ASPIG/6–IP/3
23/05/2024

International Civil Aviation Organization

Sixth Meeting of the Aerodrome Safety, Planning & Implementation Group

(ASPIG/6) ***(Muscat, Oman, 27-29 May 2024)***

Agenda Item 5: Any Other Business

OUTCOMES OF THE CYBERSECURITY AND RESILIENCE SYMPOSIUM (DOHA, QATAR, 6 - 8 NOVEMBER 2023)

(Presented by the Secretariat)

SUMMARY

This paper provides an update on the Outcomes of the Cybersecurity and Resilience Symposium held in Doha, Qatar, from 6 to 8 November 2023, leading to a regional agreement on a Conclusion about Cybersecurity Systems Resilience, during the MIDANPIRG/21 that was successfully held in Abu Dhabi, UAE from 4 to 8 March 2024.

REFERENCES

- Resolution A41-19: Addressing Cybersecurity in Civil Aviation
- Aviation Cybersecurity Strategy
- Cybersecurity Action Plan

1. INTRODUCTION

1.1 The Cybersecurity and Resilience Symposium was held in Doha, Qatar, from 6 to 8 November 2023. The meeting may wish to recall that the MIDANPRG/21 noted with appreciation the outcomes of the Symposium at **Appendix A** and agreed to the following Conclusion:

> *MIDANPIRG CONCLUSION 21/28: CYBERSECURITY SYSTEMS RESILIENCE*
>
> *That, States consider the recommendations in Appendix 5M which would support the enhancement of their cybersecurity systems resilience.*

2. ACTION BY THE MEETING

2.1 The meeting is invited to note the information contained in this paper.

Recommendation emanating from the

Cybersecurity and Resilience Symposium

(Doha, Qatar, 6 – 8 November 2023)

MID States are encouraged to consider the following recommendations emanating from the Symposium, to support the enhancement of their cybersecurity systems resilience:

Item 1: Cyber-attack Governance and effective legislation and regulations: a path to Cyber maturity

- 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.

Item 2: Aviation Cybersecurity Framework: to enhance the resilience of aviation infrastructure against cyber threats

- 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.

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

- 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.

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

- 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.

Item 5: Emergency Response and Contingency Planning

- 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.

Item 6: Human Factors in Cybersecurity

- 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.
- 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.

- END –