ICAO

MIDANPIRG 21 and RASG-MID 11

ABU DHABI, UAE | MARCH 4-8, 2024

HOSTED BY

United Arab Emirates

ANS Cyber Resilience

Regional Developments on Cybersecurity

Cybersecurity and Resilience Symposium Outcomes

Mohamed Iheb Hamdi
ICAO Regional Officer, Aerodromes and Ground Aids
ICAO MID Coordinator for ANS Cybersecurity

Regional Developments on Cybersecurity

MIDANPIRG CONCLUSION 20/43:
MID REGION ANS CYBERSECURITY 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 Cybersecurity Action Plan at **Appendix 6.6G** 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,

Regional Developments on Cybersecurity

MIDANPIRG CONCLUSION 20/44:
ANS CYBERSECURITY CAPACITY BUILDING ACTIVITIES

That, to assist States building capacity on ANS cybersecurity & resilience, capacity building activities on ANS Cybersecurity be organized in 2024

Regional Developments on Cybersecurity

MIDANPIRG CONCLUSION 20/45:
ENHANCEMENT ATM DATA CYBERSECURITY (ADCS) PORTAL

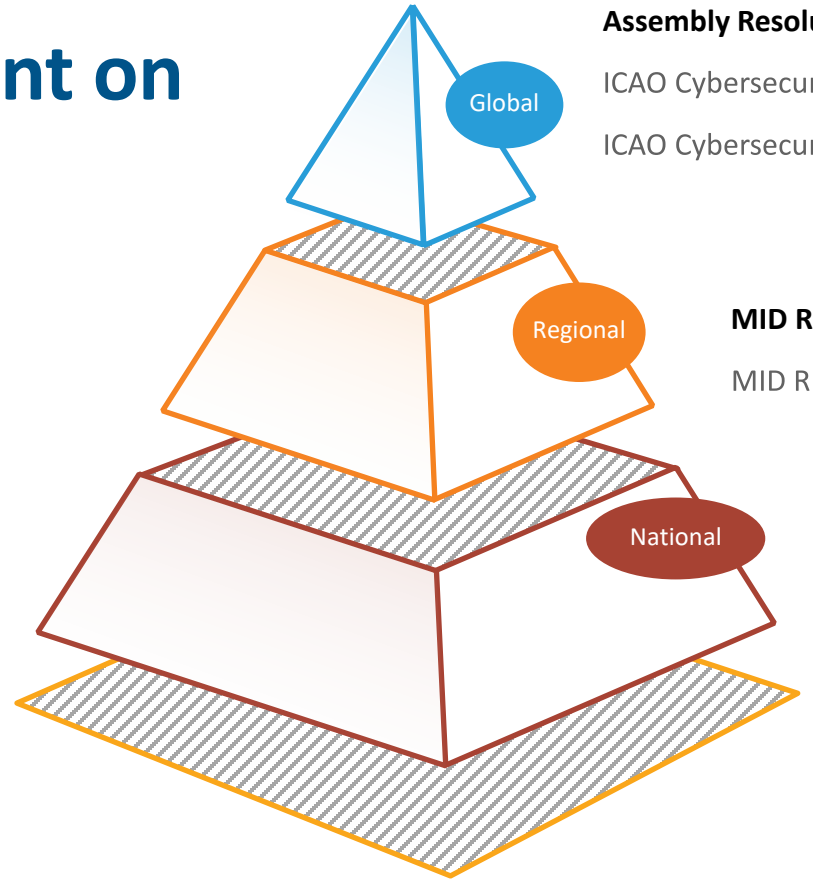
That, States be urged to:

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 cybersecurity, through the ADCS Portal.

MID State engagement on Cybersecurity



Assembly Resolution A41-19

ICAO Cybersecurity Strategy

ICAO Cybersecurity Action Plan

MID REGION

MID REGION ANS CYBERSECURITY ACTION PLAN

State Level

States Commitment to implement the MIDANPIRG CONCLUSION 20/43

Cybersecurity and Resilience Symposium

(Doha, Qatar, 6 – 8 November 2023)

Outcomes Summary

- 95 Participants
- 13 States
- 3 International Organizations

Agenda

Session 1: Setting the scene

Session 2: Cyber-attack Governance and effective legislation and regulations: a path to Cyber maturity

Session 3: Aviation Cybersecurity Framework: to enhance the resilience of aviation infrastructure against cyber threats

Session 4: Effective Cybersecurity intelligence and Monitoring techniques: to mitigate Cyber-attack impact

Session 5: Emergency Response and Contingency Planning

Session 6: Cybersecurity Case study

Session 7: Human Factors in Cybersecurity

Session 8: Aviation Cybersecurity: Emerging Challenges and Solutions

Cyber-attack Governance and effective legislation and regulations: a path to Cyber maturity

Main recommendations for States:

- **Establish competent national authorities responsible for cybersecurity.**
- **Develop and enforce comprehensive legislation and regulations to enhance cybersecurity.**
- **Foster international cooperation and information sharing to address cyber threats collectively.**

Aviation Cybersecurity Framework: to enhance the resilience of aviation infrastructure against cyber threats

Main recommendations for States:

- **Enhance cybersecurity awareness and training programs for aviation personnel.**
- **Implement robust risk management frameworks to identify and mitigate cyber threats.**
- **Foster collaboration between aviation stakeholders to share information and best practices.**

Effective Cybersecurity intelligence and Monitoring techniques: to mitigate Cyber-attack impact

Main recommendations for States:

- **Establish robust information sharing networks and platforms for cybersecurity intelligence.**
- **Develop national contingency plans that incorporate cybersecurity considerations.**
- **Invest in advanced monitoring tools and capabilities, including the establishment of SOC.**

Emergency Response and Contingency Planning

Main recommendations for States:

- **Develop emergency response plans specific to the aviation sector.**
- **Conduct regular drills and simulations to test and improve emergency response preparedness.**
- **Enhance collaboration and communication channels among stakeholders in emergency situations.**

Cybersecurity Case study Discussed

Main recommendations for States:

- **Conduct regular cybersecurity training and exercises to improve incident response capabilities.**
- **Establish collaboration and coordination mechanisms for incident response among relevant organizations.**
- **Stay updated on emerging cybersecurity trends and share knowledge within the aviation community.**

Human Factors in Cybersecurity

Main recommendations for States:

- **Implement comprehensive cybersecurity training programs for aviation personnel at all levels.**
- **Foster a culture of cybersecurity awareness and accountability within organizations.**
- **Invest in continuous skill development and capacity building to mitigate human-related cybersecurity risks.**

Aviation Cybersecurity: Emerging Challenges and Solutions

Main recommendations for States:

- **Promote research and development in aviation cybersecurity to address emerging challenges.**
- **Implement risk-based approaches to cybersecurity, considering the evolving threat landscape.**
- **Foster collaboration between aviation stakeholders, technology providers, and cybersecurity experts to develop innovative solutions.**

Thank You

ICAO