilities and data flows at interfaces between civil and military aviation systems, and collaborate in response to common cyber threats and recovery from cyber incidents;
h) develop and participate in government/industry partnerships and mechanisms, nationally and internationally, for the systematic sharing of information on cyber threats, incidents, trends and mitigation efforts;
i) design and implement a robust cybersecurity culture across the civil aviation sector;
j) encourage States to continue contributing to ICAO in the development of international Standards, strategies, and best practices to support advancing aviation cybersecurity and cyber resilience; and
k) continue collaborating in the development of ICAO's cybersecurity framework according to a horizontal, cross-cutting and functional approach involving aviation safety, aviation security, facilitation, air navigation, communication, surveillance, air traffic management, aircraft operations, airworthiness, and other relevant disciplines.

2.3 The meeting may wish to recall that MIDANPIRG/19 meeting encouraged States to ensure alignment of ANS national Cyber Security plan with ICAO of Cybersecurity Action Plan (CyAP), 2nd version.

2.4 The Air Navigation Cyber Security Working Group (ACS WG) conducted gap analysis between ICAO Cyber Security Action plan and the current implementation level in the MID region, the ACS WG/1 has developed initial list of actions for 2023-2024 (Draft MID Region ANS Cyber Security Action Plan) as at **Appendix A**.

2.5 The Draft MID Region ANS Cyber Security actions plan is a living document that will be reviewed and updated regularly, based on the global development and Regional implementation Status. The CNS SG/12 meeting proposed that the ACS WG/2 develop a survey to establish how States have implemented the identified actions. Therefore, the following Draft Conclusion is proposed:

Why	To assist States achieving the objectives of ICAO Cyber Security Strategy seven pillars in ANS area in a timely manner
What	Endorse MID Region ANS Cyber Security actions plan
Who	MIDANPIRG
When	May 2023

DRAFT CONCLUSION 20/XX: ***MID REGION ANS CYBER SECURITY ACTION PLAN***

That, in order to assist States achieving the objectives of ICAO Cyber Security Strategy seven pillars in ANS area in the MID Region:

a) the MID Region ANS Cyber Security actions plan at ***Appendix A*** *is endorsed;*

b) urge States to implement identified actions in a timely manner; and

c) ACS WG to develop a survey to establish how States have implemented the identified actions.

2.6 The CNS SG/12 meeting discussed the qualification and training needs for ANS Cyber Security inspector. The meeting requested ICAO to organize capacity building activities on ANS Cyber security in 2024-2025. Therefore, the CNS SG/12 proposed the following Draft Decision:

Why	To assist States building capacity on ANS cyber Security & Resilience
What	To organize Workshops/Training Course on ANS cyber Security & Resilience
Who	ICAO MID
When	2024

DRAFT DECISION 20/XX: ***ANS CYBER SECURITY CAPACITY BUILDING ACTIVITIES***

That, ICAO MID Office to organize capacity building activities on ANS Cyber Security in 2024.

2.7 The meeting may wish to note that ICAO MID will organize Cyber Security and Resilience symposium in Doha, Qatar, 6-8 November 2023.

2.8 The ANS Cyber Resilience Tabletop Exercise (TTX) was successfully conducted 13-15 November 2022. The CNS SG/12 supported the following recommendations emanated from the TTX:

b) States to develop disaster recovery plans as part of the resilient aviation ecosystem; the plan should consider communication, coordination and management oversight to support decision-making;
c) States to develop Cyber incidents management plan including defining clear lines of communication and escalation;
d) States to promote Cyber awareness training for all staff and in particular senior management recognizing that social engineering and Phishing continue to be a leading vector of attacks, humans are always the weakest link;
e) CAAs are encouraged to collaborate with their National Computer Emergency Response Team (CERT) for cross industry incident management, as appropriate;
f) Cyber Resilience is an evolving issue and States should include it in ANS contingency plan and to ensure that Contingency plan is known and practiced;
g) Cyber Resilience related procedures, risk analysis, exercises and trainings should be established and implemented;
h) An agreement on procedure on more timely coordination between FAS (ATSU) and airlines for abnormal flight plan submission is required;
i) States to perform drills, practice and have lessons learned on a regular basis, with the participation of all internal and external Stakeholders including senior management;
j) States to ensure regular coordination between regulators, ANSPs, airport operators and airlines regarding Cyber Resilience;
k) Contingency plan should be in place which including back up system and condition for manual procedure;
l) States to support implementation of Network monitoring, in particular monitoring of:
   - external links (external to the system)
   - security incidents specially during cases of cyber attacks; and
   - fault reporting and advance notification of maintenance activities; and
m) The experts to deal with cyber security/safety issues of ATM systems should be consisted of IT expertise as well as necessary knowledge on ANS and operational process.

2.9 In accordance with the MID Region ANS Cyber Security action plan, States should share experience on cyber threats and incidents. In this regard, the meeting recalled that UAE developed and hosted ATM data cyber security portal (ADCS Portal). Thus, the CNS SG/12 meeting requested ACS WG to review the portal function and propose solution(s) to enhance its use in the MID Region. Therefore, the following Draft Conclusion is proposed:

Why	To enhance the functions and make benefits of the ATM Data cyber security portal
What	To provide feedback on ADCS functions and tools and use it effectively
Who	MID States
When	Before October 2023

DRAFT CONCLUSION 20/XX: ENHANCEMENT ATM DATA CYBER SECURITY (ADCS) PORTAL

That, States be urged to:

a) review and update, as deem necessary, ANS Cyber Security focal point(s);

*b) provide feedback to the ADCS to Admin by **1 October 2023** for further enhancements; and*

c) use the ADCS effectively, share their experience related to cyber security, through the ADCS Portal

3. ACTION BY THE MEETING

3.1 The meeting is invited to:

a) urge States to:

i) Implement Assembly resolution A41-19;
ii) participate actively in the Cyber Security and Resilience Symposium;
iii) make extensive use of the ADCS and provide feedback as required in para XX; and
iv) review the recommendations emanated from the ANS Cyber Resilience TTX; and

b) endorse Draft Conclusions and Decision at Para. 2.5, 2.6 and 2.9

APPENDIX A

MID Region ANS Cyber Security Action Plan

2023-2024

Action Number	Specific Measures/Task	by	Start date of Implementation	Traceability to Cybersecurity Action Plan
MID-01	States to develop their own national/organizational Cyber Security policies using ICAO model Cybersecurity Policy at attachment A	MID States	2023	CyAP 0.1
MID-02	Plan, organize and support international and regional events to promote cybersecurity in civil aviation.	MID States ICAO MID	2023 - 2024	CyAP 1.8
MID-03	Establish a governance structure in the civil aviation for ANS cybersecurity field.	MID States	2023	CyAP 2.1
MID-04	Promote coordination mechanisms between civil aviation authorities and cybersecurity authorities.	MID States	2023	CyAP 2.4
MID-05	Establishment of a civil aviation ANS cybersecurity point of contact network.	MID States	2023	CyAP 5.5
MID-06	To share cybersecurity-related information using ADCS portal	MID States	2023 - 2024	CyAP 5.2
MID-07	develop and implement capabilities and plans for civil aviation cybersecurity incident detection, analysis and response at operational level.	MID States	2023 - 2024	CyAP 6.4
MID-08	Conduct periodically ANS Cyber Resilience table top and live exercises at Regional and national levels	MID States	2023 – 2024	CyAP6.6
MID-09	Organization of ANS Cyber Sec capacity building activities (ANS Cyber Security oversight, Managing Security risks in ATM)	ICAO MID	2023 – 2024	CyAP 7.5
MID-10	Identify potential threats and vulnerabilities for ANS systems	ACS WG MID States	2023 – 2024	-

-END-