International Civil Aviation Organization

MIDANPIRG Communication, Navigation and Surveillance Sub-Group

Twelfth Meeting (CNS SG/12)
(Amman, Jordan, 2-4 May 2023)

Agenda Item 4: CNS planning and implementation in the MID Region

OUTCOME OF THE FIRST MEETING OF ANS CYBER SECURITY WORKING GROUP (ACS WG/1) MEETING

(Presented by Secretariat.)

SUMMARY

This paper presents the outcome of the First Meeting of ANS Cyber Security Working Group (ACS WG/1) Meeting including the Draft MID region ANS Cyber Security Action plan and recommendation emanated from the ANS Cyber Resilience Table-top exercise. The Paper also address the issue of enhancement of the ATM Cyber Security portal

Action by the meeting is at paragraph 3.

REFERENCES

- Annex 17- Aviation Security
- Assembly Resolution A41-19
- MIDANPIRG/19 Meeting Report (14-17 February 2023, Riyadh, Saudi Arabia)

1. INTRODUCTION

1.1 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.

1.2 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.

1.3 The 41st Assembly called upon States and industry stakeholders 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.

1.4 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.

1.5 The First meeting of ANS Cyber Security Working Group (ACS WG/1) was successfully held during in Amman, Jordan, 16 November 2022.

2. DISCUSSION

2.1 The meeting may wish to recall that, the CNS SG/11 meeting tasked the Air Navigation Cyber Security Working Group (ACS WG) to conduct in depth GAP analysis between ICAO Cyber Security Action plan and the current implementation level in the MID region. Accordingly, the ACS WG/1 has developed initial list of actions for 2023-2024 as at **Appendix A**.

2.2 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. A survey will be conducted to establish how States have implemented the identified actions

2.3 The meeting may wish to note that ANS Cyber Resilience Tabletop Exercise (TTX) was successfully conducted 13-15 November 2022. The objectives of the workshop were to empower participants with measures to mitigate the exploitation of critical Air Navigation Systems, develop awareness on cyber issues affecting aviation, and foster a culture that promotes a secure and resilient use of the cyberspace. The documentation including the outcome of the TTX is at https://www.icao.int/MID/Pages/2022/Cyber%20SEC%20TTX.aspx

2.4 The TTX was presented with three (3) scenarios involving different aspects of Aviation Cyber security and Cyber resilience, which included ATM information sharing disruption, Senior leadership social engineering and Airport notification systems interference

2.5 The ACS WG/1 meeting reviewed the outcome of the TTX and propose the following recommendations emanated from the TTX:

a) 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.

b) States to develop Cyber incidents management plan including defining clear lines of communication and escalation.

c) 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.

d) CAAs are encouraged to collaborate with their National Computer Emergency Response Team (CERT) for cross industry incident management, as appropriate.

e) 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.

f) Cyber Resilience related procedures, risk analysis, exercises and trainings should be established and implemented.

g) An agreement on procedure on more timely coordination between FAS (ATSU) and airlines for abnormal flight plan submission is required.

h) 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.

i) States to ensure regular coordination between regulators, ANSPs, airport operators and airlines regarding Cyber Resilience.

j) Contingency plan should be in place which including back up system and condition for manual procedure.

k) 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.

l) 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.

2.6 The ACS WG/1 discussed the need to share experience on cyber threats and incidents, in this regard, the meeting recalled that UAE developed and hosted ATM data cyber security portal. The meeting tasked the ACS WG to review the portal and propose solution to enhance its use in the MID Region. Accordingly, the meeting propose the following Draft Conclusion:

DRAFT CONCLUSION CNS 12/XX: ENHANCEMENT ATM DATA CYBER SECURITY (ADCS) PORTAL

That, States be urged to:

i. assign ANS Cyber Security focal point(s) to register on the ADCS Portal;

*ii. provide feedback to the ADCS Admin by **1 July 2023** for further enhancements; and*

iii. 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) review, discuss and amend, as deem necessary, the Draft MID Region ANS Cyber Security Action Plan as **Appendix A**;

b) review, discuss and propose action, as appropriate, to the recommendations at para 2.5; and

c) agree to Draft Conclusion at para 2.6.

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-