International Civil Aviation Organization

MIDANPIRG/21 & RASG-MID/11 Meetings

(Abu Dhabi, UAE, 4 – 8 March 2024)

Agenda Item 5.3: ANS (AIM, PBN, AGA-AOP, ATM-SAR, CNS and MET

ADDRESSING THE CHALLENGES OF SECURE INFORMATION SHARING IN CIVIL AVIATION: THE RISKS OF UNSECURED EMAIL COMMUNICATION

(Presented by the United Arab Emirates)

SUMMARY

This paper underscores the critical issue of sharing sensitive and confidential aviation-related information through unsecured channels. It highlights the risks associated with such practices, including data breaches, unauthorized access, and non-compliance with international aviation regulations and standards. By addressing this critical issue, we can foster a more secure and resilient global aviation network in alignment with ICAO Aviation Cybersecurity Strategy.

Action by the meeting is at paragraph 3

REFERENCES

- ICAO Aviation Cybersecurity Strategy - October, 2019
- ICAO Cybersecurity Culture in Civil Aviation - January 2022
- ISO/IEC 27001
- NIST Cybersecurity Framework

1. INTRODUCTION

1.1 In an era where digital communication has become integral to the operations of civil aviation, the security of information shared through these channels is significant.

1.2 However, a concerning trend has emerged where states utilize unsecured email systems for the exchange of confidential aviation-related information specifically while establishing new or troubleshooting existing inter connectivity. This practice not only poses a significant risk to the integrity and confidentiality of sensitive data but also potentially jeopardizes the safety and security of global aviation operations.

1.3 The need to address this issue is underscored by the growing sophistication of cyber threats and the critical nature of the information being exchanged. This paper aims to bring attention to the risks associated with the use of unsecured emails for official communication in the civil aviation sector and to propose strategies to mitigate these risks, aligning with ICAO and international standards and best practices.

1.4 The commitment of all civil aviation stakeholders to bolster cyber resilience is pivotal in safeguarding the aviation sector against cyber threats that may compromise safety, security, and operational continuity. This commitment is a fundamental aspect of enhancing the sector's defense against potential cyber-attacks. The ICAO Cyber Security Strategy emphasizing the need for a united front in cybersecurity efforts across the aviation industry.

2. DISCUSSION

2.1 Prevalent Practices: Many states continue to rely on conventional email systems for the transmission of sensitive aviation-related information. These practices persist despite growing cybersecurity threats. Such practices are observed mainly within the CNS domain of ANSP’s during activities of establishing new or troubleshooting existing inter connectivity links.

2.2 The use of unsecured communication channels significantly increases the risk of sensitive information being accessed by unauthorized parties. This risk is particularly acute given the nature of the Air Navigation Services sophisticated and interconnected environment, which often includes operational IP details and network security measures.

2.3 Unsecured communication channels such as emails are vulnerable to interception, potentially allowing malicious actors to gain insights into secure operations, or even orchestrate cyber-attacks.

2.4 This practice stands in potential violation of various international data protection regulations and fails to adhere to the cybersecurity guidelines recommended by ICAO and other bodies.

2.5 In the aviation sector, where the exchange of confidential information is a routine yet critical operation, the application of NIST guidelines and the ISO/IEC 27000 series, particularly ISO/IEC 27001, becomes increasingly relevant.

2.6 The NIST framework, renowned for its comprehensive approach to cybersecurity, offers valuable guidance tailored to managing and mitigating cyber risks, particularly pertinent when addressing the challenge of sharing confidential information through unsecured channels. It emphasizes a risk-based approach, concentrating on the identification, protection, detection, response, and recovery from cybersecurity threats.

2.7 Similarly, ISO/IEC 27001, a key part of the ISO/IEC 27000 series, offers a systematic methodology for managing sensitive company information, making it particularly relevant for the aviation industry. This standard advocates for the implementation of a robust Information Security Management System (ISMS), which is instrumental in securing all forms of data, including that exchanged via electronic communications

2.8 By integrating these standards into their operations, aviation entities can significantly bolster their defenses against cyber threats, ensuring the integrity and confidentiality of vital information flows in the sector, particularly in securing confidential data shared over unsecured channels. This integration ensures robust protection of vital information flows, aligning with ICAO's strategies and action plans. Such compliance not only enhances cybersecurity but also supports the safety and efficiency of global aviation operations, reinforcing a unified approach to tackling digital threats in the aviation industry

3. ACTION BY THE MEETING

3.1 The meeting is invited to

a) take note of the information contained in this paper;

b) Urge states to enforce respective cyber security measures and refrain from sharing confidential information through unsecured channels; and

c) encourage States to increase awareness of cybersecurity, including activities to establish appropriate cyber hygiene.

- END -