INTERNATIONAL CIVIL AVIATION ORGANIZATION

MIDDLE EAST OFFICE

FIRST MEETING ANS CYBERSECURITY WORKING GROUP

(ACS WG/1)

(Jordan, 16 November 2022)

SUMMARY OF DISCUSSIONS

1.   PLACE AND DURATION

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

2.   OPENING

2.1   The meeting was opened by Ms. Muna Alnadaf, Regional Officer, Communication, Navigation and Surveillance, who extended a warm welcome to all participants to the first meeting of the ACS WG and wished them a successful meeting and a pleasant stay in Jordan. Mrs. Alnadaf thanked Jordan CARC for hosting the ACS WG/1 Meeting.

2.2   Mrs. Alnadaf highlighted that Cyber threats are currently growing at an increasing rate,,,, and therefore becoming a common concern to civil aviation, the reduction of cyber vulnerabilities and associated risks is critical to improve the resilience of the global aviation system.

3.   ATTENDANCE

3.1   The Meeting was attended by a total of twenty five (25) participants from six (6) States (Egypt, Iraq, Jordan, Qatar, Saudi Arabia, UAE), 1 Other States (Tunisia) and 1 International Organization (IATA) and ICAO Headquarters, ICAOMID. The list of participants is at **Attachment A**.

4.   Officers and Secretariat

4.1   Mrs. Muna Alnadaf, ICAO MID Regional Officer, Communication, Navigation and Surveillance (RO/CNS) was the Secretary of the meeting.

5.   DISCUSSION

Adoption of Provisional Agenda and Election of Chairperson

5.1   The meeting reviewed and adopted the Provisional Agenda
.
5.2   Mr. Yousif Al Awadi, Director - Communication, Navigation, Surveillance Systems – UAE, was unanimously elected as the Chairperson of the ANS Cyber Security Working Group (ACS WG).

5.3   Mr. Alawdi thanked the particpants for their trust and highlighted the need for effective participation of States and all stakeholders.

Regional ANS Cybersecurity Implementation

-     Conduct of the Regional Cybersecurity GAP Analysis

5.4   The meeting recalled that the CNS SG/11 meeting agreed to task the Air Navigation Cyber Security Working Group (ACS WG) to conduct in depth GAP analysis and propose action to the CNS SG/12 meeting.

5.5   The meeting received a presentation from Egypt on the subject, a gap analysis has been conducted between the ICAO cyber security action plan and the current implementation level in the MID Region. Initial list of actions have been identified for 2023-2024 as at **Appendix B**.

5.6   The meeting agreed to further review and update the MID Region ANS Cyber Security action Plan during the second meeting of the group and to conduct a survey to establish how States have implemented the identified actions

-     Review of the outcome of the Cyber Resilience Table Top Exercise

5.7   The meeting reviewed the outcome of the Cyber Resilience Table Top Exercise (13-15 November 2023, Amman, Jordan as at **Appendix C**.

5.8   The meeting recognized the need to conduct Cyber TTX at national level periodically for all stakeholders.

5.9   The meeting highlighted the need to establish Security Operation Center (SOC) for ANS cyber resilience.

5.10   The meeting agreed to the recommendations emenated from the TTX to be presented to the CNS SG/12 meeting for further review and endorsement.

-    ATM Data and Cybersecurity Portal

5.11   The The meeting discussed the need to share experience on cyber threats and incidents, in this regard, the meeting commended UAE for developing and hosting the ATM data cyber security portal (ADCS). The meeting agreed to request States assigning focal points and activate the use of ADCS

5.12   The ATM data cyber security (ADCS) portal has been established to be used as a prototype platform for information sharing of ANS cyber security.

Future Work Programme

5.13   The meeting was informed that Cyber Security and Resileince Symposium will be held in Doha, Qatar, 6-8 November 2023. The meeting agreed to conduct the second meeting of the ACS WG back-to-back with the Symposium.

Any other business

5.13   The meeting received a presentation on effective and efficient Communication management; including the core components of communication plan, communication types, various methods, tools and techniques.

6.   CLOSING

6.1   In closing, Mr. Al Awadi thanked the participants for their participation and excellent contribution to the meeting.

6.2   The participants thanked ICAO for organizing such a fruitful Meeting, as well as Jordan CARC for the hosting.

First Meeting of ANS Cyber Security Working Group (ACS WG/1)

(Amman, Jordan, 16 November 2022)

State/ Org	Contact	Title	Email
MID STATES			
Egypt	Mr. Ahmed Abdelwahab Mohamed El Marady	Senior Safety Oversight Inspector/ Communications, Navigation and Surveillance- ATSEP Engineer	ahmedabdelwahab02@yahoo.com ahmed.abdel-wahab@civilaviation.gov.eg
Iraq	Mr. Mostafa Z.Abdulameer Al-Dujai	Security & Network Specailist	cybersecurity@gcans.gov.iq
	Mr. Waleed Khaled Eesee Lami	CNS Manager	Cns.manager@gcans.gov.iq Waleed-khaled85@yahoo.com
Jordan	Mr. Ahmad Odeh	Training Supervisor	ahmad.odeh@carc.gov.jo
	Mr. Bassam Abed	Air Traffic Controller	bassam.abid@carc.gov.jo
	Mr. Ibrahim Mahmoud Suleiman Fara	Director of Technical Support	i.faraj@carc.gov.jo
	Mrs. Lina Abuawwad	Air Navigation Specialist	lina.abuawwad@carc.gov.jo
	Mr. Maha Khalifah Ali Al-jarah	Air Traffic Control Officer	maha.al-jarah@carc.gov.jo
	Mr. Mahmoud Mohammad R. Sabrah	Acting Director Air Navigation Services	m.sabra@carc.gov.jo
	Mrs. Marwa Khader Alta'any	Aviation Secutiry Inspector	marwa.taani@carc.gov.jo
	Mrs. Taghreed Al-assad	Head of Communication & Navigation Aids Division/KHIA	taghreed.al-assad@carc.gov.jo
	Mr. Wesam Jebreen	Air Navigation Specialist	wesam.jebreen@carc.gov.jo
Qatar	Mr. Salman Abdulla Alansari	Electronic Technician	Salman.abdulla@caa.gov.qa
	Mr. Khalid Mubarak Al Muftah	Electronic Equipment Consultant	Khalid@caa.gov.qa
Saudi Arabia	Mr. Abdullah Mohammed Albathi	Safety & Aviation Standards Sector	abalbathi@gaca.gov.sa
	Mr. Faisal A. Alzahrani	ESD-Automation Engineering Supervisor	fzahrani@sans.com.sa
	Dr. Majed Rajab	IT & Cyber Security Consultancy	M_m751@hotmail.com
	Mr. Bandar Al-Ansari		balansari@gaca.gov.sa
	Mr. Sultan Ahmad Hasan Alafifi	Cybersecurity Governance Senior Specialist	Sltn986@gmail.com
UAE	Mr. Chaudhary Shahzad Liaqat	Senior Specialist – ANS Engineering	Shahzad@szc.gcaa.ae
	Mr. Yousif Al Awadhi	Director-Communication, Navigation, Surveillance Systems	yawadi@szc.gcaa.ae
OTHER STATES			
Tunisia	Mr. Nsiri Khaled	CNS/ATM Senior Engineer	Khaled.nsiri@ifatsea.org
ORGANIZATIONS/INDUSTRIES			
IATA	Ms. Sharron Caunt	Regional Director Safety & Flight Operations (Africa & Middle East)	caunts@iata.org

State/ Org	Contact	Title	Email
ICAO HEADQUARTERS			
ICAO HQ	Mr. Michael Goodfellow	Technical Officer, Global Interoperable Systems, ANB/AN/GIS	MGoodfellow@icao.int
	Mr. Anton Kornetskiy	Technical Officer, Global Interoperable Systems, ANB/AN/GIS	AKornetskiy@icao.int
ICAO MID STAFF			
ICAO-MID	Mrs. Muna Alnadaf	RO/CNS	malnadaf@icao.int
	Mrs. Hoda Gabriel	Technical Assistant	hgabriel@icao.int

-END-

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	-

----

Cybersecurity Table Top Exercise

AMMAN, JORDAN | 24-27 OCTOBER 2022

Outcome of the Cyber Resilience Tabletop Exercise

History of the Workshop

➢ Hosted by Jordan CARC

➢ Eighty-four (84) participants from seven (7) States (Iraq, Jordan, Qatar, Saudi Arabia, Tunis and United States) and 1 Organization (IATA)

Objective

The objectives of this exercise are 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.

Summary of discussions

1- The Workshop was apprised of the Regional activities on the Cyber Resilience.

2- The Workshop was apprised of the Global challenges for Cybersecurity and what actions ICAO was undertaking to address them.

Cybersecurity Table Top Exercise

AMMAN, JORDAN | 24-27 OCTOBER 2022

3- The workshop 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

4- The workshop demonstrated global benefits for the aviation ecosystem by being part of IATF by reviewing actual Unmanned Aviation System (UAS) operation use cases related to a broad range of aviation stakeholders.

Cybersecurity Table Top Exercise

AMMAN, JORDAN | 24-27 OCTOBER 2022

1st Scenario: An airline is missing flight plan acknowledgements from enroute ANSPs. Airline keeps submitting the flight plans till they get an acknowledgement. Flooding/Duplicated Flight Plans into the FPL processing (FDP) and also surveillance data sharing.

2nd Scenario: The media is aware of the issue going on. ANSP leadership tries to coordinate a common response. The issues within the ATM infrastructure have undermined the capacity of the system by 50%. .

3rd Scenario: Capital City Airport (Flight Information Display Sub-System-FIDS malfunction) (Boarding delays due to no-show passengers at the gate and passenger are being directed to incorrect gates)

5- The Workshop noted that the International Aviation Trust Framework (IATF) aims to enable trusted, secured, and resilient A/G, G/G and A/A data exchange between all stakeholders; furthermore, it was apprised of the core principles and benefits of the IATF;

6- The Workshop was apprised of UAE's activities related to ANS Cyber Resilience including, but not limited to, establishment of Security Operation Center (SOC), continuous enhancement of the ADCS portal and conduct of various training/workshops;

Cybersecurity Table Top Exercise

AMMAN, JORDAN | 24-27 OCTOBER 2022

7- The National Cyber security center in Jordan briefed the Workshop on the role of cybersecurity in advancing digital transformation, Cyber dependency and Risk management process.

The Workshop celebrated the international day of ATSEP (12 November 2022)

Recommendations

➢ 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.

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

➢ 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.

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

➢ 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.

➢ Cyber Resilience related procedures, risk analysis, exercises and trainings should be established and implemented;

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

➢ 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;

➢ States to ensure regular coordination between regulators, ANSPs, airport operators and airlines regarding Cyber Resilience;

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

- ➢ 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
- ➢ 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;